LA NECESIDAD DE UNA REFORMA DE LA LEY ORGÁNICA 15 /1999 DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

www.asociacioncli.es

PROPUESTA DE PROYECTO DE LEY POR EL QUE SE MODIFICA LA LEY ORGANICA 15/1999, DE 13 DE DICIEMBRE DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

LA NECESIDAD DE UNA REFORMA DE LA LEY ORGÁNICA 15 /1999 DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

El progreso de la Sociedad de la Información, provocado por el avance de las Nuevas Tecnologías, exige una revisión firme de la normativa que la regula, y en especial por cuanto se vean afectados los derechos fundamentales.

I. EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS.

El derecho fundamental a la Protección de Datos de Carácter Personal, surge dentro de la llamada "Sociedad de la Información", como un concepto indefinido jurídicamente. La realidad evolutiva y las oportunidades que las Nuevas Tecnologías han ido abriendo para el tratamiento de todo tipo de datos e información, hicieron necesario conceptuar y plasmar este nuevo derecho fundamental en los textos constitucionales de todos los Estados Miembros de la Unión Europea. Así, la **"autodeterminación informativa"**, *derecho que asiste a una persona para decidir, por sí misma, de qué datos pueden disponer otros y en qué circunstancias, con qué límites, pueden ser revelados en cuando forman parte de su intimidad (son secretos de su vida)*[1], nace en la doctrina alemana, y se confirma como definitiva mediante la Sentencia del Tribunal Federal de Alemán (*BVerfG*) de 15 de septiembre de 1983. Siguiendo estos postulados, los repertorios normativos europeos comienzan a tratar esta materia estableciendo la protección de la intimidad en un sentido más amplio, proclamándose el derecho a la protección de datos de carácter personal como derecho fundamental, autónomo y de obligado respeto por los Estados, en el Convenio Europeo para la protección de los Derechos Humanos y las Libertades Fundamentales (Roma,1950), en el Convenio 108/1981 del Consejo de Europa, para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Estrasburgo, 1981), la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en

[1] BAON RAMIREZ, Rogelio. *VISION GENERAL DE LA INFORMATICA EN EL NUEVO CODIGO PENAL*. En: Revista del Consejo General del Poder Judicial. C.G.P.J. Núm. XI., Ambito jurídico de las tecnologías de la información, Madrid, 1996, pág. 82 y 85.

lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos, y en lo que a España respecta, el artículo 18 de la Constitución y la LO 15/99 de Protección de Datos de Carácter Personal.

II. EL PROGRESO DE LA SOCIEDAD DE LA INFORMACIÓN.

Desde la promulgación de la antigua LORTAD en 1992, hasta hoy, el contenido del derecho fundamental a la Protección de Datos de Carácter Personal, no ha variado en su esencia, pero sí las formas de protegerlo, y ello en el sentido de que cada día nos vemos involucrados en situaciones que nos exigen tomar decisiones importantes sobre los tratamientos de nuestros datos de carácter personal, bien en el trabajo (vigilancia electrónica del trabajador), en el cuidado de nuestra salud (tarjeta sanitaria electrónica), en la elección democrática de nuestros representantes (voto electrónico), en nuestro ocio (comercio electrónico, compras y reservas en la Red), ... y un larguísimo etcétera.

Por este motivo, la jurisprudencia se ha visto obligada a "actualizar e interpretar" las disposiciones que hoy nos están dando las pautas de actuación, tanto para el tratamiento de los datos de carácter personal como para su defensa frente a injerencias no autorizadas. Junto a ella, la Agencia Española de Protección de Datos, órgano garante del cumplimiento de la legislación sobre protección de datos y del control sobre su aplicación, tiene entre sus funciones la de dictar, sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la Ley, y en su caso "aclarar" los términos legales de ésta.

Y todo ello, en estos últimos años, nos ha dado un resultado: **la necesidad de reformar la LOPD** y adaptarla coherentemente a las exigencias de esta realidad evolutiva.

III. PROPUESTAS DE REFORMA DE LA COMISIÓN DE LIBERTADES E INFORMÁTICA A LA LOPD.

Partiendo del Derecho Comunitario y Nacional, la jurisprudencia habida hasta hoy, las instrucciones de la Agencia Española de Protección de Datos, argumentos desarrollados por los diferentes partidos políticos en momentos anteriores a la promulgación de la LOPD, el derecho comparado y la experiencia de haber tomado el pulso a los distintos sectores sociales, la Comisión de Libertades e Informática ha elaborado una serie de propuestas que no pretenden sino mejorar las evidentes carencias de esta Ley.

índice

PROPUESTAS DE LA CLI PARA UN PROYECTO DE LEY POR EL QUE SE MODIFIQUE LA LEY ORGANICA 15/1999, DE 13 DE DICIEMBRE DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

1 .- EXPOSICIÓN DE MOTIVOS.

La Comisión de Libertades e Informática, defiende la necesidad de la redacción de una exposición de motivos, que desarrolle las razones de la transposición de la Directiva 45/96/CE, el espíritu de la anterior LORTAD, y del art. 1 de la LOPD actual. Se presenta un preámbulo que explica la necesidad de dicha exposición de motivos, tal y como existía en la antigua LORTAD, se hace un repaso por el desarrollo del derecho y las principales novedades de la reforma.

EXPOSICIÓN DE MOTIVOS

(….)

La primera ley que en España reguló el tratamiento automatizado de los datos de carácter personal fue la LO 5/92 (LORTAD). Contenía un didáctico y elogiado, en su momento, preámbulo del que es posible rescatar a modo de memoria histórica algunos principios, ya que la jurisprudencia y el desarrollo legislativo nacional e internacional demandan una exposición actualizada que justifique las variantes de la actual ley de protección de datos de carácter personal. Un principio inalterable es que el conocimiento ordenado de los datos de carácter personal permite dibujar un determinado perfil de la persona, que puede resultar luego valorado favorable o desfavorablemente para todas sus actividades públicas o privadas. Y no cabe duda que el tratamiento de datos de carácter personal , desde los más inocuos hasta los más sensibles, puede incidir negativamente o menoscabar el ejercicio de derechos intrínsecos del ser humano. Las generaciones de derechos fundamentales han evolucionado, ampliándose por reacción a cambios sociales, políticos, económicos o tecnológicos, así, el siglo XXI conlleva, entre otras realidades, la revolución Tecnológica, y ahí se incorpora la protección de los datos de carácter personal o libertad informática, en su doble contenido: el negativo o exclusión de todo lo externo que afecte a la intimidad y el positivo o posibilidad de ejercer las facultades que

permiten a la persona controlar por el acceso, rectificación, cancelación u oposición, todos sus datos.

Retomando la dogmática de la Constitución Española, el Art. 18 reconoce el derecho individual al honor, intimidad personal y familiar y propia imagen, y en el párrafo 4, en un innegable alarde innovador, emplaza a limitar 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 legislador tenía ante sí, básicamente dos campos de actuación: El primero, la informática, que en los años setenta era tanto un potencial recurso de apertura al progreso tecnológico, como una herramienta agresiva para los tradicionales derechos fundamentales. Y el segundo, formado por los derechos fundamentales de la intimidad y el honor. El primer desarrollo legislativo del Art. 18, lo materializa la LO 1/82 de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Se presentó la ocasión de incluir una disposición transitoria ordenando que, en tanto no se desarrollara el Art. 18.4, la intromisión en tales derechos ocasionada por el uso de la informática quedaba sujeta a lo previsto en esa ley.

La Constitución Española nominalmente no concede identidad jurídica propia como derecho fundamental a la protección de datos de carácter personal . Es la Jurisprudencia del Tribunal Constitucional la que comienza pronunciando en la STC 254/1993 que la "libertad informática", estaba reconocida por el Art. 18.4 CE (....) como la libertad de controlar el uso de datos de carácter personal insertos en un programa informático: lo que se conoce con el nombre de "habeas data" .

Tampoco la LORTAD explicitaba como derecho de la personalidad la protección de datos de carácter personal . Su finalidad es hacer frente a los riesgos que para los mismos puede suponer el acopio y tratamiento por medios informáticos, y su objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos. No obstante supuso la primera cobertura legal al habeas data, compendio de los derechos nucleares de acceso, rectificación, cancelación y oposición del afectado sobre sus datos de carácter personal .

La expansión de las Tecnologías de la Información y del Conocimiento en el nuevo orden de la Sociedad de la Información, apremia a la Unión Europea a instar a los Estados miembros la incorporación en su respectivo Derecho interno de la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal y a la libre circulación de los mismos. Es entonces cuando el Derecho comunitario procede a precisar y ampliar los contenidos del Convenio de 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos de carácter personal y España se adapta al derecho comunitario con la aprobación de la LO 15/99 de protección de datos de carácter personal (LOPD), derogándose la anterior LORTAD. Diversos artículos de la nueva Ley se recurren por inconstitucionalidad y el Tribunal Constitucional se pronuncia estimando el recurso en la sentencia 292/2000, porque los preceptos recurridos no respetan el contenido esencial del derecho

fundamental al honor y a la intimidad personal y familiar así como del derecho fundamental ahora denominado derecho a la Protección de Datos.

Los Fundamentos Jurídicos de la STC 292/00 renuevan la doctrina jurídica, establecen su contenido esencial y regulan el ejercicio de facultades que integran el derecho fundamental a la protección de datos. Significó el ensanchamiento, a través de la jurisprudencia, del catálogo de derechos y libertades reconocidos expresamente en la Constitución Española. La consolidación legítima como derecho fundamental, de la protección de datos de carácter personal, y el reforzamiento de su protección, se presenta respectivamente en la Carta de los Derechos Fundamentales de la Unión Europea en el año 2000 y en la Directiva 2002/58/CE que pretende garantizar el respeto de los derechos fundamentales y los principios consagrados en la Carta, así como, especificar y completar la Directiva 95/46, en lo que respecta al tratamiento de los datos de carácter personal en el sector de las comunicaciones electrónicas.

Concluye el aporte jurídico de la Unión Europea en el ámbito de los derechos fundamentales, con el consenso de los Estados y la firma del Tratado por el que se establece una Constitución para Europa, y que supone un impulso para la protección de los datos de carácter personal. La Constitución les da categoría de principios para el desarrollo de la vida democrática de la Unión y los integra entre los derechos de libertad de la renovada Carta de los Derechos Fundamentales de la Unión.

Junto al reconocimiento del derecho fundamental a la protección de los datos de carácter personal evolucionan límites y garantías en su ejercicio. La LO 15/99 de Protección de Datos de Carácter Personal, es la norma que ha venido regulando la base de los principios de su protección, así como, de los derechos de las personas en su ejercicio. Los siete Títulos que la componen tienen por objetivo la adecuación del ordenamiento jurídico nacional al comunitario y la adaptación a las circunstancias sociales y legales internas.

Algunos de los motivos que justifican la presente reforma son: La necesidad de acabar con la incertidumbre –cuando no inconstitucionalidad en su sentido literal- que provocaba la existencia del término “incompatibles” en al art. 4.2 referido a las finalidades para las cuales se recaban los datos, dejando ya sentado que los datos recabados para una finalidad concreta no podrán ser utilizados para finalidades distintas a aquella. El término incompatibles queda -tal y como aparece en la Directiva 95/46/CE - para los tratamientos; La introducción de la figura del Delegado de Protección de Datos como un garante del derecho y colaborador de las Autoridades de Control en materia de protección de datos; La regulación específica de los requisitos para la obtención de los datos de los menores de edad; La necesidad de disociar los datos en los casos de tratamientos al margen de la regulación general siempre que tal disociación sea posible; La posibilidad de adoptar medidas cautelares previas al tratamiento de datos cuando estos menoscaben derechos de los interesados; La modificación de la composición del Consejo de Protección de Datos para adaptarlo mejor a las principales realidades sociales implicadas en materia de protección de datos; La supresión del censo promocional; La introducción de las llamadas “Listas Robinson”; la prevención de que el régimen sancionador se adapte mejor a la realidad sancionadora dando un margen mayor a la Administración para

adecuar las sanciones a la realidad concreta de cada infracción y estableciendo medidas para evitar en la medida de lo posible que económicamente sea más rentable abonar una sanción que cumplir con la legalidad, etc.

2.- DERECHO FUNDAMENTAL.

Se propone un replanteamiento de la redacción del artículo 1, para incluir directamente en la Ley Orgánica 15/99 de Protección de Datos de Carácter Personal (en adelante LOPD) que lo que se va a desarrollar es la protección de un derecho fundamental, autónomo e independiente (STC 292/00) intentando salvar la literalidad del texto constitucional.

> **Artículo 1. Objeto.**
>
> La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

A estos efectos, **la Comisión de Libertades e Informática propone la siguiente redacción**:

> **Art. 1.** La presente Ley Orgánica tiene por objeto garantizar y proteger el derecho fundamental a la protección de los datos de carácter personal, así como el honor e intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos en lo que concierne al tratamiento de dichos datos.

3.- DEFINICIONES

El artículo 3, establece una serie de definiciones que ayudan a la comprensión del texto legal, y para su mejora se propone la introducción de dos nuevas definiciones, una sobre el "Delegado de Protección de Datos", una de las novedades propuestas por la CLI, existentes en otros ordenamientos, y cuyo fundamento de inclusión se encontrará en el apartado 11, y otra sobre lo que se considera "Bloqueo de datos", extraída de la definición que para ello da el art. 1.1 del R.D. 1332/1994.

A estos efectos, **la Comisión de Libertades e Informática propone la introducción de las siguientes definiciones:**

> **Art. 3 e. bis) Delegado de Protección de Datos:** Persona física o jurídica, de naturaleza pública o privada, encargada de velar por el cumplimiento de lo dispuesto en la presente Ley y en su normativa de desarrollo en el seno de las entidades que traten datos de carácter personal

Art. 3 k) Bloqueo de datos: la identificación, reserva e implantación de los medios necesarios que garanticen su conservación con el fin de impedir su tratamiento.

4.- FICHEROS DE TERRORISMO.

El tratamiento de los ficheros de datos de carácter personal sobre la investigación y represión del terrorismo, exige un trato especial por la materia que se trata, y así se excluye de la aplicación de la LOPD.

> **Artículo 2. Ámbito de aplicación**
>
> **2.** El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:
>
> **c)** A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada (...).

A juicio de la CLI, ello no significa que sea incompatible con la normativa establecida en la LOPD, y por tanto es posible respetar las garantías previstas sobre los derechos de los ciudadanos en el sentido que proponemos.

La exclusión del régimen de protección de datos prevista en esta letra c) carece de sentido cuando:

- por un lado, la Ley contempla la exclusión de los ficheros sometidos a la normativa sobre protección de materias clasificadas, en la letra anterior del mismo apartado,
- por otro, el artículo 22 de la propia norma establece un régimen especial relativo a los ficheros de las Fuerzas y Cuerpos de Seguridad.
- finalmente, en los artículos 23 y 24, se prevén excepciones a los derechos de los afectados por razones, entre otras, de defensa del Estado, seguridad pública, necesidades de las investigaciones en curso de las Fuerzas y Cuerpos de Seguridad o de la persecución de infracciones penales.

El 1 de octubre de 1998 entró en vigor en España el Convenio hecho en Bruselas el 26 de julio, basado en el artículo K.3 del Tratado de la Unión Europea, por el que se crea una Oficina Europea de Policía (en adelante, Convenio Europol), entre cuyos objetivos está el de cooperación entre los Estados Miembros, con vistas a la prevención y lucha contra el terrorismo, el tráfico ilícito de estupefacientes y otras formas graves de delincuencia internacional. Para ello, establece un sistema de información informatizado, al que, en virtud de su artículo 7, los Estados suministrarán datos directamente "observando su legislación nacional", y que serán facilitados por Europol al resto de Estados en determinados supuestos.

Pues bien, el Convenio Europol no excluye el citado sistema de información de las garantías y del sistema de protección de datos estipulado en los respectivos ordenamientos estatales. Antes bien, además de introducir garantías propias para impedir una invasión desproporcionada de la intimidad por causa de las previsiones del Convenio, realiza continuamente llamadas a la legislación nacional y comunitaria sobre datos de carácter personal, para hacer efectiva la protección que los Estados miembros deben garantizar en cumplimiento del mismo y del Convenio de Roma de

1981, al que expresamente cita en su artículo 13. Se pueden citar en este sentido los artículos: 7.3, 8.4, 9.1, 17.1, 19.3, y en especial el artículo 14, relativo al nivel de protección de los datos, y los artículos 23. 2. y 38.11, sobre las competencias de la autoridad nacional de control en materia de este convenio y la protección de los ciudadanos

En resumen, la exclusión del ámbito de aplicación de la Ley Orgánica, de los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada, no sólo es contraria a las previsiones incluidas en los Convenios Internacionales para la protección de datos de carácter personal firmados por España, sino que dificulta gravemente la aplicación del Convenio Europol, específicamente realizado para el tratamiento de datos de carácter personal con estos fines, y especialmente en lo que se refiere al sistema de garantías previsto en el mismo para la protección del derecho fundamental a la autodeterminación informativa.

Además, resulta incompatible con las propias previsiones que la Ley Orgánica, en sus artículos 22 a 24, establece en relación con la recogida y tratamiento para fines policiales, de datos de carácter personal, por las Fuerzas y Cuerpos de Seguridad, y su régimen específico. En efecto, la interrelación entre los ficheros creados para la persecución de los delitos es de hecho tal, que resulta impensable la estanqueidad de los mismos a los efectos de su adecuación al régimen de protección establecido en la Ley Orgánica.

A estos efectos, **la Comisión de Libertades e Informática propone la siguiente modificación:**

> **Art. 2.3.** Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos de carácter personal:
>
> 2.3. f) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.

***Conexión:** art. 23.2

5.- FINALIDAD.

El principio de finalidad se recoge en el artículo 4 de la LOPD con la siguiente redacción:

> **Artículo 4. Calidad de los datos.**
>
> **2.** Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

La esencia de todo el sistema de protección de los datos de carácter personal, es que el titular de los mismos tenga la seguridad de que la recogida de sus datos tiene una finalidad legítima concreta, de la que debe ser informado previamente al amparo del artículo 5.1 de la misma Ley, y que sus datos serán utilizados con esta concreta finalidad, y no otra. En otro caso, perdería además toda virtualidad y eficacia la posibilidad de ejercitar los derechos de acceso, rectificación o cancelación de los datos, al no poder tener la certeza de para qué se utilizarán éstos.

En la Sentencia 292/00, el Tribunal Constitucional dispone que el consentimiento de la persona para la obtención, almacenamiento y tratamiento –cualquier tratamiento pues no hace distingos- requiere como complemento indispensables "la facultad de saber en cada momento quién dispone de esos datos de carácter personal y a qué uso los esta sometiendo" (FJ 7). Si los responsables del tratamiento disponen que los datos recogidos para un determinado fin sean aplicados a otro distinto -por muy compatible que sea- se está anulando el original consentimiento del interesado y obviando el necesario para ese nuevo fin. Esto también se confirmó en otras sentencias del TC, la 254/93 (FJ 6 y 7), y la 11/98 (FJ 4º).

El Tribunal Constitucional tiene clara la distinción entre finalidades "distintas" y finalidades "incompatibles" pues señala que "*el derecho a consentir en la recogida y el tratamiento de los datos personales no implica en modo alguno consentir la cesión de tales datos a terceros (...) Y la cesión de los mismos a un tercero para proceder a un tratamiento con fines distintos de los que originaron su recogida, aun cuando sean compatibles con estos* (art. 4.2) *supone una nueva posesión y uso que requiere el consentimiento del interesado*". (FJ 13) .

Más recientemente, hemos de citar la Sentencia de la Sala de lo Contencioso Administrativo de la Audiencia Nacional de 11 de Febrero de 2002, en su FJ4, que dice que "*En relación con la interpretación de la expresión "finalidades incompatibles" (...) el diccionario de la Real Academia establece que "incompatibilidad" significa "repugnancia que tiene una cosa para unirse con otra, o de dos o más personas entre sí", por tanto, una interpretación literal ampararía el uso de los datos para cualquier fin abriendo una gama indefinida e ilimitada de finalidades, pues es muy difícil imaginar usos que produzcan la repugnancia que evoca la incompatibilidad, por lo que "semejante interpretación conduce al absurdo y como tal ha de rechazarse", como hemos declarado en Sentencia de 8 de febrero de 2002. Teniendo en cuenta, además, que dicho término se introduce en la Ley de 1999, como ha declarado la doctrina, por una traducción poco precisa del artículo 6 de la Directiva 46/1995, de 24 de octubre, pues tal adjetivo se refería al tratamiento y no a los fines, con el objeto precisamente de asegurar que el tratamiento, sea cual sea éste, no pudiera resultar incompatible con el fin determinado, explícito y legítimo en virtud del cual se recogieron los datos".*

A estos efectos, **la Comisión de Libertades e Informática propone la siguiente redacción:**

> **Art. 4. 2.** Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades distintas de aquellas para las que los datos hubieran sido recogidos ni podrán tratarse posteriormente de manera incompatible

con dichos fines. No se considerara incompatible el tratamiento posterior y disociado de estos datos con fines históricos, estadísticos o científicos.

***Conexión**: D.A.4ª.

6.- DATOS HISTÓRICOS, ESTADÍSTICOS O CIENTÍFICOS.

El mismo artículo 4 de la LOPD, hace referencia a los datos tratados como históricos, estadísticos o científicos:

> **Artículo 4. Calidad de los datos.**
>
> **2.** Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

La propuesta de la CLI se hace necesaria para proteger estos datos en dos sentidos:

1. necesidad de la disociación de datos, cuando esto sea posible, es decir, permita el tratamiento en el sentido en que lo prevé la Ley.

2. proteger estos datos por cuanto pudieran poner en peligro la seguridad de las personas, su honor, la intimidad de su vida privada y familiar y su propia imagen, en cuyo caso, y a tenor de los dispuesto:

   a) por la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español, en lo que a documentos históricos se refiere (artículo 57.1c.).
   b) por dos importantes informes de la AEPD: "Publicación en Internet de datos históricos", y "Alcance del concepto del tratamiento de datos históricos con fines científicos o de investigación 2000", que coinciden en disponer que estos datos *no podrán ser públicamente consultados sin que medie consentimiento expreso e informado de los afectados o hasta que haya transcurrido un plazo de 25 años desde su muerte si su fecha es conocida o, en otro caso, de 50 años a partir de la fecha de los documentos en que consten*.
   c) Por la propia Disposición Adicional Tercera. Tratamiento de los expedientes de las derogadas Leyes de Vagos y Maleantes y de Peligrosidad y Rehabilitación Social, de la actual LOPD.
   d) Considerando 29, Directiva 46/95/CE.

A estos efectos, **la Comisión de Libertades e Informática propone la redacción de un segundo párrafo:**

> **Art. 4. 2.** 2º párrafo:

Si no pudiera realizarse la disociación por requerirlo así estos fines, los datos no podrán ser tratados si con ello se pusiese en peligro la seguridad de las personas, su honor, la intimidad de su vida privada y familiar y su propia imagen, ni, en todo caso, podrán ser públicamente consultados sin que medie consentimiento expreso e informado de los afectados o hasta que haya transcurrido un plazo de 25 años desde su muerte si su fecha es conocida o, en otro caso, de 50 años a partir de la fecha de los documentos en que consten.

***Conexión:** arts. 4.5, 5.5, 11.2.e) y 21.

7.- CONSENTIMIENTO

El consentimiento al tratamiento de los datos de carácter personal por su titular, se recoge en el art. 6 de la LOPD.

Artículo 6. Consentimiento del afectado.

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

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias ; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

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.

4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

En esta redacción se puede apreciar, la falta de previsión específica de una mención a los comunes “CONTRATOS DE ADHESIÓN” y la previsión de la exigencia de justificación para poder revocar el consentimiento dado.

La problemática de los contratos de adhesión, consiste en que el hecho de consentir al tratamiento de una serie de datos de carácter personal, no puede implicar el consentir en un solo acto, para el tratamiento de éstos, todos o alguno de ellos, con una finalidad distinta, pues se desvirtuaría lo que planteamos ya para el artículo 4.2., afectando esto también a una nueva propuesta en el artículo 6.1. *El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.*

Cada vez más proliferan contratos tipo tanto en el ámbito de la telefonía, de la banca o de los seguros (la CLI ha presentado dos denuncias ante la AEPD por estos temas), en los cuales se incluye una cláusula que informa (cuando no se hace constar que el interesado otorga su "consentimiento expreso") al afectado que los datos que serán objeto de tratamiento por motivos inherentes a la prestación del servicio van a ser tratados para fines de marketing y cedidos a terceros para estos mismos fines. Estas cláusulas dejan al interesado un plazo de 30 días para oponerse al tratamiento (exigiéndole normalmente que se haga fehacientemente, es decir mediante carta certificada). Si no se opone en dicho plazo, empezará el tratamiento de sus datos, si bien, el interesado podrá revocar tal consentimiento en cualquier momento. Aun cuando se produjeron unas autorizaciones a nivel reglamentario, el consentimiento así prestado no es válido por carecer de los requisitos esenciales exigidos por la LOPD: informado (nadie se lee la "letra pequeña" de los contratos"), libre (el afectado, en caso de que tome conocimiento efectivo de la cláusula, no tiene opción cómoda e igual de oponerse o a mostrar su disconformidad), específico (en muchos casos se hace una referencia general a "las empresas del Grupo", refiriéndose a una lista publicada en una página web, práctica avalada recientemente por la AEPD y dado el método utilizado (correo ordinario que no asegura en todos los casos su recepción –pérdida, ausencia del destinatario, segundas viviendas- etc, o su recepción puntal) este consentimiento tácito no resulta "inequivocamente" realizado.

A estos efectos, **la Comisión de Libertades e Informática propone la siguiente redacción:**

> **Art. 6.1.** El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa. No será válido el consentimiento otorgado mediante un contrato de adhesión, salvo que figure forma separada al clausulado general e implique una declaración expresa del interesado

*__Conexión:__ art. 5.3

Por otra parte, y sobre la exigencia de MOTIVACIÓN SUFICIENTE para poder revocar el consentimiento dado por una persona, la LOPD en su actual redacción, establece que el consentimiento puede ser, por una parte, revocado (6.3), sin que se le atribuyan efectos retroactivos, y siempre y cuando exista causa justificada para ello, y por otra parte, limita la legítima oposición (6.4) a cualquier tratamiento que no ha recabado previo consentimiento (por no ser necesario), a que existan motivos fundados y que respondan a una concreta situación personal. Es obvio que esta situación no cabe

plantearla como una regla general puesto que choca de lleno con el contenido esencial del derecho a la protección de datos de carácter personal, el derecho del individuo a disponer de sus propios datos, y así lo sostiene, sin mayores justificaciones, entre otras, la Sentencia 292/00 en su fundamento jurídico 7º : *son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele."*

A estos efectos, **la Comisión de Libertades e Informática propone la siguiente redacción:**

> **Art. 6. 3.** El consentimiento a que se refiere este artículo podrá ser revocado por el afectado en cualquier momento sin que se le atribuyan efectos retroactivos.
>
> **Art. 6. 4.** En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento. (----) En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

8.- CESIONES DE DATOS SENSIBLES POR LAS ADMINISTRACIONES PÚBLICAS.

El artículo 7 de la LOPD hace referencia a los datos especialmente protegidos, y en apartado número cinco expone lo siguiente:

> **Artículo 7. 5**. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

Recientemente ha aparecido este tema a propósito de la introducción del carné por puntos (noticia aparecida entre otros, en www.elmundomotor.com el 10.11.04). Las aseguradoras pidieron a la Dirección General de Tráfico (DGT) tener acceso al Registro de Conductores e Infractores "para tener conocimiento del estado de puntos de sus posibles clientes", según las propuestas para el anteproyecto de Ley por el que

se modifica el texto articulado de la Ley de Tráfico para regular los permisos y licencias de conducción por puntos.

Sin embargo, para que una empresa privada tenga acceso a datos de infractores en materia de seguridad vial "debe ser habilitado por Ley, aprobada en el Parlamento",según indicaron fuentes de la AEPD. En caso contrario, solo tendría acceso "el órgano competente para imponer sanciones", por lo que "las cesiones serán las que habilite la ley". Por este motivo, antes de aprobar el Registro de Conductores e Infractores, la Agencia Española de Protección de Datos deberá emitir un informe preceptivo dando su opinión sobre aspectos como los accesos al registro, o la gestión y la organización del mismo, y respetando lo afirmado por la Ley.

A estos efectos, **la Comisión de Libertades e Informática propone la siguiente redacción:**

> **Art**. **7. 5.** Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras. Ninguna entidad o persona física privada podrá acceder a estos datos, salvo que exista previa autorización judicial .

9.- DATOS DE LOS MENORES.

La Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) no hace ninguna referencia específica a la protección de los datos de carácter personal del menor ni establece ningún tipo de disposición especial con respecto a los mismos, y esta falta de previsión legislativa ha provocado, que la Agencia Española de Protección de Datos (AEPD) haya concluido en su Memoria 2000 lo siguiente:

"*A nuestro juicio, con carácter general, deben diferenciarse dos supuestos básicos, el primero referido a los mayores de 14 años, a los que la Ley atribuye capacidad para la realización de determinados negocios jurídicos, y el consentimiento que pudieran dar los menores de dicha edad*"

Respecto de los mayores de catorce años, debe recordarse en primer término, que el artículo 162.1º del Código Civil exceptúa de la representación legal del titular de la patria potestad a "*los actos referidos a derechos de la personalidad u otros que el hijo, de acuerdo con las leyes y con sus condiciones de madurez, pueda realizar por sí mismo"*. Según esto, la AEPD, ha considerado que *el menor en este caso, tiene condiciones suficientes de madurez para prestar su consentimiento al tratamiento de los datos*, citando como ejemplo además la capacidad para testar (con la única excepción del testamento ológrafo) prevista en el artículo 662.1 del Código Civil para los mayores de catorce años.

Citamos además, *y en lo referente a la prestación del consentimiento para la cesión, que, el artículo 4.3 de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica*

del Menor, "considera intromisión ilegítima en el derecho al honor, a la intimidad personal y familiar y a la propia imagen del menor, cualquier utilización de su imagen o su nombre en los medios de comunicación que pueda implicar menoscabo de su honra o reputación, o que sea contraria a sus intereses incluso si consta el consentimiento del menor o de sus representantes legales".

Por su parte, 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, establece en su art. 3.1 que "*El consentimiento de los menores e incapaces deberá prestarse por ellos mismos si sus condiciones de madurez lo permiten, de acuerdo con la legislación civil*".

Volviendo al informe jurídico de la AEPD, termina ésta concluyendo que *"En consecuencia, a tenor de las normas referidas, cabe considerar que los mayores de catorce años disponen de las condiciones de madurez precisas para consentir, por sí mismo, el tratamiento automatizado de sus datos de carácter personal.*

Respecto de los restantes menores de edad, no puede ofrecerse una solución claramente favorable a la posibilidad de que por los mismos pueda prestarse el consentimiento al tratamiento, por lo que la referencia deberá buscarse en el artículo 162 1º del Código Civil, tomando en cuenta, fundamentalmente, sus condiciones de madurez.

En consecuencia, a la vista de lo anteriormente señalado, será necesario recabar el consentimiento de los menores para la recogida de sus datos, con expresa información de la totalidad de los extremos contenidos en el artículo 5.1 de la Ley, recabándose, en caso de menores de catorce años cuyas condiciones de madurez no garanticen la plena comprensión por los mismos del consentimiento prestado, el consentimiento de sus representantes legales."

A estos efectos, **la Comisión de Libertades e Informática propone su introducción a través de la siguiente redacción:**

Artículo 7 bis. Datos de menores.

1. Los datos de carácter personal de los menores, no serán recabados sin su consentimiento expreso e informado sobre la totalidad de los extremos contenidos en el artículo 5 de esta Ley, en cualquier caso, los datos especialmente protegidos sólo podrán ser recabados o tratados cuando así lo disponga una ley.

Cuando sean menores de catorce años o sus condiciones de madurez no garanticen la plena comprensión de la información que se les facilita, el consentimiento habrá de ser prestado por sus representantes legales."

2. En cualquier caso, los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores, y con el conocimiento de éstos, los derechos de acceso, rectificación, cancelación, oposición o

cualesquiera otros que pudieran corresponderles en el contexto de la presente Ley.

3. El tratamiento de los datos de carácter personal de los menores, deberá realizarse con las medidas de confidencialidad suficientes y necesarias para evitar abusos en su manipulación.

10.- DATOS DE SALUD.

El artículo 8 de la LOPD, que desarrolla los datos de salud, datos sensibles, debe ser más claro y específico, recogiendo lo que en el articulado de la LOPD se refiere a ellos y limitando las posibles injerencias de terceros ajenos que no necesitan conocerlos para cumplir con sus funciones laborales, bien en el ámbito sanitario o fuera de él. Actualmente, se establece que:

> **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 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 la legislación estatal o autonómica sobre sanidad.

Este artículo se completa con lo expuesto en el artículo 7.6, que hace referencia tanto a los datos de salud, como a los de ideología, afiliación sindical, religión y creencias, permitiendo su conocimiento cuando dicho *tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto*. Pues bien, la gestión de los servicios sanitarios debe distinguirse como labor administrativa de la labor que necesariamente realiza el personal sanitario, y por ello descartar como necesario para una correcta realización de estas gestiones administrativas el conocer los datos de salud de un paciente y huelga decir nada sobre los datos de ideología, afiliación sindical, religión y creencias.

En cuanto al tratamiento de estos datos, (ya sólo consideramos los de salud) necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento, no puede dejarse a criterio y arbitrio total del personal sanitario, sino que en estos casos extremos debe exigirse un control mayor en respeto a la legislación vigente en esta materia, por lo que se propone sobre este supuesto el que *no sea posible recabar el consentimiento de sus representantes legales,* la necesidad de su *puesta en conocimiento del Ministerio Fiscal o la Autoridad Judicial.* Y todo ello, esto en respeto a:

- la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, (artículos 4 a 11),
- las disposiciones del Código Civil sobre incapacidad (artículos 199 y siguientes),
- el Convenio para la protección de los Derechos Humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina Oviedo, España, el 4 de abril de 1997 (Artículo 6),
- la Declaración de Helsinki de la Asociación Médica Mundial sobre Principios éticos para las investigaciones médicas en seres humanos, Adoptada por la 18ª Asamblea Médica Mundial Helsinki, Finlandia, Junio 1964 y enmendada por posteriores asambleas mundiales, la última, la 52ª Asamblea General Edimburgo, Escocia, Octubre 2000, en sus principios básicos para toda investigación médica (números 24, 24 y 26)
- la (artículo 6.3) Recomendación n. R (97) 5, de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados miembros sobre Protección de Datos Médicos.
- El Convenio 108 del Consejo de Europa de protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

A ésta argumentación, cabe añadir que "datos médicos", datos de especial protección, no son sólo los datos médicos estrictamente, si no que también se deben encuadrar en este término los de datos de otras especialidades que podrían no considerarse incluidas si nos ceñimos a la expresión "datos médicos" (por ejemplo, datos de podología, ópticos, los de enfermería ...etc.), por lo que se propone utilizar la expresión "datos de salud" y "diagnóstico de salud".

A estos efectos, **la Comisión de Libertades e Informática propone la siguiente redacción** para su primer apartado:

> **Artículo 8. Datos relativos a la salud**
>
> 1. (se reubica en este punto lo dispuesto en el actual art. 7.6) No obstante lo dispuesto en el artículo 7, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren el apartado 3 de dicho artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico de salud, la prestación de asistencia sanitaria o tratamientos de salud, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. Cuando dicho tratamiento no requiera esencialmente la identidad de las personas y en todo caso cuando se trate de un tratamiento de datos que sea necesario para la gestión de los servicios sanitarios deberá efectuarse la previa disociación de los mismos.
>
> También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando sea necesario para salvaguardar el interés vital del afectado, o de otra persona, en el supuesto de que esté física o

jurídicamente incapacitado para dar su consentimiento y no sea posible recabar el consentimiento de sus representantes legales sin perjuicio, en todo caso, de su posterior e inmediata puesta en conocimiento del Ministerio Fiscal o la Autoridad Judicial.

Datos Genéticos:

La Recomendación (97) 5 del Comité de Ministros del Consejo de Europa, relativa a la protección de datos médicos, a pesar de que define la expresión *"dato médico" como todos los datos de carácter personal relativos a la salud de una persona, añadiendo que dicha expresión afecta igualmente a los datos manifiesta y estrechamente relacionados con la salud, así como con las informaciones genéticas*, la inclusión de un inciso específico sobre este tipo de datos, en el artículo relativo a los datos de salud, se hace necesaria por cuanto esta misma recomendación, la recoge estableciendo específicamente que:

4.7. Los datos genéticos recogidos y procesados para el tratamiento preventivo, el diagnóstico o el tratamiento del afectado o para investigación científica sólo deben emplearse con esos fines o para permitir al afectado tomar una decisión libre e informada en estas materias.

4.8. El procesamiento de datos genéticos con fines judiciales o de investigación criminal debe ser objeto de una ley específica que ofrezca medidas de salvaguardia adecuadas.

Los datos sólo deben emplearse para establecer si hay un eslabón genético en el conjunto de pruebas aportadas, para prevenir un peligro real o para reprimir un delito específico. En ningún caso deben emplearse para determinar otras características que pueden ser establecidas genéticamente.

4.9. La recogida y procesamiento de datos genéticos con cualquier otro fin distinto de los previstos en los Principios 4.7 y 4.8 sólo debe permitirse, en principio, por razones de salud y en particular para evitar un serio perjuicio a la salud del afectado o de terceros.

Sin embargo, puede permitirse la recogida y procesamiento de datos genéticos en orden a predecir enfermedades en casos en que exista un interés superior y bajo la sujeción a las medidas de salvaguardia definidas por la ley.

Se recomienda en sus considerandos, que los gobiernos de los Estados miembros "*den pasos para asegurar que los principios contenidos en el apéndice a esta recomendación se reflejen en sus leyes y en la práctica"*, lo que supone, a la luz de esta previsión, la necesidad de una Ley específica y orgánica por cuanto desarrolla facetas del contenido esencial de un derecho fundamental (artículo 53 CE) en relación con los datos genéticos. Se añade a esto, y a juicio de la AEPD, en el informe sobre Tratamiento de datos genéticos para la localización de personas desaparecidas o en investigación criminal - Año 2000, que **"***no siendo posible la conservación de los datos*

para otros fines (de aquellos para lo que fueron recabados) *y mucho menos para elaborar perfiles genéticos de la población (la denominada codificación genética) o mantener bancos de ADN obtenidos sin consentimiento del afectado para la investigación de futuras conductas criminales. A nuestro juicio, esta conservación sólo sería posible en caso de que una norma con rango de Ley así lo permitiese (ex artículo 7.3 de la Ley Orgánica 15/1999)".*

A estos efectos, **la Comisión de Libertades e Informática propone su introducción a través de la siguiente redacción:**

Art. 8. 3. El tratamiento de los datos de carácter personal obtenidos del análisis de material genético, sólo podrá realizarse previa habilitación legal, con el consentimiento expreso, escrito e informado del interesado y, en cualquier caso, exclusivamente para fines de salud o de investigación científica, por razones de salud - en particular para evitar un serio perjuicio a la salud del afectado o de terceros, o permitir al afectado tomar una decisión libre e informada en estas materias- y para fines judiciales o de investigación criminal en la prevención de un peligro real o un delito concreto.

11.- DELEGADO DE PROTECCIÓN DE DATOS.

El artículo 18.2 de la Directiva 95/46/CE introduce la figura del Delegado de Protección de Datos, como refuerzo a las posibilidades que ofrece para la simplificación o la omisión de la notificación. En España, no se han previsto estas opciones en consonancia con el espíritu garantista de nuestra Ley , pero igualmente, esta figura puede ayudar al cumplimiento efectivo de sus preceptos, de la forma que exponemos.

El Delegado de Protección de Datos, que no debe confundirse en el caso de la legislación española por la figura contemplada en el artículo 12 LOPD que habla de "encargado del tratamiento" y que cubre la realidad de la subcontratación, tiene encomendado por la Directiva el velar por la aplicación de la normativa de protección de datos en el ámbito de la empresa, y en su caso de las Administraciones públicas, sobre todos los tipos de tratamientos de datos de carácter personal que ésta pueda realizar. El espíritu de la disposición consiste en acercar la normativa de protección de datos a la empresa y adaptarse a la misma, con el fin de incrementar su efectivo cumplimiento y con ello la protección de los derechos de los afectados.

El Delegado de Protección de Datos puede ser considerado como una "especie" de autoridad de control implantada a nivel empresarial o de Administración Pública. Por este motivo, tiene que reunir las mismas características que la Autoridades de Control, es decir, disponer de las competencias necesarias para el desempeño de su función y ser independiente dentro de la empresa:

- conocimiento en la materia
- capacidad inspectora
- independencia, no debe ser sometido a la jerarquía empresarial y gozar de un poder de actuación autónomo (poderes de investigación, poderes de intervención).
- capacidad para dictar recomendaciones vinculantes.

- sujeto al secreto profesional.
- en comunicación directa con la AEPD, debiendo ésta destinar recursos específicos para asegurar la fluidez del diálogo y la efectiva asimilación de los problemas planteados. Esto atiende a la necesidad de un conocimiento en profundidad de la realidad empresarial que puede escapar a la AEPD.

Sistema planteado a la luz del estudio del Derecho comparado:

Los países que han implantado esta figura han optado bien por un sistema obligatorio, como Alemania, donde cada empresa de más de 4 empleados está obligada por ley a dotarse de un Delegado de protección de datos, bien por un sistema facultativo, como en Holanda, Suecia y Francia, si bien ésta última se ha limitado a contemplar la figura del Delegado de Protección de Datos como condición para la exoneración de la declaración de ficheros a la autoridad de control.

Atendiendo a criterios económicos, preconizamos un sistema mixto que obligaría, por ley, a la Administración y las grandes empresas (más de 250 empleados) a dotarse de un Delegado de Protección de Datos, dejando la opción a las demás empresas y organizaciones.

A estos efectos, **la Comisión de Libertades e Informática propone su introducción a través de la siguiente redacción:**

Artículo 10. bis. El Delegado de Protección de Datos.

1. El Delegado de Protección de Datos velará por el cumplimiento de lo dispuesto en la presente Ley y en su normativa de desarrollo en el seno de las entidades que traten datos de carácter personal. La designación de un Delegado de Protección de Datos será obligatoria para las entidades que empleen más de 250 personas y en las Administraciones Públicas con respeto en todo caso a su autonomía competencial.

2. El Delegado de Protección de Datos deberá reunir los requisitos de independencia y capacidad necesarios al buen desempeño de su cargo. Reglamentariamente se desarrollará su nombramiento, naturaleza, ámbito de actuación y condiciones del ejercicio de sus competencias. En todo caso:

a) Si el Delegado de Protección de Datos forma parte del ámbito de organización y dirección de la entidad, se garantizará su independencia dentro de la misma, debiendo únicamente rendir cuentas ante su máximo responsable, pudiendo inspeccionar y dictar órdenes y/o recomendaciones en el ámbito propio de sus competencias bajo sanción de corrección interna, sin perjuicio de las responsabilidades civiles, penales o administrativas que puedan derivar de dicho incumplimiento.

b) Deberá evitarse cualquier conflicto de intereses que pueda menoscabar la garantía de independencia que debe reunir el Delegado de

Protección de Datos. Los conflictos de intereses se valorarán atendiendo a la relación preexistente entre el Director de la entidad y el Delegado y a todas las demás circunstancias profesionales que rodeen al Delegado y puedan influir en su independencia.

c) Deberá poseer conocimientos informáticos consolidados y conocimientos jurídicos que le habiliten para el desempeño de su función.

3. La Agencia Española de Protección de Datos o, en su caso, el Organismo competente de cada Comunidad Autónoma habilitarán un canal de comunicación directo con los Delegados de Protección de Datos con el fin de coadyuvar al eficaz desempeño de su función y de recibir las aportaciones prácticas de los mismos en materia de protección de datos.

***Conexión.:** D.A. 10ª

12.- DERECHOS DE LAS PERSONAS: artículos 15.2 y 16.1.

Los artículos 13 a 19, recogen los derechos de las personas en lo que respecta a los tratamientos sobre sus datos de carácter personal, en concreto, en los artículos 15 y 16, se recogen los derechos de acceso, rectificación y cancelación. Se quiere hacer mención especial de distintos párrafos de estos artículos:

Artículo 15. Derecho de acceso.

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

Artículo 16. Derecho de rectificación y cancelación.

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

Esta redacción, carece de previsión alguna que permita al interesado conocer efectivamente que sus derechos se han ejercitado, y que el responsable del fichero a accedido a su petición en el plazo establecido. Cuando tal situación se da, conlleva indefensión para el ciudadano ante el ejercicio de sus propios derechos, pues le resultaría difícil de otro modo tener constancia de cómo se tratan sus datos personales y en qué situación están, e incluso sobre la posibilidad, en su caso, de plantear la correspondiente denuncia.

A estos efectos, **la Comisión de Libertades e Informática propone la siguiente redacción:**

> **Art. 15. 2.** La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización o audición, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, o cualquier otro medio semejante, siempre que el interesado así lo solicite dicha información deberá serle entregada o remitida por cualquiera de estos últimos medios en el plazo de 10 días.

Se añade que, apareciendo en otros artículos de la LOPD consagrado el derecho de oposición, no se incluye expresamente junto con éstos otros de igual naturaleza. No es lógica la exclusión de éste derecho en el artículo que respalda el ejercicio de los principales derechos del titular de datos de carácter personal, teniendo en cuenta que los artículos siguientes (17, 18, 20 ....etc.) así lo establecen y la Sentencia 292/00 así lo ratifica como uno más de éstos derechos (FJ 7º). Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos de carácter personal y con qué fin, y el derecho a poder oponerse a esa posesión y uso. Por ello, y sin más argumentación, lo incluimos citado, a la espera de su regulación por el Reglamento de desarrollo de la Ley.

A estos efectos, **la Comisión de Libertades e Informática propone la siguiente redacción:**

> **Art. 16. 1.** El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación, cancelación u oposición al tratamiento de los datos de carácter personal del interesado en el plazo de diez días, notificando al mismo mediante cualquier medio del que quede constancia documental de su recepción, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.
>
> **Art. 16. 4.** Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación, oposición o cancelación efectuada a quienes se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la rectificación o cancelación

Conexión: art. 23

13.- FUNCIONES DE LA AUTORIDAD DE CONTROL: Medidas Cautelares.

Partiendo de que las autoridades de control son entes de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada, que actúan con independencia de las Administraciones Públicas en el ejercicio de sus funciones y tienen potestad sancionadora, no entendemos cómo no se ha previsto para ellas la

posibilidad de implantar medidas cautelares, provisionales, en aquellos supuestos en que la inspección de razones justificadas para ello.

El artículo 18, es el artículo que establece los principios básicos para la tutela de los derechos de las personas, y nada prevé sobre la posibilidad abierta de adoptar medidas cautelares.

> **Artículo 18. Tutela de los derechos.**
>
> 1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.
>
> 2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación.
>
> 3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses.
>
> 4. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

El Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos rige las funciones de la AEPD, y su artículo 2.2.c sobre el régimen jurídico establece que, en defecto de ésta (y de la LOPD) para el ejercicio de sus funciones públicas, rigen 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. La Sección V, sobre la Inspección de Datos, regula en los artículos 28 y 29 respectivamente las funciones inspectoras e instructoras, pero no hace mención de la posibilidad de implantar medidas cautelares.

Como fundamento de esta mejora en la Ley, de las funciones de la Agencia, debemos acudir a la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, cuyo artículo (Medidas de carácter provisional) 136, establece que *“Cuando así esté previsto en las normas que regulen los procedimientos sancionadores, se podrá proceder mediante acuerdo motivado a la adopción de medidas de carácter provisional que aseguren la eficacia de la resolución final que pudiera recaer.”*

Si bien es cierto que el artículo 49 ya prevé una forma de medida provisional, *"Potestad de inmovilización de ficheros"*, el retraso en la adopción de las medidas correctoras o de salvaguardia de los derechos individuales podría producir efectos irreparables, y consideramos esta previsión sumamente restrictiva y que olvida otras posibilidades que podrían darse en el transcurso del tratamiento de datos de carácter personal. Pongamos por caso el avance de las Tecnologías, en sistemas de rastreo, lo

que desde Estados Unidos nos llega como RFID (Radio Frecuency Identification), Este nuevo sistema consta de una antena y un chip que almacena un Código Electrónico de Producto (EPC, Individual Item Level Unique Reference Number) de 64 ó 96 bits y es accesible por radio frecuencia a través de su antena, y permite posibilidades de rastreo aún inéditas sobre datos de carácter personal de aquel que lo lleve implantado, bien en un producto que acaba de comprar, bien en una tarjeta de crédito, DNI o su propio cuerpo. Pues bien, esto requeriría en un supuesto de potencial infracción el aviso inmediato a las personas que puedan estar siendo rastreadas y no conste que han consentido para ello. Este es en concreto un problema que aún va más allá de esta argumentación, y que requeriría su propio espacio legal.

A estos efectos, **la Comisión de Libertades e Informática propone su introducción a través de la siguiente redacción:**

> **Art. 18. 5.** Si en el curso de una inspección, se observara que determinados tratamientos de datos de carácter personal, pudieran producir graves perjuicios a sus titulares, las autoridades de control podrán acordar la implantación de medidas cautelares, acordes al mandato de la presente Ley.

*** Conexión:** art. 49.1

14.- DERECHO A INDEMNIZACIÓN.

Respecto del derecho a la reparación de los daños y perjuicios, el artículo 19 establece que:

Artículo 19. Derecho a indemnización

> 1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados

Y el artículo 23 de la Directiva 95/46/C establece que:

"1. Los Estados miembros dispondrán que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la presente Directiva, tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido.

2. El Responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño."

Con fundamento en todo ello, los procedimientos de reparación del daño sufrido en materia de protección de datos de carácter personal deben acomodarse de institutos

de garantía previstos para la protección de otros derechos que poco o nada tienen que ver con las características del derecho en cuestión. Si bien esta situación podía sostenerse en base al artículo 18.4 CE, el hecho de que el Tribunal Constitucional haya reconocido el derecho fundamental a la protección de datos como derecho fundamental autónomo de los derechos reconocidos en el artículo 18.1 CE justifica que dicho derecho pueda gozar de procedimientos independientes y adaptados a su naturaleza. Por ello, se exhorta al legislador a introducir procedimientos judiciales adaptados al derecho fundamental a la protección de datos, diferenciados de los derechos protegidos por el artículo 18.1 CE.

A estos efectos, **la Comisión de Libertades e Informática propone su introducción a través de la siguiente redacción:**

Art. 19.1. Derecho a indemnización

1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados. Para la defensa del derecho a la protección de datos el afectado podrá acudir al procedimiento establecido para la protección de los derechos fundamentales.

15.- CONTROL PREVIO PARA CREACIÓN DE FICHEROS PÚBLICOS.

El artículo 20, establece lo siguiente:

Artículo 20. Creación, modificación o supresión.

1. La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el "Boletín Oficial del Estado" o Diario Oficial correspondiente.

Esta previsión es escasa en lo que se refiere al marco establecido para el tratamiento de estos ficheros, pues es necesario, que a parte de su creación, se refuercen las competencias de inspección de las autoridades de control, de forma que pueda tomar las medidas oportunas en el caso de que apareciesen indicios o sospechas de que se puede lesionar el derecho fundamental en el tratamiento que se haga de estos ficheros.

La Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal y a la libre circulación de estos datos, establece una previsión similar en su artículo 20, y de él se extrae la necesidad de un control a priori más efectivo, tanto por parte de la AEPD como por parte de los Organismos de Control Autonómicos, y todo ello debido a que es la Ley 30/92, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento

Administrativo Común, la que establece en su Artículo 4.1 sobre los *principios de las relaciones entre las Administraciones Públicas, establece que las Administraciones públicas actúan y se relacionan de acuerdo con el principio de lealtad institucional y, en consecuencia, deberán:*

> *- Facilitar a las otras Administraciones la información que precisen sobre la actividad que desarrollen en el ejercicio de sus propias competencias.*
>
> *- Prestar, en el ámbito propio, la cooperación y asistencia activas que las otras Administraciones pudieran recabar para el eficaz ejercicio de sus competencias.*

El art.18.2 señala que *respecto de la coordinación de competencias, las normas y actos dictados por los órganos de las Administraciones Públicas en el ejercicio de su propia competencia deberán ser observadas por el resto de los órganos administrativos, aunque no dependan jerárquicamente entre sí o pertenezcan a otra Administración.*

Completando esto con la facultad propia de una autoridad de control en esta materia, de dictar informes, instrucciones y recomendaciones, limitaría las posibilidades de vulneración de los principios de esta Ley, bien por desconocimiento de los que redactan las normas de creación de ficheros, bien por pura negligencia. No olvidemos que es el criterio interpretativo de la Autoridad de Control, el que debe primar en ausencia de un criterio judicial (criterio lento y difícil de conseguir), aunque por supuesto, nunca lo sustituirá en su caso.

A estos efectos, **la Comisión de Libertades e Informática propone su introducción a través de la siguiente redacción:**

> **Art. 20. 1.** La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el "Boletín Oficial del Estado" o Diario Oficial correspondiente.
>
> Las autoridades de control, podrán realizar las comprobaciones previas que sean necesarias sobre los tratamientos que puedan suponer riesgos específicos para los derechos y libertades de los interesados velando en esos casos por que sean examinados antes del comienzo del tratamiento. Dichas comprobaciones previas se acordarán obligatoriamente de oficio cuando hubieran tenido indicios suficientes de dichos riesgos o cuando hayan recibido notificación al respecto del responsable del tratamiento, por el encargado de la protección de datos o, en su caso, por el Delegado de Protección de Datos, quienes, en caso de duda, deberán consultar a las autoridades de control.

16.- GUÍAS DE SERVICIOS DE TELECOMUNICACIONES.

El artículo 28, se refiere a aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación, y en concreto a los contenidos en las guías de teléfonos.

> **Artículo 28. Datos incluidos en las fuentes de acceso público.**
>
> 4. Los datos que figuren en las guías de servicios de telecomunicaciones disponibles al público se regirán por su normativa específica.

La Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, establece lo siguiente:

Artículo 22. Concepto y ámbito de aplicación.

1. Se entiende por servicio universal el conjunto definido de servicios cuya prestación se garantiza para todos los usuarios finales con independencia de su localización geográfica, con una calidad determinada y a un precio asequible.

Bajo el mencionado concepto de servicio universal se deberá garantizar, en los términos y condiciones que reglamentariamente se determinen por el Gobierno:

b) Que se ponga a disposición de los abonados al servicio telefónico disponible al público una guía general de números de abonados, ya sea impresa o electrónica, o ambas, y se actualice, como mínimo, una vez al año. Asimismo, que se ponga a disposición de todos los usuarios finales de dicho servicio, incluidos los usuarios de teléfonos públicos de pago, al menos un servicio de información general sobre números de abonados. Todos los abonados al servicio telefónico disponible al público tendrán derecho a figurar en la mencionada guía general, sin perjuicio, en todo caso, del respeto a las normas que regulen la protección de los datos personales y el derecho a la intimidad.

Este artículo remite en materia de protección de datos, a la normativa específica, y si acudimos a ella (art.28.4 LOPD) tenemos el mismo problema, nos remite a la normativa específica, convirtiéndose en un círculo legislativo vacío e incoherente.

Además, el artículo 28 de la Ley Orgánica 15/1999 regula el tratamiento y las normas de protección de los datos incluidos en las fuentes de acceso público. Estas fuentes de acceso público son definidas en el artículo 3 de la misma Ley, como aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencias que, en su caso, el abono de una contraprestación. La propia norma enumera algunas de estas fuentes, como el censo promocional, los repertorios telefónicos, las listas de personas pertenecientes a grupos profesionales, los Diarios y Boletines oficiales y los medios de comunicación.

La regulación de este tipo de fuentes es esencial para garantizar, en un contexto en que los avances técnicos y los medios para realizar tratamientos de la información se incrementan en índices de progresión inimaginables, el derecho a la

autodeterminación informativa recogido en el artículo 18.4 de la Constitución. Ahora, podemos decir que está casi al alcance de cualquiera la utilización de técnicas informáticas con una extraordinaria capacidad de invasión de la intimidad, mediante el tratamiento de los datos de carácter personal incluidos en las fuentes de acceso público existentes.

A estos efectos, **la Comisión de Libertades e Informática propone la supresión del art. 28.4.**

17.- LISTAS DE MOROSOS.

La Ley Orgánica 15/1999 contiene entre sus principios generales, el principio de calidad de los datos, que, ligado al principio de proporcionalidad de los datos, exige que los mismos sean adecuados a la finalidad que motiva su recogida, pero en relación con la prestación de servicios de información sobre solvencia patrimonial y crédito, la LOPD es escasa en sus precisiones:

> **Artículo 29. Prestación de servicios de información sobre solvencia patrimonial y crédito.**
>
> 3. En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable del tratamiento 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 de la persona o entidad a quien se hayan revelado los datos.
>
> 4. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos.

La recogida y tratamiento de datos de carácter personal debe efectuarse desde su subordinación a los principios de calidad de los datos y de proporcionalidad que establece la Ley (Artículo 4) y además tener en cuenta que constituye infracción de carácter grave, de acuerdo con lo dispuesto en el artículo 44.3.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”.

Doctrina judicial.

Sentencia de la Sala de lo Contencioso Administrativo de la Audiencia Nacional, de 9 de marzo de 2001.

'Uno de los principios que inspira la legislación sobre tratamiento automatizado de datos de carácter personal es el de calidad de datos. Este principio implica, entre otras

cosas, que los datos sean necesarios y pertinentes para la finalidad para la cal hubieran sido recabados o registrados (art. 4.5 de la LO 5/1992) y que sean exactos y completos art. 4.4 de la LO 5/1992. Por lo tanto, si los datos han dejado de ser necesarios para los fines para los cuales fueron recabados o registrados o resultan inexactos, se debe proceder (..) a su cancelación, sin necesidad de solicitud del afectado. Y así se infiere del propio tenor literal de los artículos 4.4 y 4.5 de la LO 5/1992, que utiliza la expresión imperativa 'serán cancelados' y sin condicionarla a la existencia de una previa solicitud del afectado. En suma, la norma establece la obligación del responsable del fichero de proceder de oficio y con la debida diligencia a cancelar los datos inexactos o que han dejado de ser necesarios para la finalidad del fichero y sin necesidad de solicitud previa del afectado'.

Sentencia de la Sección Novena de la Sala de lo Contencioso Administrativo del Tribunal Superior de Justicia de Madrid, de 5 de noviembre de 1998.

'Sin embargo, aunque (...) no hubo (...) una intención de dañar ni enriquecimiento injusto (...) los hechos han tenido una doble perturbación para la perjudicada: (...) imputarle una deuda inexistente (.....) lo más grave fue su inclusión en un Registro Informático de Morosos y además sin conocimiento de la perjudicada (....) y de esa inclusión indebida en el Registro de Morosos no eran responsables los que llevan el Registro sino los que suministraron el dato'.

Sentencia de la Sección Octava de la Sala de lo Contencioso Administrativo del Tribunal Superior de Justicia de Madrid, de 18 de octubre de 2000.

'(....) para incluir en un fichero de solvencia patrimonial el dato relativo a una deuda, ésta, además de cierta, vencida y exigible, ha de haber resultado efectivamente impagada (....) debiendo además, el acreedor (como requisito previo a la inclusión del dato en un fichero de estas características) proceder en la forma más arriba descrita y cuya finalidad no es otra que garantizar la exactitud de los datos que se pretende incluir'.

Sentencia de la Audiencia Nacional de 10-05-2002. Sala de lo contencioso-administrativo. Sección Primera. Conservación de datos de obligaciones satisfechas en ficheros de solvencia patrimonial y crédito. Saldo cero.

“la inclusión de datos en este tipo de fichero comporta una serie de consecuencias desfavorables al afectado, por lo que la simple constancia de "saldo 0", es una inexactitud, pues para que exista deuda es necesario que la cuantía sea superior a cero. Lo contrario supone no reflejar una situación actual del deudor, que claramente le perjudica”

“quien tuvo deudas, y ya no las tiene, no pueda ser considerado como un deudor con saldo cero, es decir, no hay deudores al corriente en sus pagos o con deudas canceladas.

La AEPD, también recoge estos argumentos en su Memoria 2001 página, 237: *La situación de "saldo 0" y diferentes resoluciones por infracción del artículo 29.4 en relación con el 4.3 de la LOPD.*

A estos efectos, **la Comisión de Libertades e Informática propone la siguiente redacción:**

> **Art. 29.3.** En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos que están siendo tratados en este sentido, la entidad que los ha facilitado, los motivos de su inclusión en este tipo de tratamiento, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses, y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.
>
> **Art. 29.4** Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos. En todo caso, se prohíbe el tratamiento de datos de deudas canceladas o ficheros de "saldo cero".

18.- "LISTA ROBINSON".

La redacción del artículo 30 de la LOPD respondió en su momento a la necesidad de enmarcar la actividad de publicidad y de prospección comercial, a limitar las fuentes de las cuales podían extraerse los datos de carácter personal. El artículo 3 j) LOPD vino a reforzar el marco regulador al definir de forma estricta el concepto de fuentes accesibles al público y de esta forma limitar las fuentes de datos de carácter personal que se pudieran recabar sin consentimiento del interesado. Además de establecer un mecanismo que permitiera a los interesados oponerse al tratamiento de forma sencilla y gratuita.

> **Artículo 30. Tratamientos con fines de publicidad y de prospección comercial.**
>
> 1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.

Sin embargo, considerando el elevado número de empresas que se dedican a dichas actividades, el ejercicio del derecho de oposición se revela una falacia por el problema que supone al usuario tener que dirigirse por carta a cada una de las empresas que le

envíen publicidad con el fin de que dejen de remitirle publicidad de forma indiscriminada. Sobre todo si tomamos en cuenta que el derecho de oposición, a efectos de pruebas y por el perjuicio que supone a la empresa, tiene que ser ejercido mediante escrito, con el fin de desalentar a los usuarios que se ven obligados a gastar tiempo y dinero para poder ejercer su derecho a "que le dejen en paz".

Frente a esta situación, la Federación de Comercio Electrónico y Marketing Directo (en adelante FECEMD) inscribió en el Registro de la AEPD un Código de Conducta enfocado a la creación de una "lista Robinson", que permite a los afectados manifestar de forma gratuita, a través de Internet, sus preferencias en materia de publicidad, existiendo en todo caso la posibilidad de manifestarse en contra de la recepción de cualquier tipo de publicidad. Las empresas adheridas al código de conducta se comprometen, entre otras obligaciones, a consultar la lista previamente a cualquier envío publicitario eliminando de la campaña (y no del fichero) las personas que han manifestado su voluntad de no recibir este tipo de publicidad. Esta iniciativa es loable, si bien limitada a las empresas que se han adherido de forma voluntaria.

A estos efectos, es de recordar que el Considerando 26 de la Directiva 2002/58/CE, reitera la obligación de recabar el consentimiento previo e informado del interesado, disponiendo que *"Los datos relativos a los abonados que son tratados en las redes de comunicaciones electrónicas para el establecimiento de conexiones y la transmisión de información contienen información sobre la vida privada de las personas físicas, y afectan al derecho de éstas al respeto de su correspondencia, o se refieren a los intereses legítimos de las personas jurídicas. Dichos datos sólo deben poder almacenarse en la medida en que resulten necesarios para la prestación del servicio, para fines de facturación y para los pagos de interconexión, y durante un tiempo limitado. Cualquier otro tratamiento de dichos datos que el proveedor de servicios de comunicaciones electrónicas disponibles al público pretenda llevar a cabo para la comercialización de servicios de comunicaciones electrónicas o para la prestación de servicios de valor añadido sólo puede permitirse si el abonado ha manifestado su consentimiento fundado en una información plena y exacta facilitada por el proveedor de servicios de comunicaciones electrónicas disponibles al público acerca del tipo de tratamiento que pretende llevar a cabo y sobre el derecho del abonado a denegar o a retirar su consentimiento a dicho tratamiento. Los datos sobre tráfico utilizados para la comercialización de los servicios de comunicaciones o para la prestación de servicios de valor añadido deben también eliminarse o hacerse anónimos tras la prestación del servicio. Los proveedores de servicios deben mantener siempre informados a los abonados de los tipos de dato que están tratando y de la finalidad y duración del tratamiento".*

Frente a estas insuficiencias detectadas en la LOPD y conscientes de la utilidad de un instrumento como el consentimiento implícito en el tráfico mercantil, proponemos como solución alternativa, para resolver tanto el problema del llamado "buzoneo" como el de la utilización del consentimiento implícito para el tratamiento de los datos con fines distintos a los originarios, en el sector del marketing, con el fin de incrementar la protección reconocida en la LOPD a los individuos, y en particular hacer efectivos los derechos plasmados en la normativa de protección de datos, la creación de una lista Robinson, y generalizar su uso, haciéndolo obligatorio, con el fin de asegurar que toda

empresa que se dedique a actividades de publicidad y de prospección comercial elimine, previamente al envío, los datos de carácter personal de las personas que se hayan manifestado en contra.

De esta forma, proponemos lo siguiente:

1. La creación de una "Lista Robinson" en la que conste, como ahora, las preferencias de los afectados en materia de publicidad.
2. La consulta obligatoria de esta lista por todo responsable de tratamiento que quiera realizar una campaña de marketing directo. La lista utilizada por el responsable del tratamiento deberá tener una antigüedad máxima de 15 días.
3. La cancelación sistemática de los datos de carácter personal de las personas que figuran en dicha lista siempre y cuando se hayan opuesto a la recepción de este tipo de publicidad. Esta cancelación se extenderá a los ficheros mantenidos por los responsables de tratamiento y que responde a una misma finalidad.
4. El mantenimiento de dicha lista podría recaer en la FECEMD en las condiciones actuales, excluyendo una adhesión obligatoria al Código de Conducta mantenido por dicha federación, siendo la naturaleza de la adhesión a dichos Códigos esencialmente voluntaria.
5. La introducción en la LOPD de una sanción por el envío de publicidad a las personas que se han manifestado en contra.

Esta regulación se ve completada con lo dispuesto en la LSSI para las comunicaciones comerciales a través de medios electrónicos, pero que creemos es perfectamente aplicable en este punto, en el añadido de la palabra "publicidad" para las comunicaciones comerciales.

A estos efectos, **la Comisión de Libertades e Informática propone la siguiente redacción:**

> **Art. 30.1** Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento. Al objeto de regular la utilización de tales datos para los fines a los que se refiere el párrafo anterior, se creará una lista que indique las preferencias de cada individuo en materia de publicidad directa y en la que existirá un apartado en el que constará la relación de personas que se hayan manifestado en contra de la recepción de cualquier tipo de publicidad.
>
> La Agencia Española de Protección de Datos podrá encomendar la creación y mantenimiento de dicha lista a organismos privados, siempre y cuando no se vulneren los derechos y libertades fundamentales de los individuos. Se desarrollará reglamentariamente las modalidades de funcionamiento de la lista, debiendo en todo caso asegurar la inclusión

de los interesados mediante procedimientos sencillos y gratuitos, en particular a través de Internet o cualquier otro procedimiento semejante.

30. 2. Cuando los datos procedan de fuentes accesibles al público. de conformidad con lo establecido en el párrafo segundo del artículo 5.5 de esta Ley, en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten y expresamente contendrán la palabra "publicidad".

El responsable del fichero deberá facilitar un sencillo sistema de acceso a dicha información, a través de medios de comunicación seguros y de forma gratuita, cuando por las características técnicas de la comunicación, no sea posible cumplir directa y completamente con las exigencias del artículo 5.5.

19.- CENSO PROMOCIONAL.

El Censo Promocional designa al fichero elaborado a partir del Censo Electoral, limitado a los datos de empadronamiento, por el Instituto Nacional de Estadística o de los órganos equivalentes de las Comunidades Autónomas, y la LOPD lo recoge en su artículo 30.

Artículo 31. Censo promocional.

1. Quienes pretendan realizar permanente o esporádicamente la actividad de recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial u otras actividades análogas, podrán solicitar del Instituto Nacional de Estadística o de los órganos equivalentes de las Comunidades Autónomas una copia del censo promocional, formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral.

2. El uso de cada lista de censo promocional tendrá un plazo de vigencia de un año. Transcurrido el plazo citado, la lista perderá su carácter de fuente de acceso público.

3. Los procedimientos mediante los que los interesados podrán solicitar no aparecer en el censo promocional se regularán reglamentariamente. Entre estos procedimientos, que serán gratuitos para los interesados, se incluirá el documento de empadronamiento.

Trimestralmente se editará una lista actualizada del censo promocional, excluyendo los nombres y domicilios de los que así lo hayan solicitado.

4. Se podrá exigir una contraprestación por la facilitación de la citada lista en soporte informático.

Esta figura, desconocida de la LORTAD, ha sido introducida por la LOPD, con el fin de regular y enmarcar el uso del Censo Electoral por las empresas de marketing. Este tratamiento, ya declarado ilegítimo por la LORTAD, aparecía de difícil control por la AEPD, considerando el elevado número de sanciones que fueron pronunciando a raíz de la LORTAD. El legislador introdujo esta figura con el fin de prevenir dichos abusos y de la misma forma zanjó la polémica desatada a raíz del artículo 39.3 de la Ley 7/1996, de 15 de enero de ordenación del comercio minorista, que establece que los datos de identidad y de domicilio contenidos en el censo electoral tienen el carácter de datos accesibles al público y por lo tanto son utilizables por las empresas de publicidad directa y venta a distancia, así regulado, tanto la AEPD como la Junta Electoral Central se pronunciaron en contra de tal interpretación, por el carácter ordinario y sectorial de dicha ley que en ningún caso la habilita para modificar leyes con carácter orgánico.

Ahora bien, la LOPD, a través del artículo 30, ha encargado al Instituto Nacional de Estadística y a los órganos equivalentes de las Comunidades Autónomas el desarrollo y mantenimiento del Censo, definiendo sus rasgos básicos (contenido, periodo de vigencia, procedimientos de recogida de los datos, actualización de los datos), y deja para un posterior desarrollo reglamentario el establecimiento de los procedimientos mediante los que los interesados quedarán facultados para no aparecer en el censo promocional. Pero la polémica se ha desatado en torno al último apartado del artículo que habilita dichos organismos a exigir una contraprestación a las empresas que soliciten el Censo Promocional.

Nos encontramos ante una situación que ya había sido denunciada en la Sentencia del Tribunal Constitucional alemán en el año 1983, del censo, y que puso la primera piedra del reconocimiento europeo, a nivel constitucional, de un derecho a la autodeterminación informativa. Los ciudadanos se ven obligados, por razones de interés general, a proporcionar una serie de datos relativos a su vida cotidiana, al Estado. Si bien esta finalidad aparece legítima para garantizar una buena administración, en ningún caso esta recogida masiva de datos de carácter personal, de una nación entera, puede ser desviada hacia otros fines, como es el caso del Censo Promocional. Esta habilitación hecha a la Administración vulnera el principio básico y fundamental, recogido en la LOPD, de finalidad del tratamiento que implica que el responsable del tratamiento, en ningún caso, podrá tratar los datos del interesado para fines distintos a los originales, a no ser que cuente con el consentimiento previo del mismo. Más aún cuando el Estado pretende lucrarse con la venta de unos datos que los ciudadanos se ven obligados a facilitarle por las razones antes expuestas. Si bien es cierto que el establecimiento de una contraprestación cumple la función de disuasión de tratamiento de dichos datos, punto de especial trascendencia que deberá ser contemplado en la modificación de la disposición, se deben limitar los supuestos de cesión del Censo Promocional a los responsables del tratamiento, de acuerdo con lo dispuesto en el artículo 11.1 LOPD, que acrediten el cumplimiento de fines directamente relacionados con las funciones legítimas del cesionario.

El 18 de octubre de 2002, el PSOE e IU presentaron cada uno una proposición de ley orgánica ante el Congreso tendente a exigir que se recabe el consentimiento expreso

del interesado. Si bien la proposición de IU se limitaba a introducir modificaciones en la LOPD tendentes por una parte a prohibir el comercio de datos de los ciudadanos por la Administración incluyendo un nuevo apartado en el artículo 11, y en particular en el caso del Censo Promocional, además el consentimiento previo y expreso de los afectados, la proposición del PSOE iba más allá proponiendo una modificación del artículo 3 h) de la LOPD que recoge la definición de "consentimiento" con el fin de incluir una nueva característica: la obligación de que sea en todo caso expreso. Dichas proposiciones de ley no llegaron a ser admitidas y el debate generado alrededor del tema quedó en suspenso, olvidado para la mayoría.

Hoy, dentro del marco de este Informe de propuestas de reforma de la LOPD, ha llegado el momento de retomar este debate, esperando que llegue a buen término. Si bien no nos inclinamos hacia la generalización de la exigencia de que el consentimiento sea expreso mediante las salvaguardas antes expuestas, relativas a la creación de una lista Robinson de consulta obligatoria para los tratamientos con fines de marketing directo, sí abogamos por la supresión del artículo 31 LOPD.

A estos efectos, **la Comisión de Libertades e Informática propone la supresión del art. 31.**

***Conexión**: 3.J), 11.2.bis, 28.1 y D.T. 2ª.

20.- CONSEJO CONSULTIVO.

El actual Consejo Consultivo, presenta graves carencias en cuanto a su operatividad y representación debido a lo numeroso de sus miembros, que serán más conforme se vayan creando las diferentes Agencias de Protección de Datos Autonómicas.

> **Artículo 38. 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 el Senado.
>
> Un representante de la Administración Central, designado por el Gobierno.
>
> 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 cada Comunidad Autónoma que haya creado una agencia de protección de datos en su ámbito territorial, propuesto de acuerdo con el procedimiento que establezca la respectiva Comunidad Autónoma.

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.

El Consejo Consultivo, ha de ser lo que su propio nombre indica, pero consideramos que es una designación ya muy manida, tanto, que a veces hace perder su sentido a la institución que designa. Por ello se propone partir de una denominación más acorde con lo que debe ser su función.

En cuanto a lo numeroso de su composición, la principal propuesta es sobre "el representante de una Comunidad Autónoma", en esta materia y respecto a la Autoridad de control que en ella se haya creado, debe coordinar su actividad con el resto de entes de igual naturaleza, principalmente a través de la estructuración sectorial que debe tener la AEPD, independientemente de lo previsto en el artículo 41 de la Ley. En consecuencia se propone la supresión de los representantes de cada Comunidad Autónoma en el Consejo ya que, si se mantiene, puede derivar en la inoperancia del Consejo. En este sentido, añadir que las consultas y opiniones de este colectivo, habrán de seguirse por un canal más directo e independiente (aunque compatible con sus resultados) de comunicación con la AEPD, y así lo proponemos **reforzando el art. 41.3 LOPD.**

En otro sentido, los sectores más importantes que se ven afectados por la normativa de protección de datos, no tienen su reflejo en un grupo de trabajo que pretende asesorar y acercar a la AEPD a la realidad de la aplicación de los preceptos de la LOPD. Por ello proponemos la inclusión de estos representantes, dándoles voz en los procesos de adopción de criterios interpretativos.

A estos efectos, **la Comisión de Libertades e Informática propone la siguiente redacción:**

Artículo 38. Consejo de Protección de Datos

El Director de la Agencia *Española* de Protección de Datos estará asesorado por un Consejo de Protección de Datos compuesto por los siguientes miembros:

- Un diputado, propuesto por el Congreso de los Diputados.

- Un Senador, propuesto por el Senado.

- Un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente.

- Un representante de la Administración Central, designado por el Gobierno.

- 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 representante de cada Comunidad Autónoma que haya creado una agencia de protección de datos en su ámbito territorial, propuesto de acuerdo con el procedimiento que establezca la respectiva Comunidad Autónoma.~~*)*

-Un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente.

-Un representante de las Organizaciones Sindicales más representativas, seleccionado del modo que se prevea reglamentariamente

-Un representante de las asociaciones más representativas en materia de Protección de Datos de Carácter Personal seleccionado del modo que se prevea reglamentariamente.

-Un representante de las asociaciones más representativas específicamente relacionada con el uso de Internet, seleccionado del modo que se prevea reglamentariamente.

-Un destacado jurista, con demostrada experiencia y conocimientos en el ámbito del derecho a la protección de datos, y elegido a propuesta del Consejo Superior de Universidades.

- Un titulado universitario competente en Informática elegido a propuesta de su corporación profesional..

El funcionamiento del Consejo de Protección de Datos se regirá por las normas reglamentarias que al efecto se establezcan.

*__Conexión:__ art. 36.

> **Art. 41. 3.** El Director de la Agencia de Protección de Datos deberá convocar regularmente a los órganos correspondientes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o 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.

Manteniendo el criterio de colaboración y trasparencia entre Administraciones, creemos necesario aplicarlo a la información que la Agencia transmita a los diferentes poderes del Estado, y que actualmente se recoge en el artículo 37:

> **Art. 37.** Son funciones de la Agencia de Protección de Datos:
> **k)** Redactar una memoria anual y remitirla al Ministerio de Justicia.

por ello, la **CLI propone establecer lo siguiente**:

> **Art. 37. k)** Redactar una memoria anual y remitirla a las Cortes Generales.

21.- SANCIONES.

El sistema de sanciones instaurado por la LOPD en sus artículos 44 y 45 responde a un sistema de responsabilidad objetiva, si bien la graduación de las mismas introduce la noción de culpabilidad, dejando la determinación de la cuantía de la sanción a criterio de la AEPD atendiendo a una serie de baremos tales como la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, los beneficios obtenidos, ...etc., y permite por otra parte, la aplicación de la cuantía correspondiente a la escala de infracción inmediatamente menos grave cuando se aprecie una cualificada disminución de la antijuricidad del hecho o de la culpabilidad del imputado (artículo 45.5 LOPD).

> **Artículo 44. Tipos de infracciones.**
>
> 1. Las infracciones se calificarán como leves, graves o muy graves.
>
> 2. Son infracciones leves:
>
> a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.
>
> b) No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.

c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.

d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley.

e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave

(...)

Artículo 45. Tipo 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 10.000.000 a 50.000.000 de pesetas.

3. Las infracciones muy graves serán sancionadas con multa de 50.000.000 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, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate.

6. En ningún caso podrá imponerse una sanción más grave que la fijada en la Ley para la clase de infracción en la que se integre la que se pretenda sancionar.

7. El Gobierno actualizará periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios.

Lo que proponemos a estos efectos, es, por una parte, agravar dos ilícitos que creemos deben ser reforzados, por los peligros que comporta el hecho de su

incumplimiento. El deber de información y el deber de secreto son pilares básicos para el sistema de protección de datos se carácter personal.

A estos efectos, **la Comisión de Libertades e Informática propone la siguiente introducción en la redacción para el art. 44. 2:**

> m) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción muy grave.
> n) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley.

Y por otra parte, se propone lo que creemos necesario con el fin de aminorar las consecuencias desastrosas y totalmente desproporcionadas con la gravedad del acto, que ha provocado el sistema actual de sanciones, y con el fin de establecer un sistema más justo, consiste en bajar los mínimos fijados por la comisión del acto y dejar un margen de maniobra más amplio en cuanto a la fijación del importe de la sanción que debería realizarse atendiendo a las siguientes circunstancias:

- Naturaleza de los derechos personales afectados
- Volumen de los tratamientos efectuados
- Beneficios obtenidos
- Grado de intencionalidad
- Reincidencia
- Daños y perjuicios causados a las personas interesadas y a terceras personas
- El número de personas afectadas.
- Cualquier otra circunstancia relevante para determinar el grado de antijuricidad y de culpabilidad presentes en la concreta actuación infractora.

En todo caso, la sanción impuesta no deberá en ningún caso exceder del 10% del volumen de negocio mundial de la empresa sancionada, criterios en cualquier caso que deberán ser desarrollados por el legislador en orden a la actual normativa que prevé la imposición de sanciones y los criterios de mínimos y máximos que en ella se puedan prever.

Por la misma justificación que sirvió para la introducción de la minoración de la sanción, se propone el aumento de la misma cuando concurran determinadas causas objetivas que califican la gravedad del hecho o de la conductas del sujeto infractor. Se pretende además de adecuar la sanción a la gravedad y culpabilidad, evitar que al sujeto infractor le salga mas “barato” abonar una sanción que respetar el derecho fundamental.

A estos efectos, **la Comisión de Libertades e Informática propone la siguiente redacción:**

> **Artículo 45. Tipo de sanciones**

1. Las infracciones leves serán sancionadas con multa de 600 euros a 60.000 euros.
2. Las infracciones graves serán sancionadas con multa de 60.000 euros a 300.000 euros.
3. Las infracciones muy graves serán sancionadas con multa de 300.000 euros a 600.000 de euros.

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, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, al número de personas afectadas y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

6. Del mismo modo, si en razón de las circunstancias concurrentes, se apreciara una cualificada intencionalidad en la culpabilidad o en la reincidencia o se apreciara una agravación de la antijuridicidad del hecho o si el beneficio obtenido superase económicamente el máximo de la sanción prevista para la clase de infracción de que se trate, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que siga inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate. Cuando se trate de infracciones muy graves el aumento de la sanción podrá alcanzar hasta el 10% de la facturación anual mundial de la empresa sancionada.

22.- DISPOSICIÓN ADICIONAL SEXTA.

La disposición adicional sexta, establece una previsión especial para la Modificación del artículo 24.3 de la Ley de Ordenación y Supervisión de los Seguros Privados.

Se modifica el artículo 24.3, párrafo 2.º de la Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de los Seguros Privados con la siguiente redacción:

"Las entidades aseguradoras podrán establecer ficheros comunes que contengan datos de carácter personal para la liquidación de siniestros y la colaboración estadístico actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora. La cesión de datos a los citados ficheros no requerirá el consentimiento previo del afectado, pero sí la comunicación al mismo de la posible cesión de sus datos personales a ficheros comunes para los fines señalados con expresa indicación del responsable para que se puedan ejercitar los derechos de acceso, rectificación y cancelación previstos en la Ley.

> También podrán establecerse ficheros comunes cuya finalidad sea prevenir el fraude en el seguro sin que sea necesario el consentimiento del afectado. No obstante, será necesaria en estos casos la comunicación al afectado, en la primera introducción de sus datos, de quién sea el responsable del fichero y de las formas de ejercicio de los derechos de acceso, rectificación y cancelación.
>
> En todo caso, los datos relativos a la salud sólo podrán ser objeto de tratamiento con el consentimiento expreso del afectado."

Como se puede observar, la modificación producida por esta Disposición Adicional, consiste en la autorización para llevar a cabo una verdadera cesión o comunicación de datos entre Entidades Aseguradoras, sin que sea preciso el consentimiento del afectado, ni se den las circunstancias previstas en el apartado 2 del artículo 11 de la propia Ley Orgánica. De hecho, con la modificación producida en esta Disposición Adicional, estos ficheros comunes creados por las Entidades Aseguradoras gozarían de un régimen más privilegiado que el que los artículos 21 y siguientes reconocen para los ficheros de las Administraciones Públicas.

Merece una reflexión la enorme cantidad de afectados por esta norma, que podrían, sin su consentimiento, ser incluidos en este tipo de ficheros comunes. Piénsese en la cada vez mayor exigencia, incluso legal, de suscribir pólizas de seguros a la hora de realizar cualquier tipo de operación mercantil o de carácter meramente civil. Hoy en día, se exige la suscripción de estas pólizas para solicitar un préstamo bancario de carácter personal, para adquirir una vivienda mediante préstamo hipotecario, para adquirir un vehículo, para tener animales de compañía,… Incluso las escuelas y las empresas suscriben pólizas colectivas en nombre de sus alumnos o trabajadores para la cobertura de múltiples riesgos. Por ello, el significado real de esta medida no está lejos de poder considerarse una autorización para la conformación de una base de datos de magnitudes similares a las que podrían tener a su disposición las Administraciones Públicas, con el añadido de que la amplia variedad de seguros existentes, facilita que los datos incluidos se refieran a todo tipo de facetas de la personalidad de los afectados. Adviértase que tampoco la Ley realiza una determinación precisa de los datos que pueden ser objeto de este tratamiento, limitándose a exigir el consentimiento en el supuesto de datos relativos a la salud, pero inexplicablemente, no así en el caso de otros datos especialmente protegidos por el artículo 7.

No cabe justificación alguna para el privilegio que esta Ley establece. El tantas veces ya mencionado Convenio de 1981 permite excepciones a los derechos y principios básicos de la protección de datos cuando las mismas constituyan medidas necesarias en una sociedad democrática para la protección de la seguridad del Estado, de la seguridad pública, los intereses monetarios del Estado, la represión de infracciones penales, la protección de la persona concernida o los derechos y libertades de terceros. Ciertamente, es impensable encuadrar la actividad aseguradora habitual en ninguno de estos supuestos.

Por ello, estamos firmemente convencidos de que con esta disposición se incumplen todos los principios básicos para la protección de datos que, incluidos en los Convenios y Tratados Internacionales y en el mismo Título II de la Ley Orgánica, perfilan el contenido esencial del derecho a la autodeterminación informativa del artículo 18.4 de la Constitución, en los términos reconocidos por la Jurisprudencia del Tribunal Constitucional, y en especial el principio de proporcionalidad y los relativos a la cesión o comunicación de datos.

En consecuencia, se solicita la supresión de la redacción que la disposición adicional sexta lleva a cabo del párrafo segundo del artículo 24.3 de la Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de los Seguros Privados, por vulnerar el artículo 18.4 de la Constitución, al no respetar su contenido esencial, y el artículo 53.1 de la norma fundamental por igual motivo, en cuanto exime a las Entidades Aseguradoras del cumplimiento de los principios básicos del régimen de protección de datos, sin que exista justificación alguna que explique el privilegio que la norma otorga a este sector comercial. A estos efectos **la Comisión de Libertades e Informática propone la siguiente redacción:**

> "Las entidades aseguradoras podrán establecer ficheros de datos de carácter personal que permitan la colaboración estadístico-actuarial y la prevención del fraude en la selección de riesgos y en la liquidación de siniestros. Estos últimos se regularán de conformidad con lo dispuesto en el artículo 29 de la Ley Orgánica 5/1999, de13 de diciembre, de Protección de Datos de Carácter Personal, por lo que será necesaria la notificación al afectado en la primera introducción de sus datos en el fichero pero no el consentimiento del mismo."

23.- LEGISLACIÓN LABORAL: ESTATUTO TRABAJADORES, FUNCIONARIOS CIVILES DEL ESTADO, PREVENCIÓN DE RIESGOS LABORALES Y LIBERTAD SINDICAL.

La informática y los flujos de información son factores que hacen que, cada vez más, sea imprescindible contar con una adecuada red de comunicaciones interna y externa en la red empresarial. Debido a esta generalización tecnológica, proveedores, clientes y trabajadores se comunican a través de multitud de medios tecnológicos (intranets, páginas web para ofrecer servicios, Internet, fax, teléfono, etc) al servicio de la empresa y como herramienta de trabajo para los trabajadores.

Sin embargo, estos medios también han dado lugar a que sean utilizados para fines personales o extraprofesionales, por lo que es cada vez más frecuente que desde el sector empresarial se instauren políticas y actuaciones de control de sus trabajadores.

En este sentido, deben tenerse en cuenta dos partes, una, tal y como afirma la Sentencia del Tribunal Constitucional 186/2000, de 10 de julio, "*que el poder de dirección del empresario, reconocido expresamente en el artículo 20 LET, atribuye al empresario, entre otras facultades, la de adoptar las medidas que estime más*

oportunas de vigilancia y control para verificar el cumplimiento del trabajador de sus obligaciones laborales. Mas ha de producirse en todo caso dentro del debido respeto a la dignidad del trabajador", y otra, la dignidad del trabajador, la protección de sus datos de carácter personal, su intimidad, ...etc. y los límites a las injerencias no consentidas en esta esfera, y en este sentido, se deberán respetar determinadas normas y condiciones conformes a las exigencias de buena fe que deben regir en toda relación laboral.

El punto de inflexión entre estas dos caras de una misma moneda, está en el deber del empresario de informar sobre la política de seguridad de la empresa así como de las condiciones de uso de las herramientas tecnológicas de la empresa, y el derecho del trabajador a ser informado. Este planteamiento, está ya esbozado en la normativa específica de las relaciones laborales, el problema es que no lo está de forma conexa o refundida, dando lugar a numerosas y contradictorias interpretaciones a las que pueden ponerse fin, realizando algunos cambios en la legislación vigente.

a) Algunos derechos que amparan al trabajador:

- Constitución española: artículo 18.-Derecho a la intimidad personal y al secreto de las comunicaciones:

> "Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
>
> Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
>
> 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."

- Código penal: artículo 197 y ss.- Amparo ante ataques a la intimidad. Del descubrimiento y revelación de secretos.

- Ley orgánica de protección de datos 15/99.- Protección de los datos del trabajador

Protección de los datos de los empleados por el empresario, no utilizándolos nada más que para el uso para el que han sido dados por el trabajador (relación laboral, realización de nóminas, seguros, etc.), protegiéndolos adecuadamente, no cediéndolos a terceros sin consentimiento del afectado, no manteniéndolos más que en los plazos establecidos por la ley, y utilizados de forma legítima, adecuada y pertinente.

- Estatuto de los trabajadores (artículo 18).- Protección de la dignidad e intimidad del trabajador:

Sólo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de

trabajo y en horas de trabajo. En su realización se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible.

b) Algunos derechos que amparan al empresario:

- Potestad de dirección y control del empresario.- Artículo 20.3 del Estatuto de los Trabajadores.

El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso.

- Deber de secreto profesional.- Artículo 10 LOPD y artículos 199, 200 y 278 de código penal español. El deber obliga aún después de haber causado baja en la empresa.

Coherentemente sobre estas propuestas, y lo dispuesto por el *Documento de trabajo del Grupo de Trabajo «Artículo 29»2 relativo a la vigilancia y el control de las comunicaciones electrónicas en el lugar de trabajo*, **la Comisión de Libertades e Informática propone la introducción de las siguientes disposiciones adicionales:**

> **Disposición adicional séptima. Modificaciones del Texto Refundido de la Ley del Estatuto de los Trabajadores**, aprobado por Real Decreto Legislativo 1/1995, de 24 de marzo.
>
> 1.Se modifica el artículo 4.2.c) del Texto Refundido de la Ley del Estatuto de los Trabajadores, quedando su redacción como sigue:
>
> c) A no ser discriminados para el empleo, o una vez empleados, por razones de sexo, estado civil, por la edad dentro de los límites marcados por esta Ley, raza condición social, ideas religiosas o políticas, afiliación o no a un sindicato, así como por razón de lengua, dentro del Estado español. Tampoco podrán ser discriminados por razón de disminuciones físicas, psíquicas y sensoriales, siempre que se hallasen en condiciones de aptitud para desempeñar el trabajo o empleo de que se trate, ni por su herencia biológica.
>
> 2. Se añaden los apartados 4 y 5 al artículo 4 del Texto Refundido de la Ley del Estatuto de los Trabajadores, con la siguiente redacción:
>
> "4. Asimismo, La utilización de aparatos audiovisuales de observación y vigilancia electrónica sobre los trabajadores en locales no abiertos al público del centro de trabajo, deberá ser puesta en conocimiento de éstos y sus representantes y, salvo pacto en contrario entre el empresario y los representantes de los trabajadores, sólo podrán ser

utilizados para los fines de supervisión del rendimiento profesional o laboral siempre que ello no se pudiera hacer con otros medios menos intimidatorios, y siempre que no se atente al contenido esencial del derecho a la intimidad, a la protección de datos y a la propia imagen.

5. Los trabajadores que utilicen instrumentos tecnológicos en el desarrollo de su trabajo, tendrán derecho a un uso moderado y proporcionado de éstos con fines personales cuando ello fuera necesario y siempre y cuando no afecte a su rendimiento profesional o laboral, al rendimiento económico de la empresa, sus recursos o su imagen. En estos casos, podrán preservar reservadamente sus datos, ficheros o correo de carácter personal en los correspondientes procedimientos informáticos que se desarrollen en su actividad laboral. Lo anterior no será de aplicación cuando haya fundadas necesidades organizativas o tecnológicas que lo impidan."

Disposición adicional octava. Modificaciones del Texto Articulado de la Ley de Funcionarios Civiles del Estado, aprobado por Decreto 315/1964, de 7 de febrero.

1. Se adiciona al párrafo segundo del apartado 1 del artículo 63 del Texto Articulado de la Ley de Funcionarios Civiles del Estado, la siguiente redacción:

"En aquellos supuestos en los que se exija el cumplimiento de determinadas condiciones o la superación de pruebas concretas al funcionario para el acceso o permanencia en el puesto de trabajo, se especificarán las pruebas psíquicas, físicas o de cualquier otro tipo que se le requieran, así como los exámenes médicos que el funcionario deberá pasar a tal fin.

Los resultados obtenidos en los análisis o pruebas legalmente autorizadas, deberán destinarse exclusivamente al fin para el cual prestó su consentimiento el funcionario.

Los datos obtenidos ilícitamente deberán ser destruidos de forma inmediata. Los acuerdos, valoraciones o resoluciones basadas en datos obtenidos ilícitamente serán nulos de pleno derecho."

2. Se añade un último párrafo al apartado 1 del artículo 63 del Texto Articulado de la Ley de Funcionarios Civiles del estado con la siguiente redacción:

"Los funcionarios tendrán derecho a no ser discriminados en su relación de empleo con la Administración Pública, por razones de sexo, estado civil, por la edad dentro de los límites marcados por la Ley, raza, condición social, ideas religiosas o políticas, afiliación o no a un

sindicato, así como por razón de lengua, dentro del Estado español. Tampoco podrán ser discriminados por razón de disminuciones físicas, psíquicas y sensoriales, siempre que se hallasen en condiciones de aptitud para desempeñar el trabajo o empleo de que se trate, ni por herencia genética.

La utilización de aparatos audiovisuales de observación y vigilancia electrónica sobre los funcionarios en el centro de trabajo, en locales no abiertos al público, deberá ser puesto en conocimiento de éstos y sus representantes, y, salvo pacto en contrario entre la Administración correspondiente y los representantes de los funcionarios, sólo podrán ser utilizados para los fines de supervisión del rendimiento profesional o laboral, siempre que no se atente al contenido esencial del derecho a la intimidad, a la protección de datos y a la propia imagen.

Los funcionarios que utilicen instrumentos tecnológicos en el desarrollo de su trabajo, tendrán derecho a un uso moderado y proporcionado de éstos con fines personales, en cuyo caso, y siempre y cuando no afecte a su rendimiento profesional, al rendimiento económico de la empresa, sus recursos o su imagen, podrán preservar reservadamente sus datos, ficheros o correo de carácter personal en los correspondientes procedimientos informáticos que se desarrollen en su actividad laboral. Lo anterior no será de aplicación cuando haya fundadas necesidades organizativas o tecnológicas que lo impidan."

Disposición adicional novena. Modificación de la Ley 31/1995, de 8 de noviembre de Prevención de Riesgos Laborales.

El apartado 4 del artículo 22 de la Ley 31/1995, de 8 de noviembre de Prevención de Riesgos Laborales, queda redactado de la siguiente forma:

"Los datos relativos a la vigilancia de la salud de los trabajadores no podrán ser usados con fines discriminatorios, ni en perjuicio del trabajador, ni podrán ser utilizados para fines distintos de aquellos para los cuales fueron solicitados u obtenidos, aun resultando compatibles con los mismos."

Disposición adicional décima. Modificación de la Ley Orgánica 11/1985, de 2 de Agosto, de Libertad Sindical, modificada por la Ley Orgánica 14/1994 y por la Ley 11/1994.

1. El apartado 3.2 del artículo 10 de la Ley Orgánica 11/1985, de 2 de agosto queda redactado de la siguiente forma:

Asistir a las reuniones de los comités de empresa y de los órganos internos de la empresa, o de los órganos de representación que se establezcan en las Administraciones Públicas, con voz pero sin voto, en materia de seguridad e higiene y en materia de vigilancia electrónica y Protección de Datos de Carácter Personal. Asimismo deberá informar a los trabajadores.

2. El apartado 3.3 del artículo 10 de la Ley Orgánica 11/1985, de 2 de agosto queda redactado de la siguiente forma:

Ser oídos por la empresa previamente a la adopción de medidas de carácter colectivo que afecten a los trabajadores en general y a los afiliados a su sindicato en particular, en esta u otras materias, especialmente en los despidos y sanciones de estos últimos.

24.- LEY ORGÁNICA.

La disposición final segunda, establece qué partes y cuáles no, son Ley Orgánica.

Disposición Final Segunda. Preceptos con carácter de Ley ordinaria.

Los Títulos IV, VI excepto el último inciso del párrafo 4 del artículo 36 y VII de la presente Ley, la disposición adicional cuarta, la disposición transitoria primera y la final primera tienen el carácter de Ley ordinaria.

A la luz de las materias que regula el título IV:

Ficheros de titularidad pública

Artículo 20. Creación, modificación o supresión.
Artículo 21. Comunicación de datos entre Administraciones públicas.
Artículo 22. Ficheros de las Fuerzas y Cuerpos de Seguridad.
Artículo 23. Excepciones a los derechos de acceso, rectificación y cancelación.
Artículo 24. Otras excepciones a los derechos de los afectados.

Ficheros de titularidad privada

Artículo 25. Creación.
Artículo 26. Notificación e inscripción registral.
Artículo 27. Comunicación de la cesión de datos.
Artículo 28. Datos incluidos en las fuentes de acceso público.
Artículo 29. Prestación de servicios de información sobre solvencia patrimonial y crédito.
Artículo 30. Tratamientos con fines de publicidad y de prospección comercial.
Artículo 31. Censo promocional.
Artículo 32. Códigos tipo.

El art. 81.1 de la Constitución establece que el desarrollo de los derechos fundamentales y libertades públicas requiere una Ley Orgánica. En este sentido, el art. 81.1 CE establece lo siguiente:

"*1. Son leyes orgánicas las relativas al desarrollo de los derechos fundamentales y de las libertades públicas, las que aprueben los Estatutos de Autonomía y el régimen electoral general y las demás previstas en la Constitución*".

Sobre el alcance de la reserva de Ley Orgánica establecida en el art. 81.1 CE, la Sentencia del Tribunal Constitucional 173/1998, de 23 de julio, en su Fundamento Jurídico 7 señala lo siguiente:

El Tribunal Constitucional, desde la STC 5/1981, ha destacado "la necesidad de aplicar un criterio estricto o "restrictivo" para determinar el alcance de la reserva y ello tanto en lo referente al término "desarrollar", como a "la materia" objeto de reserva. Se trata, dice este Tribunal en reiteradas resoluciones, de evitar petrificaciones del ordenamiento y de preservar la regla de las mayorías parlamentarias no cualificadas.

Más concretamente, se ha afirmado que requiere ley orgánica únicamente la regulación de un derecho fundamental o de una libertad pública que "desarrolle" la Constitución de manera directa y en elementos esenciales para la definición del derecho fundamental, ya sea en una regulación directa, general y global del mismo o en una parcial o sectorial, pero, igualmente, relativa a aspectos esenciales del derecho, y no, por parcial, menos directa o encaminada a contribuir a la delimitación y definición legal del derecho".

"Precisando un poco más esta definición (...) se afirma que lo que está constitucionalmente reservado a la Ley Orgánica es la regulación de determinados aspectos esenciales para la definición del derecho, la previsión de su ámbito y la fijación de sus límites en relación con otras libertades constitucionalmente protegidas".

De tal manera, el Fundamento Jurídico 5 de la STC 292/2000, señala lo siguiente:

"Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE)."

Todo ello, a la luz de las materias de obligada regulación por Ley Orgánica, y teniendo en cuenta aquellas que así deben ser desarrolladas, en éste u otros títulos de la LOPD. Dejamos de este modo abiertas estas argumentaciones a otros ámbitos de la Ley que hoy son Ley Ordinaria, debiendo ser Ley Orgánica.

A estos efectos, **la Comisión de Libertades e Informática propone la siguiente redacción:**

> **Disposición Final Segunda. Preceptos con carácter de Ley Ordinaria**
>
> Los artículos 20 y 21 del título IV y los títulos VI excepto el último inciso del párrafo 4 del artículo 36 y VII de la presente Ley, la Disposición Adicional Cuarta, la Disposición Transitoria Primera y la Final Primera, tienen el carácter de Ley Ordinaria.

25.- ACTUALIZACIONES SOBRE LA LEGISLACIÓN VIGENTE.

La promulgación de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, ha provocado la introducción de **dos reformas,** en sus artículos 37.2 y en el artículo 48.3, que tienen su reflejo a lo largo del articulado propuesto para la LOPD.

> "37. 2. Las resoluciones de la Agencia Española de Protección de Datos se harán públicas, una vez hayan sido notificadas a los interesados. La publicación se realizará preferentemente a través de medios informáticos o telemáticos.
> Reglamentariamente podrán establecerse los términos en que se lleve a cabo la publicidad de las citadas resoluciones.
> Lo establecido en los párrafos anteriores no será aplicable a las resoluciones referentes a la inscripción de un fichero o tratamiento en el Registro General de Protección de Datos ni a aquéllas por las que se resuelva la inscripción en el mismo de los Códigos tipo, regulados por el artículo 32 de la presente Ley Orgánica."

> "48. 3. Los procedimientos sancionadores tramitados por la Agencia Española de Protección de Datos, en ejercicio de las potestades que a la misma atribuyan esta u otras Leyes, salvo los referidos a infracciones de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, tendrán una duración máxima de seis meses."

La Propuesta de la CLI, tiene su reflejo en la nueva redacción dada al art.37.1.c):

> Art.37. 1 Son funciones de la Agencia Española de Protección de Datos:
>
> e) Dictar y dar publicidad, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.

Así como ha provocado la introducción de la **nueva denominación** de la Agencia estatal de Protección de datos, en su art. el artículo 79 cambiándola a lo largo del texto legal por la denominación: "**Agencia Española de Protección de Datos"**.

27.- ACTUALIZACIÓN DE LAS EXPRESIONES "DATOS PERSONALES", "TELEMÁTICO" Y AUTOMATIZADO.

La Ley 15/99 tiene por objeto la protección de los "datos de carácter personal" y no los "datos personales", en desarrollo de la constitución, de un Derecho Fundamental de las personas físicas, pero luego utiliza ambos conceptos como sinónimos en su articulado. Consideramos esto un error, por lo siguiente:

Los "datos de carácter personal" son datos personales con dos fuertes restricciones:
a) Conciernen única y exclusivamente a personas físicas.
b) Estos datos identifican personas físicas o las hacen identificables.

La correcta definición de algunos conceptos, corrobora esta precisión:

a) Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables.

b) Fichero: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

d) Personal: Perteneciente a la persona o propio o particular de ella.

e) Datos personales: Cualquier información concerniente (perteneciente, propio, particular) a la persona.

Por tanto, entendemos que los datos personales, aunque pueden comprender en esencia los "datos de carácter personal", no tiene por qué ser así, pues aquellos que conciernen a personas jurídicas, o designando personas físicas, no lo hacen de forma que sean identificadas o identificables, no entrarían dentro de la calificación de "datos de carácter personal", y por tanto exceden del objeto de la LOPD. Un correcto planteamiento del articulado legal, debería prever esta distinción, al margen de que en el lenguaje común se utilicen ambos como sinónimos.

En similar situación se plantea la supresión de los términos "telemático" y "automatizado", el primero por cuanto un medio telemático, no es más que una aplicación a que se destina un dispositivo informático, y como ya se suele acompañar del término "informático", entendemos que debe suprimirse. El segundo, teniendo en cuenta que en el año 2007, la Ley será aplicable tanto a ficheros automatizados, como a los no automatizados, este término diferenciador ya no tiene sentido.

27.- NOTA FINAL: *CONEXIONES.

Las referencias reseñadas como "***Conexiones**", se refieren a aquellos artículos cuya modificación se ve provocada por lo expuesto en el correspondiente apartado, además del que en él se expone. Para su mejor localización, a continuación se trascribe la versión del texto legal de la LOPD una vez reformado.

ANEXO I :
TEXTO LEGAL MODIFICADO.

PROYECTO DE LEY POR EL QUE SE MODIFICA LA LEY ORGANICA 15/1999, DE 13 DE DICIEMBRE DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.-

EXPOSICIÓN DE MOTIVOS

(….)

La primera ley que en España reguló el tratamiento automatizado de los datos de carácter personal fue la LO 5/92 (LORTAD). Contenía un didáctico y elogiado, en su momento, preámbulo del que es posible rescatar a modo de memoria histórica algunos principios, ya que la jurisprudencia y el desarrollo legislativo nacional e internacional demandan una exposición actualizada que justifique las variantes de la actual ley de protección de datos de carácter personal. Un principio inalterable es que el conocimiento ordenado de los datos de carácter personal permite dibujar un determinado perfil de la persona, que puede resultar luego valorado favorable o desfavorablemente para todas sus actividades públicas o privadas. Y no cabe duda que el tratamiento de datos de carácter personal , desde los más inocuos hasta los más sensibles, puede incidir negativamente o menoscabar el ejercicio de derechos intrínsecos del ser humano. Las generaciones de derechos fundamentales han evolucionado, ampliándose por reacción a cambios sociales, políticos, económicos o tecnológicos, así, el siglo XXI conlleva, entre otras realidades, la revolución Tecnológica, y ahí se incorpora la protección de los datos de carácter personal o libertad informática, en su doble contenido: el negativo o exclusión de todo lo externo que afecte a la intimidad y el positivo o posibilidad de ejercer las facultades que permiten a la persona controlar por el acceso, rectificación, cancelación u oposición, todos sus datos.

Retomando la dogmática de la Constitución Española, el Art. 18 reconoce el derecho individual al honor, intimidad personal y familiar y propia imagen, y en el párrafo 4, en un innegable alarde innovador, emplaza a limitar 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 legislador tenía ante sí, básicamente dos campos de actuación: El primero, la informática, que en los años setenta era tanto un potencial recurso de apertura al progreso tecnológico, como una herramienta agresiva para los tradicionales derechos fundamentales. Y el segundo, formado por los derechos fundamentales de la intimidad y el honor. El primer desarrollo legislativo del Art. 18, lo materializa la LO 1/82 de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Se presentó la ocasión de incluir una disposición transitoria ordenando que, en tanto no se desarrollara el Art. 18.4, la intromisión en tales derechos ocasionada por el uso de la informática quedaba sujeta a lo previsto en esa ley.

La Constitución Española nominalmente no concede identidad jurídica propia como derecho fundamental a la protección de datos de carácter personal . Es la Jurisprudencia del Tribunal Constitucional la que comienza pronunciando en la STC 254/1993 que la "libertad informática", estaba reconocida por el Art. 18.4 CE (....) como la libertad de controlar el uso de datos de carácter personal insertos en un programa informático: lo que se conoce con el nombre de "habeas data" .

Tampoco la LORTAD explicitaba como derecho de la personalidad la protección de datos de carácter personal . Su finalidad es hacer frente a los riesgos que para los mismos puede suponer el acopio y tratamiento por medios informáticos, y su objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos. No obstante supuso la primera cobertura legal al habeas data, compendio de los derechos nucleares de acceso, rectificación, cancelación y oposición del afectado sobre el tratamiento de sus datos de carácter personal .

La expansión de las Tecnologías de la Información y de las Comunicaciones en el nuevo orden de la Sociedad de la Información, apremia a la Unión Europea a instar a los Estados miembros la incorporación en su respectivo Derecho interno de la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal y a la libre circulación de los mismos. Es entonces cuando el Derecho comunitario procede a precisar y ampliar los contenidos del Convenio de 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos de carácter personal y España se adapta al derecho comunitario con la aprobación de la LO 15/99 de protección de datos de carácter personal (LOPD), derogándose la anterior LORTAD. Diversos artículos de la nueva Ley se recurren por inconstitucionalidad y el Tribunal Constitucional se pronuncia estimando el recurso en la sentencia 292/2000, porque los preceptos recurridos no respetan el contenido esencial del derecho fundamental al honor y a la intimidad personal y familiar así como del derecho fundamental ahora denominado Derecho a la Protección de Datos.

Los Fundamentos Jurídicos de la STC 292/00 renuevan la doctrina jurídica, establecen su contenido esencial y regulan el ejercicio de facultades que integran el derecho fundamental a la protección de datos. Significó el ensanchamiento, a través de la jurisprudencia, del catálogo de derechos y libertades reconocidos expresamente en la Constitución Española. La consolidación legítima como derecho fundamental, de la protección de datos de carácter personal, y el reforzamiento de su protección, se presenta respectivamente en la Carta de los Derechos Fundamentales de la Unión Europea en el año 2000 y en la Directiva 2002/58/CE que pretende garantizar el respeto de los derechos fundamentales y los principios consagrados en la Carta, así como, especificar y completar la Directiva 95/46, en lo que respecta al tratamiento de los datos de carácter personal en el sector de las comunicaciones electrónicas.

Concluye el aporte jurídico de la Unión Europea en el ámbito de los derechos fundamentales, con el consenso de los Estados y la firma del Tratado por el que se establece una Constitución para Europa, y que supone un impulso para la protección

de los datos de carácter personal. La Constitución les da categoría de principios para el desarrollo de la vida democrática de la Unión y los integra entre los derechos de libertad de la renovada Carta de los Derechos Fundamentales de la Unión.

Junto al reconocimiento del derecho fundamental a la protección de los datos de carácter personal evolucionan límites y garantías en su ejercicio. La LO 15/99 de protección de datos de carácter personal, es la norma que ha venido regulando la base de los principios de su protección, así como, de los derechos de las personas en su ejercicio. Los siete Títulos que la componen tienen por objetivo la adecuación del ordenamiento jurídico nacional al comunitario y la adaptación a las circunstancias sociales y legales internas.

Algunos de los motivos que justifican la presente reforma son: La necesidad de acabar con la incertidumbre –cuando no inconstitucionalidad en su sentido literal- que provocaba la existencia del término "incompatibles" en al art. 4.2 referido a las finalidades para las cuales se recaban los datos, dejando ya sentado que los datos recabados para una finalidad concreta no podrán ser utilizados para finalidades distintas a aquella. El término incompatibles queda -tal y como aparece en la Directiva 95/46/CE - para los tratamientos; La introducción de la figura del Delegado de Protección de Datos como un garante del derecho y colaborador de las Autoridades de Control en materia de protección de datos; La regulación específica de los requisitos para la obtención de los datos de los menores de edad; La necesidad de disociar los datos en los casos de tratamientos al margen de la regulación general siempre que tal disociación sea posible; La posibilidad de adoptar medidas cautelares previas al tratamiento de datos cuando estos menoscaben derechos de los interesados; La modificación de la composición del Consejo de Protección de Datos para adaptarlo mejor a las principales realidades sociales implicadas en materia de protección de datos; La supresión del censo promocional; La introducción de las llamadas "Listas Robinson"; la prevención de que el régimen sancionador se adapte mejor a la realidad sancionadora dando un margen mayor a la Administración para adecuar las sanciones a la realidad concreta de cada infracción y estableciendo medidas para evitar en la medida de lo posible que económicamente sea más rentable abonar una sanción que cumplir con la legalidad, etc.

Artículo 1. Objeto. La presente Ley Orgánica tiene por objeto garantizar y proteger el derecho fundamental a la protección de los datos de carácter personal, así como el honor e intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos en lo que concierne al tratamiento de dichos datos.

Artículo 2. Ámbito de aplicación

1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en territorio español en el

marco de las actividades de un establecimiento del responsable del tratamiento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación Española en aplicación de normas de Derecho Internacional público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:

a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.

3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos de carácter personal:

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

b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.

c) Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del Régimen del personal de las Fuerzas Armadas.

d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes.

e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

f) Los Ficheros establecidos para la investigación del terrorismo y de formas de delincuencia organizada.

Artículo 3. Definiciones

A los efectos de la presente Ley Orgánica se entenderá por

a) Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables.

b) Fichero: Todo conjunto organizado de datos de carácter personal, 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 o tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

e) Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.3.

e bis) Delegado de Protección de Datos: Persona física o jurídica, de naturaleza pública o privada, encargada de velar por el cumplimiento de lo dispuesto en la presente Ley y en su normativa de desarrollo en el seno de las entidades que traten datos de carácter personal.

f) Procedimiento de disociación: Todo tratamiento de datos de carácter personal de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

g) Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos de carácter personal por cuenta del responsable del tratamiento.

h) Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos de carácter personal que le conciernen.

i) Cesión o comunicación de datos: Toda revelación de datos de carácter personal realizada a una persona distinta del interesado.

j) Fuentes accesibles al público: Aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines Oficiales y los medios de comunicación.

k) Bloqueo de datos: la identificación, reserva e implantación de los medios necesarios que garanticen su conservación con el fin de impedir su tratamiento.

TÍTULO II
PRINCIPIOS DE LA PROTECCIÓN DE DATOS

Artículo 4. Calidad de los datos

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades distintas de aquellas para las que los datos hubieran sido recogidos ni podrán tratarse posteriormente de manera incompatible con dichos fines. No se considerara incompatible el tratamiento posterior y disociado de estos datos con fines históricos, estadísticos o científicos. Si no pudiera realizarse la disociación por requerirlo así estos fines , los datos no podrán ser tratados si con ello se pusiese en peligro la seguridad de las personas, su honor, la intimidad de su vida privada y familiar y su propia imagen, ni, en todo caso, podrán ser públicamente consultados sin que medie consentimiento expreso e informado de los afectados o hasta que haya transcurrido un plazo de 25 años desde su muerte si su fecha es conocida o, en otro caso, de 50 años a partir de la fecha de los documentos en que consten.

3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual 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 16.

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 o 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 los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

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 interesados a los que se soliciten datos de carácter personal deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que le sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de tránsito, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

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 necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos de carácter personal que se solicitan o de las circunstancias en que se recaban.

4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.

5. No será de aplicación lo dispuesto en el apartado anterior cuando expresamente una Ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, y esté disociado salvo que puedan afectar a la seguridad de las personas, a su honor, a la intimidad de su vida privada y familiar y a su propia imagen, Si no pudiera realizarse la disociación por requerirlo así estos fines , los datos no podrán ser tratados si con ello se pusiese en peligro la seguridad de las personas, su honor, la intimidad de su vida privada y familiar y su propia imagen, ni, en todo caso, podrán ser públicamente consultados sin que medie consentimiento expreso e informado de los afectados o hasta que haya transcurrido un plazo de 25 años desde su muerte si su fecha es conocida o, en otro caso, de 50 años a partir de la fecha de los documentos en que consten.

Tampoco será de aplicación, cuando la información al interesado resulte imposible o exija esfuerzos

desproporcionados, y medie previa autorización de la Agencia Española de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

Asimismo, tampoco regirá lo dispuesto en el apartado cuarto cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

Artículo 6. Consentimiento del afectado

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa. No será válido el consentimiento otorgado mediante un contrato de adhesión, salvo que figure forma separada al clausulado general e implique una declaración expresa del interesado.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7 apartado 6 de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

3. El consentimiento a que se refiere este artículo podrá ser revocado por el afectado en cualquier momento sin que se le atribuyan efectos retroactivos.

4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

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 el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

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 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 ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras. Ninguna entidad o persona física privada podrá acceder a estos datos, salvo que exista previa autorización judicial.

Artículo 7 bis. Datos de menores.

1. Los datos de carácter personal de los menores, no serán recabados sin su consentimiento expreso e informado sobre la totalidad de los extremos contenidos en el artículo 5 de esta Ley, en cualquier caso, los datos especialmente protegidos sólo podrán ser recabados o tratados cuando así lo disponga una ley.

Cuando sean menores de catorce años o sus condiciones de madurez no garanticen la plena comprensión de la información que se les facilita, el consentimiento habrá de ser prestado por sus representantes legales."

2. En cualquier caso, los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores, y con el conocimiento de éstos, los derechos de acceso, rectificación, cancelación, oposición, o cualesquiera otros que pudieran corresponderles en el contexto de la presente Ley.

3. El tratamiento de los datos de carácter personal de los menores, deberá realizarse con las medidas de confidencialidad suficientes y necesarias para evitar abusos en su manipulación.

Artículo 8. Datos relativos a la salud

1. No obstante lo dispuesto en el artículo 7 podrán ser objeto de tratamiento los datos de carácter

personal a que se refieren el apartado 3 de dicho artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico de salud, la prestación de asistencia sanitaria o tratamientos de salud, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. Cuando dicho tratamiento no requiera esencialmente la identidad de las personas y en todo caso cuando se trate de un tratamiento de datos que sea necesario para la gestión de los servicios sanitarios deberá efectuarse la previa disociación de los mismos.

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando sea necesario para salvaguardar el interés vital del afectado, o de otra persona, en el supuesto de que esté física o jurídicamente incapacitado para dar su consentimiento y no sea posible recabar el consentimiento sus representantes legales sin perjuicio, en todo caso, de su posterior e inmediata puesta en conocimiento del Ministerio Fiscal o la Autoridad Judicial.

2. 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 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 la legislación estatal o autonómica sobre sanidad.

3. El tratamiento de los datos de carácter personal obtenidos del análisis de material genético, sólo podrá realizarse previa habilitación legal, con el consentimiento expreso, escrito e informado del interesado y, en cualquier caso, exclusivamente para fines de salud o de investigación científica, por razones de salud - en particular para evitar un serio perjuicio a la salud del afectado o de terceros, o permitir al afectado tomar una decisión libre e informada en estas materias- y para fines judiciales o de investigación criminal en la prevención de un peligro real o un delito concreto.

Artículo 9. Seguridad de los datos

1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

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

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

Artículo 10. Deber de secreto

El responsable del fichero 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 aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Artículo 10. bis. El Delegado de Protección de Datos.

1. El Delegado de Protección de Datos velará por el cumplimiento de lo dispuesto en la presente Ley y en su normativa de desarrollo en el seno de las entidades que traten datos de carácter personal. La designación de un Delegado de Protección de Datos será obligatoria para las entidades que empleen más de 250 personas y en las Administraciones Públicas con respeto en todo caso a su autonomía competencial.

2. El Delegado de Protección de Datos deberá reunir los requisitos de independencia y capacidad necesarios al buen desempeño de su cargo. Reglamentariamente se desarrollará su nombramiento, naturaleza, ámbito de actuación y condiciones del ejercicio de sus competencias. En todo caso:

a) Si el Delegado de Protección de Datos forma parte del ámbito de organización y dirección de la entidad, se garantizará su independencia dentro de la misma, debiendo únicamente rendir cuentas ante su máximo responsable, pudiendo inspeccionar y dictar órdenes y/o recomendaciones en el ámbito propio de sus competencias bajo sanción de corrección interna, sin perjuicio de las responsabilidades civiles, penales o administrativas que puedan derivar de dicho incumplimiento.

b) Deberá evitarse cualquier conflicto de intereses que pueda menoscabar la garantía de independencia que debe reunir el Delegado de Protección de Datos. Los conflictos de intereses se valorarán atendiendo a la relación preexistente entre el Director de la entidad y el Delegado y a todas las demás circunstancias profesionales que rodeen al Delegado y puedan influir en su independencia.

c) Deberá poseer conocimientos informáticos consolidados y conocimientos jurídicos que le habiliten para el desempeño de su función.

3. La Agencia Española de Protección de Datos o, en su caso, el Organismo competente de cada Comunidad Autónoma habilitarán un canal de comunicación directo con los Delegados de Protección de Datos con el fin de coadyuvar al eficaz desempeño de su función y de recibir las aportaciones prácticas de los mismos en materia de protección de datos.

Artículo 11. Comunicación de datos

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

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

a) Cuando la cesión está autorizada en una Ley.

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

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

d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e) Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior, y siempre que sea posible disociado de los datos con fines históricos, estadísticos o científicos. Si no pudiera realizarse la disociación por requerirlo así estos fines , los datos no podrán ser tratados si con ello se pusiese en peligro la seguridad de las personas, su honor, la intimidad de su vida privada y familiar y su propia imagen, ni, en todo caso, podrán ser públicamente consultados sin que medie consentimiento expreso e informado de los afectados o hasta que haya transcurrido un plazo de 25 años desde su muerte si su fecha es conocida o, en otro caso, de 50 años a partir de la fecha de los documentos en que consten.

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 o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

11.2. bis. Los entes públicos, independientemente de su adscripción territorial o funcional, en ningún caso podrán ceder con fines comerciales datos de carácter personal que obren en su poder.

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de

aquél a quien se pretenden comunicar.

4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

5. Aquél a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.

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

Artículo 12. Acceso a los datos por cuenta de terceros

1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

TÍTULO III

DERECHOS DE LAS PERSONAS

Artículo 13. Impugnación de valoraciones

1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una

valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.

3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.

4. La valoración sobre el comportamiento de los ciudadanos basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

Artículo 14. Derecho de Consulta al Registro General de Protección de Datos

Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita.

Artículo 15. Derecho de acceso

1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos así como las comunicaciones realizadas o que se prevén hacer de los mismos.

2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización o audición, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, o cualquier otro medio semejante, siempre que el interesado así lo solicite dicha información deberá serle entregada o remitida por cualquiera de estos últimos medios en el plazo de 10 días.

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 interesado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.

Artículo 16. Derecho de rectificación, cancelación y oposición.

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación, cancelación u oposición al tratamiento de los datos de carácter personal del interesado en el plazo de diez días, notificando al mismo mediante cualquier medio del que quede constancia documental de su recepción, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.

3. La cancelación dará lugar al bloqueo de los datos,

conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación, oposición o cancelación efectuada a quienes se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la rectificación o cancelación.

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 tratamiento y el interesado.

Artículo 17. Procedimiento de oposición, acceso, rectificación o cancelación

1. Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente.

2. No se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación.

Artículo 18. Tutela de los derechos

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

2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia Española de Protección de Datos o, en su caso, del Organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación.

3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses.

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

5. . Si en el curso de una inspección, se observara que determinados tratamientos de datos de carácter personal, pudieran producir graves perjuicios a sus titulares, las autoridades de control podrán acordar la implantación de medidas cautelares, acordes al mandato de la presente Ley.

Artículo 19. Derecho a indemnización

1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por

el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados. Para la defensa del derecho a la protección de datos el afectado podrá acudir al procedimiento establecido para la protección de los derechos fundamentales.

2. 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.

3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

TÍTULO IV
DISPOSICIONES SECTORIALES
CAPÍTULO PRIMERO

Ficheros de titularidad pública

Artículo 20. Creación, modificación o supresión

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

Las autoridades de control, podrán realizar las comprobaciones previas que sean necesarias sobre los tratamientos que puedan suponer riesgos específicos para los derechos y libertades de los interesados velando en esos casos por que sean examinados antes del comienzo del tratamiento. Dichas comprobaciones previas se acordarán obligatoriamente de oficio cuando hubieran tenido indicios suficientes de dichos riesgos o cuando hayan recibido notificación al respecto del responsable del fichero, por el encargado del tratamiento o, en su caso, por el Delegado de Protección de Datos, quienes, en caso de duda, deberán consultar a las autoridades de control.

2. Las disposiciones de creación o de modificación de ficheros deberán indicar:

a) La finalidad del fichero y los usos previstos para el mismo.

b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.

c) El procedimiento de recogida de los datos de carácter personal.

d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.

e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.

f) Los órganos de las Administraciones responsables del fichero.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

3. En las disposiciones que se dicten para la supresión de los ficheros se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.

Artículo 21. Comunicación 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 comunicados a otras Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación tenga por objeto el tratamiento posterior, y siempre que sea posible disociado, de los datos con fines históricos, estadísticos o científicos. Si no pudiera realizarse la disociación por requerirlo así estos fines, los datos no podrán ser tratados si con ello se pusiese en peligro la seguridad de las personas, su honor, la intimidad de su vida privada y familiar y su propia imagen, ni, en todo caso, podrán ser públicamente consultados sin que medie consentimiento expreso e informado de los afectados o hasta que haya transcurrido un plazo de 25 años desde su muerte si su fecha es conocida o, en otro caso, de 50 años a partir de la fecha de los documentos en que consten.

2. Podrán, en todo caso, ser objeto de comunicación 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 comunicación 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.

4. En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley.

Artículo 22. Ficheros de las Fuerzas y Cuerpos de Seguridad

1. Los ficheros 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 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 exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.

4. Los datos de carácter personal 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 judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Artículo 23. Excepciones a los derechos de acceso, rectificación, cancelación y oposición.

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 los derechos de acceso, y 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 de acceso, oposición y cancelación 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.

Se deberá atender en todo caso el derecho a la rectificación siempre que esté suficientemente motivado por el titular de los datos.

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 Española de Protección de Datos o del Organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones Tributarias Autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

Artículo 24. Otras excepciones a los derechos de los afectados

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.

CAPÍTULO II

Ficheros de titularidad privada

Artículo 25. Creación

Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas.

Artículo 26. Notificación e inscripción registral

1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia Española de Protección de Datos.

2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.

3. Deberán comunicarse a la Agencia Española de Protección de Datos los cambios que se produzcan en la finalidad del fichero, en su responsable y en la dirección de su ubicación.

4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles.

En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia Española de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero a todos los efectos.

Artículo 27. 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), e) y 6 del artículo 11, ni cuando la cesión venga impuesta por Ley.

Artículo 28. Datos incluidos en las fuentes de acceso público

1. Los datos de carácter personal que figuren en las listas de personas pertenecientes a grupos de profesionales a que se refiere el artículo 3 j) de esta Ley deberán limitarse a los que sean estrictamente necesarios para cumplir la finalidad a que se destina cada listado. La inclusión de datos adicionales por las entidades responsables del mantenimiento de dichas fuentes requerirá el consentimiento del interesado, que podrá ser revocado en cualquier momento.

2. Los interesados tendrán derecho a que la entidad responsable del mantenimiento de los listados de los Colegios profesionales indique gratuitamente que sus datos de carácter personal no pueden utilizarse para fines de publicidad o prospección comercial.

La atención a la solicitud de exclusión de la información innecesaria o de inclusión de la objeción al uso de los datos para fines de publicidad o venta a distancia deberá realizarse en el plazo de diez días respecto de las informaciones que se realicen mediante consulta o comunicación por medios informáticos y en la siguiente edición del listado cualquiera que sea el soporte en que se edite.

3. Las fuentes de acceso público que se editen en forma de libro o algún otro soporte físico, perderán el carácter de fuente accesible con la nueva edición que se publique.

En el caso de que se obtenga por medios informáticos una copia de la lista en formato electrónico, ésta perderá el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su obtención.

Artículo 29. 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 datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

2. Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el creedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, 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.

3. En los supuestos a que se refieren los dos apartados anteriores cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos que están siendo tratados en este sentido, la entidad que los ha

facilitado, los motivos de su inclusión en este tipo de tratamiento, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.

4. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquellos. En todo caso, se prohíbe el mantenimiento de líneas o el tratamiento de datos con saldo cero.

Artículo 30. Tratamientos con fines de publicidad y de prospección comercial.

1 Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, podrán recabar nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.

Al objeto de regular la utilización de tales datos para los fines a los que se refiere el párrafo anterior, se creará una lista que indique las preferencias de cada individuo en materia de publicidad directa y en la que existirá un apartado en el que constará la relación de personas que se hayan manifestado en contra de la recepción de cualquier tipo de publicidad. Esta lista deberá ser consultada por los responsables de tratamientos con fines de publicidad y de prospección comercial, con carácter previo a cada envío, con el fin de cancelar los datos de los afectados que hayan manifestado su deseo de no recibir este tipo de publicidad del tratamiento.

La Agencia Española de Protección de Datos podrá encomendar la creación y mantenimiento de dicha lista a organismos privados, siempre y cuando no se vulneren los derechos y libertades fundamentales de los individuos. Se desarrollará reglamentariamente las modalidades de funcionamiento de la lista, debiendo en todo caso asegurar la inclusión de los interesados mediante procedimientos sencillos y gratuitos, en particular a través de Internet o cualquier otro procedimiento semejante.

2. En todo caso, cuando los datos procedan de fuentes accesibles al público de conformidad con lo establecido en el párrafo segundo del artículo 5.5 de esta Ley, en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten y expresamente contendrán la palabra “publicidad”.

El responsable del fichero deberá facilitar un sencillo sistema de acceso a dicha información, a través de medios de comunicación seguros y de forma gratuita, cuando por las

características técnicas de la comunicación, no sea posible cumplir directa y completamente con las exigencias del artículo 5.5.

3. En el ejercicio del derecho de acceso los interesados tendrán derecho a conocer el origen de sus datos de carácter personal, así como del resto de información a que se refiere el artículo 15.

4. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

Artículo 31. (sin contenido)

Artículo 32. Códigos tipo

1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada así como las organizaciones en que se agrupen, 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 a los principios y disposiciones de la presente Ley y sus normas de desarrollo.

2. 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 incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.

3. 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 y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia Española de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas.

TÍTULO V

MOVIMIENTO INTERNACIONAL DE DATOS

Artículo 33. Norma general

1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento 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 Española de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia Española de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos de finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Artículo 34. 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 internacional.

c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico de salud, la prestación de asistencia sanitaria o tratamiento de salud o la gestión de servicios sanitarios.

d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.

g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.

h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro

Público y aquélla sea acorde con la finalidad del mismo.

k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

TÍTULO VI

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Artículo 35. Naturaleza y régimen jurídico.

1. La Agencia Española de Protección de Datos es un Ente de Derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena 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.

2. En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la presente Ley y sus disposiciones de desarrollo, la Agencia Española de Protección de Datos actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En sus adquisiciones patrimoniales y contratación estará sujeta al Derecho privado.

3. Los puestos de trabajo de los órganos y servicios que integren la Agencia Española 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.

4. La Agencia Española 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.

5. La Agencia Española 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 36. El Director

1. El Director de la Agencia Española de Protección de Datos dirige la Agencia y ostenta su representación. Será nombrado, de

entre quienes componen el Consejo de Protección de Datos, mediante Real Decreto, por un período de cuatro años.

2. Ejercerá sus funciones con plena independencia y objetividad, y no estará sujeto a instrucción alguna en el desempeño de aquéllas.

En todo caso, el Director deberá oír al Consejo de Protección de Datos en aquéllas propuestas que éste le realice en el ejercicio de sus funciones.

3. El Director de la Agencia Española 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 de Protección de Datos, 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 Española de Protección de Datos tendrá la consideración de alto cargo y quedará en la situación de servicios especiales si con anterioridad estuviera desempeñando una función pública. En el supuesto de que sea nombrado para el cargo algún miembro de la carrera judicial o fiscal, pasará asimismo a la situación administrativa de servicios especiales.

Artículo 37. Funciones

1. Son funciones de la Agencia Española 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, oposición y cancelación de datos.

b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.

c) Dictar y dar publicidad, sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos 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 de los datos de carácter personal.

f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.

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 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.

k) Redactar una memoria anual y remitirla a las Cortes Generales.

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 de carácter personal .

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 46.

n) Cuantas otras le sean atribuidas por normas legales o reglamentarias.

2. Las resoluciones de la Agencia Española de Protección de Datos se harán públicas, una vez hayan sido notificadas a los interesados. La publicación se realizará preferentemente a través de medios informáticos.

Reglamentariamente podrán establecerse los términos en que se lleve a cabo la publicidad de las citadas resoluciones.

Lo establecido en los párrafos anteriores no será aplicable a las resoluciones referentes a la inscripción de un fichero o tratamiento en el Registro General de Protección de Datos ni a aquéllas por las que se resuelva la inscripción en el mismo de los Códigos tipo, regulados por el artículo 32 de esta Ley Orgánica.

Artículo 38. Consejo de Protección de Datos

El Director de la Agencia Española de Protección de Datos estará asesorado por un Consejo de Protección de Datos compuesto por los siguientes miembros:

- Un diputado, propuesto por el Congreso de los Diputados.

- Un Senador, propuesto por el Senado.

- Un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente.

- Un representante de la Administración Central, designado por el Gobierno.

- 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 representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente

- Un representante de las Organizaciones Sindicales más representativas, seleccionado del modo que se prevea reglamentariamente

- Un representante de las asociaciones más representativas en materia de Protección de Datos de Carácter Personal seleccionado del modo que se prevea reglamentariamente.

- Un representante de las asociaciones más representativas específicamente relacionadas con el uso de Internet, seleccionado del modo que se prevea reglamentariamente.

- Un destacado jurista, con demostrada experiencia y conocimientos en el ámbito del derecho a la protección de datos, y elegido a propuesta del Consejo Superior de Universidades.

-Un titulado universitario competente en Informática elegido a propuesta de su corporación profesional.

El funcionamiento del Consejo de Protección de Datos se regirá por las normas reglamentarias que al efecto se establezcan.

Artículo 39. El Registro General de Protección de Datos

1. El Registro General de Protección de Datos es un órgano integrado en la Agencia Española de Protección de Datos.

2. Serán objeto de inscripción en el Registro General de Protección de Datos

a) Los ficheros de que sean titulares las Administraciones Públicas.

b) Los ficheros de titularidad privada.

c) Las autorizaciones a que se refiere la presente Ley.

d) Los códigos tipo a que se refiere el artículo 32 de la presente Ley.

e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

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 40. Potestad de inspección

1. Las autoridades de control podrán inspeccionar los ficheros a que hace referencia la presente Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos.

A tal efecto, podrán 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 41. Órganos correspondientes de las Comunidades Autónomas

1. Las funciones de la Agencia Española de Protección de Datos reguladas en el artículo 37, a excepción de las mencionadas en los apartados j), k) y l), y en los apartados f) y g) en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 46 y 49, en relación con sus específicas competencias serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido.

2. Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros para el ejercicio de las competencias que se les reconoce sobre los mismos.

3. El Director de la Agencia Española de Protección de Datos deberá convocar regularmente a los órganos correspondientes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación. El Director de la Agencia Española 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 42. Ficheros de las Comunidades Autónomas en materia de su exclusiva competencia.

1. Cuando el Director de la Agencia Española de Protección de Datos constate que el mantenimiento o uso de un determinado fichero de las Comunidades Autónomas

contraviene algún precepto de esta Ley en materia de su exclusiva competencia podrá requerir a la Administración correspondiente que se adopten 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 Española de Protección de Datos podrá impugnar la resolución adoptada por aquella Administración.

TÍTULO VII

INFRACCIONES Y SANCIONES

Artículo 43. Responsables

1. Los responsables de los ficheros y los encargados de los tratamientos 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 46, apartado 2.

Artículo 44. Tipos de infracciones.

1. Las infracciones se calificarán como leves, graves o muy graves.

2. Son infracciones leves:

a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos de carácter personal objeto de tratamiento cuando legalmente proceda.

b) No proporcionar la información que solicite la Agencia Española de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.

c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.

3. Son infracciones graves:

a) Proceder a la creación de ficheros 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 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.

d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos 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 de los derechos de acceso y oposición 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 sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.

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 Española 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.

k) No inscribir el fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando haya sido requerido para ello por el Director de la Agencia Española de Protección de Datos.

l) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado.

m) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley.

n) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave.

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 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 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 de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia Española 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 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 Española de Protección de Datos.

f) Tratar 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, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.

h) No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

i) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

Artículo 45. Tipo de sanciones

1. Las infracciones leves serán sancionadas con multa de 600 euros a 60.000 euros.

2. Las infracciones graves serán sancionadas con multa de 60.000 euros a 300.000 euros.

3. Las infracciones muy graves serán sancionadas con multa de 300.000 euros a 600.000 de euros.

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, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, al número de personas afectadas y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda

inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate.

6. Del mismo modo, si en razón de las circunstancias concurrentes, se apreciara una cualificada intencionalidad en la culpabilidad o en la reincidencia o se apreciara una agravación de la antijuridicidad del hecho o si el beneficio obtenido superase económicamente el máximo de la sanción prevista para la clase de infracción de que se trate, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que siga inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate. Cuando se trate de infracciones muy graves el aumento de la sanción podrá alcanzar hasta el 10% de la facturación anual mundial de la empresa sancionada.

7. El Gobierno actualizará periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios.

Artículo 46. Infracciones de las Administraciones Públicas.

1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de los que sean responsables las Administraciones Públicas, el Director de la Agencia Española de Protección de Datos dictará una resolución estableciendo las medidas que proceda 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 Autoridad de control que corresponda las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

4. El Director de la Autoridad de Control que corresponda, comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores.

Artículo 47. 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

causas no imputables al presunto infractor.

4. Las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año.

5. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel 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 está paralizado durante más de seis meses por causa no imputable al infractor.

Artículo 48. Procedimiento 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. Las resoluciones de la Agencia Española de Protección de Datos u órgano correspondiente de la Comunidad Autónoma agotan la vía administrativa.

3. Los procedimientos sancionadores tramitados por la Agencia Española de Protección de Datos, en ejercicio de las potestades que a la misma atribuyan esta u otras Leyes, salvo los referidos a infracciones de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, tendrán una duración máxima de seis meses._

Artículo 49. Potestad de inmovilización de ficheros

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

DISPOSICIONES ADICIONALES

Primera. Ficheros preexistentes

Los ficheros y tratamientos, inscritos o no en el Registro General de Protección de Datos deberán adecuarse a la presente Ley Orgánica dentro del plazo de tres años, a contar desde su entrada en vigor. En dicho plazo, los ficheros de titularidad privada deberán ser comunicados a la Agencia Española

de Protección de Datos y las Administraciones Públicas, responsables de ficheros de titularidad pública, deberán aprobar la pertinente disposición de regulación del fichero o adaptar la existente.

En el supuesto de ficheros y tratamientos no automatizados, su adecuación a la presente Ley Orgánica y la obligación prevista en el párrafo anterior deberá cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados..

Segunda. Ficheros y Registro de Población de las Administraciones Públicas.

1. La Administración General del Estado y las Administraciones de las Comunidades Autónomas podrán solicitar al Instituto Nacional de Estadística, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes y en el censo electoral correspondientes a los territorios donde ejerzan sus competencias, para la creación de ficheros o registros de población.

2. Los ficheros o registros de población tendrán como finalidad la comunicación de los distintos órganos de cada administración pública con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico administrativas derivadas de las competencias respectivas de las Administraciones Públicas.

Tercera. Tratamiento de los expedientes de las derogadas Leyes de Vagos y Maleantes y de Peligrosidad y Rehabilitación Social.

Los expedientes específicamente instruidos al amparo de las derogadas Leyes de Vagos y Maleantes, y de Peligrosidad y Rehabilitación Social, que contengan datos de cualquier índole susceptibles de afectar a la seguridad, al honor, a la intimidad o a la imagen de las personas, no podrán ser consultados sin que medie consentimiento expreso de los afectados, o hayan transcurrido 50 años desde la fecha de aquéllos.

En este último supuesto, la Administración General del Estado, salvo que haya constancia expresa del fallecimiento de los afectados, pondrá a disposición del solicitante la documentación, suprimiendo de la misma los datos aludidos en el párrafo anterior, mediante la utilización de los procedimientos técnicos pertinentes en cada caso.

Cuarta. Modificación del artículo 112.4 de la Ley General Tributaria.

El apartado cuarto del artículo 112 de la Ley General Tributaria pasa a tener la siguiente redacción:

4. La cesión de aquellos datos de carácter personal, objeto de tratamiento que se debe efectuar a la Administración tributaria conforme a lo dispuesto en el artículo 111, en

los apartados anteriores de este artículo o en otra norma de rango legal, no requerirá el consentimiento del afectado.

Quinta . Competencias del Defensor del Pueblo y órganos autonómicos semejantes.

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.

Sexta. Modificación del artículo 24.3 de la Ley de Ordenación y Supervisión de los Seguros Privados.

Se modifica el artículo 24.3, párrafo 2º de la Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de los Seguros Privados con la siguiente redacción:

"Las entidades aseguradoras podrán establecer ficheros de datos de carácter personal que permitan la colaboración estadístico-actuarial y la prevención del fraude en la selección de riesgos y en la liquidación de siniestros. Estos últimos se regularán de conformidad con lo dispuesto en artículo 29 de la Ley Orgánica 5/1999, de13 de diciembre, de Protección de Datos de Carácter Personal,, por lo que será necesaria la notificación al afectado en la primera introducción de sus datos en el fichero pero no el consentimiento del mismo."

En todo caso, los datos relativos a la salud sólo podrán ser objeto de tratamiento con el consentimiento expreso del afectado".

Séptima. Modificación del Texto Refundido de la Ley del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 1/1995, de 24 de marzo.

1.Se modifica el artículo 4.2.c) del Texto Refundido de la Ley del Estatuto de los Trabajadores, quedando su redacción como sigue:

c) A no ser discriminados para el empleo, o una vez empleados, por razones de sexo, estado civil, por la edad dentro de los límites marcados por esta Ley, raza condición social, ideas religiosas o políticas, afiliación o no a un sindicato, así como por razón de lengua, dentro del Estado español. Tampoco podrán ser discriminados por razón de disminuciones físicas, psíquicas y sensoriales, siempre que se hallasen en condiciones de aptitud para desempeñar el trabajo o empleo de que se trate, ni por su herencia biológica.

Se añaden los apartados 4 y 5 al artículo 4 del Texto Refundido de la Ley del Estatuto de los Trabajadores, con la siguiente redacción:

"4. Asimismo, La utilización de aparatos audiovisuales de observación y vigilancia electrónica sobre los trabajadores en locales no abiertos al público del centro de trabajo, deberá ser puesta en conocimiento de éstos y sus representantes y, salvo pacto en contrario entre el empresario y los representantes de los trabajadores, sólo podrán ser utilizados para los fines de supervisión del rendimiento profesional o laboral siempre que

ello no se pudiera hacer con otros medios menos intimidatorios, y siempre que no se atente al contenido esencial del derecho a la intimidad, a la protección de datos y a la propia imagen.

5. Los trabajadores que utilicen instrumentos tecnológicos en el desarrollo de su trabajo, tendrán derecho a un uso moderado y proporcionado de éstos con fines personales cuando ello fuera necesario y siempre y cuando no afecte a su rendimiento profesional o laboral, al rendimiento económico de la empresa, sus recursos o su imagen. En estos casos, podrán preservar reservadamente sus datos, ficheros o correo de carácter personal en los correspondientes procedimientos informáticos que se desarrollen en su actividad laboral. Lo anterior no será de aplicación cuando haya fundadas necesidades organizativas o tecnológicas que lo impidan."

Octava. Modificaciones del Texto Articulado de la Ley de Funcionarios Civiles del Estado, aprobado por Decreto 315/1964, de 7 de febrero.

1. Se adiciona al párrafo segundo del apartado 1 del artículo 63 del Texto Articulado de la Ley de Funcionarios Civiles del Estado, la siguiente redacción:

"En aquellos supuestos en los que se exija el cumplimiento de determinadas condiciones o la superación de pruebas concretas al funcionario para el acceso o permanencia en el puesto de trabajo, se especificarán las pruebas psíquicas, físicas o de cualquier otro tipo que se le requieran, así como los exámenes médicos que el funcionario deberá pasar a tal fin.

Los resultados obtenidos en los análisis o pruebas legalmente autorizadas, deberán destinarse exclusivamente al fin para el cual prestó su consentimiento el funcionario.

Los datos obtenidos ilícitamente deberán ser destruidos de forma inmediata. Los acuerdos, valoraciones o resoluciones basadas en datos obtenidos ilícitamente serán nulos de pleno derecho."

2.Se añade un último párrafo al apartado 1 del artículo 63 del Texto Articulado de la Ley de Funcionarios Civiles del estado con la siguiente redacción:

"Los funcionarios tendrán derecho a no ser discriminados en su relación de empleo con la Administración Pública, por razones de sexo, estado civil, por la edad dentro de los límites marcados por la Ley, raza, condición social, ideas religiosas o políticas, afiliación o no a un sindicato, así como por razón de lengua, dentro del Estado español. Tampoco podrán ser discriminados por razón de disminuciones físicas, psíquicas y sensoriales, siempre que se hallasen en condiciones de aptitud para desempeñar el trabajo o empleo de que se trate, ni por herencia genética.

La utilización de aparatos audiovisuales de observación y vigilancia electrónica sobre los

funcionarios en el centro de trabajo, en locales no abiertos al público, deberá ser puesto en conocimiento de éstos y sus representantes, y, salvo pacto en contrario entre la Administración correspondiente y los representantes de los funcionarios, sólo podrán ser utilizados para los fines de supervisión del rendimiento profesional o laboral, siempre que no se atente al contenido esencial del derecho a la intimidad, a la protección de datos y a la propia imagen.

Los funcionarios que utilicen instrumentos tecnológicos en el desarrollo de su trabajo, tendrán derecho a un uso moderado y proporcionado de éstos con fines personales, en cuyo caso, y siempre y cuando no afecte a su rendimiento profesional, al rendimiento económico de la empresa, sus recursos o su imagen, podrán preservar reservadamente sus datos, ficheros o correo de carácter personal en los correspondientes procedimientos informáticos que se desarrollen en su actividad laboral. Lo anterior no será de aplicación cuando haya fundadas necesidades organizativas o tecnológicas que lo impidan."

Novena. Modificación de la Ley 31/1995, de 8 de noviembre de Prevención de Riesgos Laborales.

El apartado 4 del artículo 22 de la Ley 31/1995, de 8 de noviembre de Prevención de Riesgos Laborales, queda redactado de la siguiente forma:

"Los datos relativos a la vigilancia de la salud de los trabajadores no podrán ser usados con fines discriminatorios, ni en perjuicio del trabajador, ni podrán ser utilizados para fines distintos de aquellos para los cuales fueron solicitados u obtenidos, aun resultando compatibles con el mismo."

Décima. Modificación de la Ley Orgánica 11/1985, de 2 de Agosto, de Libertad Sindical, modificada por la Ley Orgánica 14/1994 y por la Ley 11/1994.

El apartado 3.2 del artículo 10 de la Ley Orgánica 11/1985, de 2 de agosto queda redactado de la siguiente forma:

Asistir a las reuniones de los comités de empresa y de los órganos internos de la empresa, o de los órganos de representación que se establezcan en las Administraciones Públicas, con voz pero sin voto, en materia de seguridad e higiene y en materia de vigilancia electrónica y Protección de Datos de carácter personal. Asimismo deberá informar a los trabajadores.

El apartado 3.3 del artículo 10 de la Ley Orgánica 11/1985, de 2 de agosto queda redactado de la siguiente forma:

Ser oídos por la empresa previamente a la adopción de medidas de carácter colectivo que afecten a los trabajadores en general y a los afiliados a su sindicato en particular, en esta u otras materias, especialmente en los despidos y sanciones de estos últimos.

DISPOSICIONES TRANSITORIAS

Primera. Tratamientos creados por Convenios Internacionales

La Agencia Española de Protección de Datos será el organismo competente para la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal respecto de los tratamientos establecidos en cualquier Convenio Internacional del que sea parte España que atribuya a una autoridad nacional de control esta competencia, mientras no se cree una autoridad diferente para este cometido en desarrollo del Convenio.

Segunda. (sin contenido)

Tercera. Subsistencia de normas preexistentes.

Hasta tanto se lleven a efecto las previsiones de la Disposición Final Primera de esta Ley, continuarán en vigor, con su propio rango, las normas reglamentarias existentes y, en especial, los Reales Decretos 428/1993, de 26 de marzo, 1332/1994, de 20 de junio y 994/1999, de 11 de junio, en cuanto no se opongan a la presente Ley.

DISPOSICIÓN DEROGATORIA

Única

Queda derogada la Ley Orgánica 15/1992, de 29 de octubre de regulación del tratamiento automatizado de los datos de carácter personal.

DISPOSICIONES FINALES

Primera. Habilitación para el desarrollo reglamentario

El Gobierno aprobará, o modificará, las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la presente Ley en el plazo máximo de un año a parir de la entrada en vigor de la ley.

Segunda. Preceptos con carácter de Ley Ordinaria

Los artículos 20 y 21 del título IV y los títulos VI excepto el último inciso del párrafo 4 del artículo 36 y VII de la presente Ley, la Disposición Adicional Cuarta, la Disposición Transitoria Primera y la Final Primera, tienen el carácter de Ley Ordinaria.

Tercera. Entrada en vigor

La presente Ley entrará en vigor en el plazo de un mes, contado desde su publicación en el Boletín Oficial del Estado.

Palacio del Congreso de los Diputados, a . .....

D. MANUEL MARÍN GONZALEZ
PRESIDENTE DEL CONGRESO
DE LOS DIPUTADOS

COMISIÓN DE LIBERTADES E INFORMÁTICA