

Se recomienda leer los materiales conjuntamente con el cuestionario correspondiente al tema para fijar la atención en las cuestiones de interés y hacer una lectura comprensiva.

También, materiales “Derecho y TICs”, Máster Oficial Sistemas y Servicios Sociedad de la Información www.uv.es/mastic

TEMA X

X. PRIVACIDAD Y PROTECCIÓN DE DATOS (I) GENERAL.....2

1. CONSTITUCIÓN Y CONVENIO EUROPEO	2
2. SENTENCIA 292/2000 DEL TRIBUNAL CONSTITUCIONAL SOBRE DERECHO A LA PROTECCIÓN DE DATOS PERSONALES.....	3
3. LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL (LOPD) CON EL REGLAMENTO RLOPD, REAL DECRETO 1720/2007, DE 21 DE DICIEMBRE.....	7
Ámbito, objeto y definiciones	8
Principios de la protección de datos, información y consentimiento.....	10
Datos especialmente protegidos	17
Cesión de datos, acceso por cuenta de tercero	18
Medidas de seguridad (ver Guía de seguridad de la AGPD, en “materiales”).....	22
Deber de secreto	26
Derechos de las personas (ver reglamento arts. 23 y ss.).....	26
Derecho de exclusión de las guías telefónicas	30
Ficheros privados, creación, etc.	31
Agencia de Protección de Datos	36
4. PROTECCIÓN DE DATOS EN LA LEY 32/2003, DE 3 DE NOVIEMBRE, GENERAL DE TELECOMUNICACIONES.....	43
<i>Derechos de abonados y usuarios de servicios de telecomunicaciones</i>	46
<i>Derechos de los destinatarios de servicios de comunicaciones electrónicas</i>	47

X. PRIVACIDAD Y PROTECCIÓN DE DATOS (I) GENERAL

1. Constitución y Convenio Europeo

Artículo 18

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Artículo 20

1. Se reconocen y protegen los derechos: a) A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción. b) A la producción y creación literaria, artística, científica y técnica. c) A la libertad de cátedra. d) A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades.

2. El ejercicio de estos derechos no puede restringirse mediante ningún tipo de censura previa.

3. La ley regulará la organización y el control parlamentario de los medios de comunicación social dependientes del Estado o de cualquier ente público y garantizará el acceso a dichos medios de los grupos sociales y políticos significativos, respetando el pluralismo de la sociedad y de las diversas lenguas de España.

4. Estas libertades tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia.

5. Sólo podrá acordarse el secuestro de publicaciones, grabaciones y otros medios de información en virtud de resolución judicial.

Convenio Para La Protección De Los Derechos Y De Las Libertades Fundamentales, Hecho En Roma El 4 De Noviembre De 1950

Artículo 8. Derecho al respeto a la vida privada y familiar.

1 Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

Artículo 11. Libertad de expresión y de información

1.- Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras.

2.- Se garantiza la libertad de los medios de comunicación y la libertad de información dentro del respeto del pluralismo y de la transparencia.

2. Sentencia 292/2000 del Tribunal Constitucional sobre derecho a la protección de datos personales

Lea y tenga en cuenta que se trata de una sentencia prácticamente "fundacional" y creativa de un derecho fundamental, el derecho de protección de datos. En este punto observe la diferencia para con el derecho a la intimidad y la definición y contenidos de este derecho.

En el recurso de inconstitucionalidad núm. 1463-2000, interpuesto por el Defensor del Pueblo, contra los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

II. Fundamentos jurídicos

1. El Defensor del Pueblo ha interpuesto el presente recurso de inconstitucionalidad contra ciertos incisos de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD, cuya Disposición final segunda les priva de la forma de Ley Orgánica) que, a su juicio, vulneran frontalmente la reserva de ley del art. 53.1 CE, el art. 18.1 y 4 CE, al no respetar el contenido esencial del derecho fundamental al honor y a la intimidad personal y familiar así como del derecho fundamental que este Tribunal ha denominado de "libertad informática" (SSTC 254/1993, de 20 de julio, 94/1998, de 4 de mayo, y 202/1999, de 8 de noviembre).

(resumen jurisprudencia precedente)

4. Sin necesidad de exponer con detalle las amplias posibilidades que la informática ofrece tanto para recoger como para comunicar datos personales ni los indudables riesgos que ello puede entrañar, dado que una persona puede ignorar no sólo cuáles son los datos que le conciernen que se hallan recogidos en un fichero sino también si han sido trasladados a otro y con qué finalidad, es suficiente indicar ambos extremos para comprender que el derecho fundamental a la intimidad (art. 18.1 CE) no aporte por sí sólo una protección suficiente frente a esta nueva realidad derivada del progreso tecnológico.

Ahora bien, con la inclusión del vigente art. 18.4 CE el constituyente puso de relieve que era consciente de los riesgos que podría entrañar el uso de la informática y encomendó al legislador la garantía tanto de ciertos derechos fundamentales como del pleno ejercicio de los derechos de la persona. Esto es, incorporando un instituto de garantía "como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona", pero que es también, "en sí mismo, un derecho o libertad fundamental" (STC 254/1993, de 20 de julio, FJ 6). Preocupación y

finalidad del constituyente que se evidencia, de un lado, si se tiene en cuenta que desde el anteproyecto del texto constitucional ya se incluía un apartado similar al vigente art. 18.4 CE y que éste fue luego ampliado al aceptarse una enmienda para que se incluyera su inciso final. Y más claramente, de otro lado, porque si en el debate en el Senado se suscitaron algunas dudas sobre la necesidad de este apartado del precepto dado el reconocimiento de los derechos a la intimidad y al honor en el apartado inicial, sin embargo fueron disipadas al ponerse de relieve que estos derechos, en atención a su contenido, no ofrecían garantías suficientes frente a las amenazas que el uso de la informática podía entrañar para la protección de la vida privada. De manera que el constituyente quiso garantizar mediante el actual art. 18.4 CE no sólo un ámbito de protección específico sino también más idóneo que el que podían ofrecer, por sí mismos, los derechos fundamentales mencionados en el apartado 1 del precepto.

5. El art. 18.4 CE fue esgrimido por primera vez en el caso de un ciudadano a quien le denegó el Gobierno Civil de Guipúzcoa información sobre los datos que sobre su persona poseía, resuelto por la STC 254/1993, de 20 de julio. Y lo dicho en esta pionera Sentencia se fue aquilatando en las posteriores, como la relativa a las normas reguladoras del número de identificación fiscal (STC 143/1994, de 9 de mayo), o la que declaró contrario a la libertad sindical (art. 28 CE), en relación con el art. 18.4 CE, el uso por una empresa del dato de la afiliación sindical para detraer haberes de los trabajadores con ocasión de una huelga promovida por determinado sindicato, STC 11/1998, de 13 de enero (cuya doctrina ha sido reiterada en una larga serie de Sentencias de este Tribunal resolviendo idéntica cuestión, y de entre las que merece destacarse la STC 94/1998, de 4 de mayo), o, finalmente y hasta la fecha, la STC 202/1999, de 8 de noviembre, en la que, con ocasión de la denegación a un trabajador de la cancelación de sus datos médicos en un fichero informatizado de una entidad de crédito sobre bajas por incapacidad temporal, se apreció que el almacenamiento sin cobertura legal en soporte informático de los diagnósticos médicos del trabajador sin mediar su consentimiento expreso constituía una desproporcionada restricción del derecho fundamental a la protección de datos personales.

Artículo 18, punto 1º y 4º afinidades y diferencias, el derecho autónomo del 18.4º

Primera peculiaridad del 4º respecto del 1º

Pues bien, en estas decisiones el Tribunal ya ha declarado que el art. 18.4 CE contiene, en los términos de la STC 254/1993, un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que, además, es en sí mismo "un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama 'la informática'", lo que se ha dado en llamar "libertad informática" (FJ 6, reiterado luego en las SSTC 143/1994, FJ 7, 11/1998, FJ 4, 94/1998, FJ 6, 202/1999, FJ 2). La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es así derecho a controlar el uso de los mismos datos insertos en un programa informático (*habeas data*) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos

personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, FJ 5, 94/1998, FJ 4).

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). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran.

6. La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, FJ 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal (SSTC 134/1999, de 15 de julio, FJ 5; 144/1999, FJ 8; 98/2000, de 10 de abril, FJ 5; 115/2000, de 10 de mayo, FJ 4), es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin.

De ahí la singularidad del derecho a la protección de datos, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal (STC 170/1987, de 30 de octubre, FJ 4), como el derecho al honor, citado expresamente en el art. 18.4 CE, e igualmente, en expresión bien amplia del propio art. 18.4 CE, al pleno ejercicio de los derechos de la persona. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado.

De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato

personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo.

Segunda peculiaridad

Pero también el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 CE. Dicha peculiaridad radica en su contenido, ya que a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido (SSTC 73/1982, de 2 de diciembre, FJ 5; 110/1984, de 26 de noviembre, FJ 3; 89/1987, de 3 de junio, FJ 3; 231/1988, de 2 de diciembre, FJ 3; 197/1991, de 17 de octubre, FJ 3, y en general las SSTC 134/1999, de 15 de julio, 144/1999, de 22 de julio, y 115/2000, de 10 de mayo), el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales (STC 254/1993, FJ 7).

7. De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

En fin, 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.

8. Estas conclusiones sobre el significado y el contenido el derecho a la protección de datos personales se corroboran, atendiendo al mandato del art. 10.2 CE, por lo dispuesto en los instrumentos internacionales que se refieren a dicho derecho fundamental. Como es el caso de la Resolución 45/95 de la Asamblea General de las Naciones Unidas donde se recoge la versión revisada de los Principios Rectores aplicables a los Ficheros Computadorizados de Datos Personales. En el ámbito europeo, del Convenio para la Protección de las Personas respecto al Tratamiento Automatizado de Datos de Carácter Personal hecho en Estrasburgo el 28 de enero de 1981, del que hemos dicho en la STC 254/1993, FJ 4, que no se limita "a establecer los principios básicos para la protección de los datos tratados automáticamente, especialmente en sus arts. 5, 6, 7 y 11", sino que los completa "con unas garantías para las personas concernidas, que formula detalladamente su art. 8", al que han seguido diversas recomendaciones de la Asamblea del Consejo de Europa.

Por último, otro tanto ocurre en el ámbito comunitario, con la Directiva 95/46, sobre Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y la Libre Circulación de estos datos, así como con la Carta de Derechos Fundamentales de la Unión Europea del presente año, cuyo art. 8 reconoce este derecho, precisa su contenido y establece la necesidad de una autoridad que vele por su respeto. Pues todos estos textos internacionales coinciden en el establecimiento de un régimen jurídico para la protección de datos personales en el que se regula el ejercicio de este derecho fundamental en cuanto a la recogida de tales datos, la información de los interesados sobre su origen y destino, la facultad de rectificación y cancelación, así como el consentimiento respecto para su uso o cesión. Esto es, como antes se ha visto, un haz de garantías cuyo contenido hace posible el respeto de este derecho fundamental...

3. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) con el reglamento RLOPD, Real Decreto 1720/2007, de 21 de diciembre

LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

Texto conjunto con extractos del *Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal*, según materias (distinto tipo de letra y cursiva).

LOPD

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

Título II. Principios de la protección de datos. (arts.4-12)

Título III. Derechos de las personas (arts.13-19)

Título IV. Disposiciones sectoriales

Capítulo I. Ficheros de titularidad pública (arts.20-24)

Capítulo I. Ficheros de titularidad privada (arts.25-32)

Título V. Movimiento internacional de datos (arts.33-34)

Título VI. Agencia de protección de datos (arts.35-42)

Título VII. Infracciones y sanciones (arts.43-49)

Disposiciones adicionales

Ámbito, objeto y definiciones

TÍTULO I

Disposiciones generales

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.

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.

c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del

fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.

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

- 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.

Reglamento

Artículo 2. Ámbito objetivo de aplicación.

1. *El presente reglamento 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.*

2. *Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.*

3. *Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal.*

4. *Este reglamento no será de aplicación a los datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos.*

Artículo 4. Ficheros o tratamientos excluidos.

El régimen de protección de los datos de carácter personal que se establece en el presente reglamento no será de aplicación a los siguientes ficheros y tratamientos:

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

Sólo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares.

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

c) A los establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos.

Ley

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.

f) Procedimiento de disociación: todo tratamiento de datos personales 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, sólo o conjuntamente con otros, trate datos personales 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 personales que le conciernen.

i) Cesión o comunicación de datos: toda revelación de datos 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, el censo promocional, 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.

Principios de la protección de datos, información y consentimiento

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 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.

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.

Reglamento 2008

Artículo 8. Principios relativos a la calidad de los datos.

1. Los datos de carácter personal deberán ser tratados de forma leal y lícita. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

2. Los datos de carácter personal sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento.

3. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

4. Sólo podrán ser objeto de tratamiento los datos que sean adecuados, pertinentes y no excesivos en relación con las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

5. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste.

Si los datos de carácter personal sometidos a tratamiento resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados en el plazo de diez días desde que se tuviese conocimiento de la inexactitud, salvo que la legislación aplicable al fichero establezca un procedimiento o un plazo específico para ello.

Cuando los datos hubieran sido comunicados previamente, el responsable del fichero o tratamiento deberá notificar al cesionario, en el plazo de diez días, la rectificación o cancelación efectuada, siempre que el cesionario sea conocido.

En el plazo de diez días desde la recepción de la notificación, el cesionario que mantuviera el tratamiento de los datos, deberá proceder a la rectificación y cancelación notificada.

Esta actualización de los datos de carácter personal no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre.

Lo dispuesto en este apartado se entiende sin perjuicio de las facultades que a los afectados reconoce el título III de este reglamento.

6. 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 obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado.

Una vez cumplido el período al que se refieren los párrafos anteriores, los datos sólo podrán ser conservados previa disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

7. Los datos de carácter personal serán tratados de forma que permitan el ejercicio del derecho de acceso, en tanto no proceda su cancelación.

Ley

Artículo 5. Derecho de información en la recogida de datos.

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

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

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

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

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

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

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, 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 personales 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, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia 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 anterior 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.

Reglamento

Sección 2.ª Deber de información al interesado

Artículo 18. Acreditación del cumplimiento del deber de información.

1. El deber de información al que se refiere el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado.

2. El responsable del fichero o tratamiento deberá conservar el soporte en el que conste el cumplimiento del deber de informar. Para el almacenamiento de los soportes, el responsable del fichero o tratamiento podrá utilizar medios informáticos o telemáticos. En particular podrá proceder al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales.

Ley

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.

Reglamento

Artículo 10. Supuestos que legitiman el tratamiento o cesión de los datos.

1. Los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello.

2. No obstante, será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando:

a) Lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes:

El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre.

El tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas.

b) Los datos objeto de tratamiento o de cesión figuren en fuentes accesibles al público y el responsable del fichero, o el tercero a quien se comuniquen los datos, tenga un interés legítimo para su tratamiento o conocimiento, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

No obstante, las Administraciones públicas sólo podrán comunicar al amparo de este apartado los datos recogidos de fuentes accesibles al público a responsables de ficheros de titularidad privada cuando se encuentren autorizadas para ello por una norma con rango de ley.

3. Los datos de carácter personal podrán tratarse sin necesidad del consentimiento del interesado cuando:

a) Se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de las competencias que les atribuya una norma con rango de ley o una norma de derecho comunitario.

b) Se recaben por el responsable del tratamiento con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento.

c) El tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del apartado 6 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre.

(resto de este artículo en comunicación de datos art. 11 Ley)

Reglamento, sobre el consentimiento

Sección 1.ª Obtención del consentimiento del afectado

Artículo 12. Principios generales.

1. El responsable del tratamiento deberá obtener el consentimiento del interesado para el tratamiento de sus datos de carácter personal salvo en aquellos supuestos en que el mismo no sea exigible con arreglo a lo dispuesto en las leyes.

La solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamientos.

2. Cuando se solicite el consentimiento del afectado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario. En caso contrario, el consentimiento será nulo.

3. Corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho.

Artículo 13. Consentimiento para el tratamiento de datos de menores de edad.

1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.

3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.

4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales.

Artículo 14. Forma de recabar el consentimiento.

1. El responsable del tratamiento podrá solicitar el consentimiento del interesado a través del procedimiento establecido en este artículo, salvo cuando la Ley exija al mismo la obtención del consentimiento expreso para el tratamiento de los datos.

2. El responsable podrá dirigirse al afectado, informándole en los términos previstos en los artículos 5 de la Ley Orgánica 15/1999, de 13 de diciembre y 12.2 de este reglamento y deberá concederle un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal.

En particular, cuando se trate de responsables que presten al afectado un servicio que genere información periódica o reiterada, o facturación periódica, la comunicación podrá llevarse a cabo de forma conjunta a esta información o a la facturación del servicio prestado, siempre que se realice de forma claramente visible.

3. En todo caso, será necesario que el responsable del tratamiento pueda conocer si la comunicación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

4. Deberá facilitarse al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos. En particular, se considerará ajustado al presente reglamento los procedimientos en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento, la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

5. Cuando se solicite el consentimiento del interesado a través del procedimiento establecido en este artículo, no será posible solicitarlo nuevamente respecto de los mismos tratamientos y para las mismas finalidades en el plazo de un año a contar de la fecha de la anterior solicitud.

Artículo 15. Solicitud del consentimiento en el marco de una relación contractual para fines no relacionados directamente con la misma.

Si el responsable del tratamiento solicitase el consentimiento del afectado durante el proceso de formación de un contrato para finalidades que no guarden relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al afectado que manifieste expresamente su negativa al tratamiento o comunicación de datos.

En particular, se entenderá cumplido tal deber cuando se permita al afectado la marcación de una casilla claramente visible y que no se encuentre ya marcada en el documento que se le entregue para la celebración del contrato o se establezca un procedimiento equivalente que le permita manifestar su negativa al tratamiento.

Artículo 16. Tratamiento de datos de facturación y tráfico en servicios de comunicaciones electrónicas.

La solicitud del consentimiento para el tratamiento o cesión de los datos de tráfico, facturación y localización por parte de los sujetos obligados, o en su caso la revocación de aquél, según la legislación reguladora de las telecomunicaciones se someterá a lo establecido en su normativa específica y, en lo que no resulte contrario a la misma, a lo establecido en la presente sección.

Artículo 17. Revocación del consentimiento.

1. El afectado podrá revocar su consentimiento a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento. En particular, se considerará ajustado al presente reglamento el procedimiento en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento o la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, los supuestos en que el responsable establezca como medio para que el interesado pueda manifestar su negativa al tratamiento el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste adicional al interesado.

2. El responsable cesará en el tratamiento de los datos en el plazo máximo de diez días a contar desde el de la recepción de la revocación del consentimiento, sin perjuicio de su obligación de bloquear los datos conforme a lo dispuesto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre.

3. Cuando el interesado hubiera solicitado del responsable del tratamiento la confirmación del cese en el tratamiento de sus datos, éste deberá responder expresamente a la solicitud.

4. Si los datos hubieran sido cedidos previamente, el responsable del tratamiento, una vez revocado el consentimiento, deberá comunicarlo a los cesionarios, en el plazo previsto en el apartado 2, para que éstos, cesen en el tratamiento de los datos en caso de que aún lo mantuvieran, conforme al artículo 16.4 de la Ley Orgánica 15/1999, de 13 de diciembre.

Datos especialmente protegidos

Ley

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.

6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, 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. También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea 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.

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.

Cesión de datos, acceso por cuenta de tercero

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 de los datos con fines históricos, estadísticos o científicos.

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.

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 aquel a quien se pretenden comunicar.

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

5. Aquel 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.

Reglamento

4. *Será posible la cesión de los datos de carácter personal sin contar con el consentimiento del interesado cuando:*

a) *La cesión responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de los datos. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.*

b) *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 o a las instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas y se realice en el ámbito de las funciones que la ley les atribuya expresamente.*

c) *La cesión entre Administraciones públicas cuando concurra uno de los siguientes supuestos:*

Tenga por objeto el tratamiento de los datos con fines históricos, estadísticos o científicos.

Los datos de carácter personal hayan sido recogidos o elaborados por una Administración pública con destino a otra.

La comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias.

5. *Los datos especialmente protegidos podrán tratarse y cederse en los términos previstos en los artículos 7 y 8 de la Ley Orgánica 15/1999, de 13 de diciembre.*

En particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

Artículo 19. Supuestos especiales.

En los supuestos en que se produzca una modificación del responsable del fichero como consecuencia de una operación de fusión, escisión, cesión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial, o cualquier operación de reestructuración societaria de análoga naturaleza, contemplada por la normativa mercantil, no se producirá cesión de datos, sin perjuicio del cumplimiento por el responsable de lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre.

Ley

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.

Reglamento

Artículo 20. Relaciones entre el responsable y el encargado del tratamiento.

1. *El acceso a los datos por parte de un encargado del tratamiento que resulte necesario para la prestación de un servicio al responsable no se considerará comunicación de datos, siempre y cuando se cumpla lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente capítulo.*

El servicio prestado por el encargado del tratamiento podrá tener o no carácter remunerado y ser temporal o indefinido.

No obstante, se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado.

2. *Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento.*

3. *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 al*

que se refiere el apartado 2 del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo.

Artículo 21. Posibilidad de subcontratación de los servicios.

1. El encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento.

2. No obstante lo dispuesto en el apartado anterior, será posible la subcontratación sin necesidad de autorización siempre y cuando se cumplan los siguientes requisitos:

a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar.

Cuando no se identifique en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.

b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

c) Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior.

En este caso, el subcontratista será considerado encargado del tratamiento, siéndole de aplicación lo previsto en el artículo 20.3 de este reglamento.

3. Si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del tratamiento los extremos señalados en el apartado anterior.

Artículo 22. Conservación de los datos por el encargado del tratamiento.

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

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.

2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

Medidas de seguridad (ver Guía de seguridad de la AGPD, en "materiales")

Ley

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.

Reglamento

TÍTULO VIII De las medidas de seguridad en el tratamiento de datos de carácter personal

Capítulo I Disposiciones generales

Artículo 79. Alcance.

Los responsables de los tratamientos o los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en este Título, con independencia de cual sea su sistema de tratamiento.

Artículo 80. Niveles de seguridad.

Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.

Artículo 81. Aplicación de los niveles de seguridad.

1. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los relativos a la comisión de infracciones administrativas o penales.

b) Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre.

c) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.

d) Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

e) Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

f) Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.

c) Aquéllos que contengan datos derivados de actos de violencia de género.

4. A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento.

5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.

b) Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesorio se contengan aquellos datos sin guardar relación con su finalidad.

6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

7. Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

8. A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.

Artículo 83. Prestaciones de servicios sin acceso a datos personales.

El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

Artículo 85. Acceso a datos a través de redes de comunicaciones.

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 80.

Artículo 86. Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.

1. Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

2. La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.

Artículo 87. Ficheros temporales o copias de trabajo de documentos.

1. Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda conforme a los criterios establecidos en el artículo 81.

2. Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

Tener en cuenta el articulado y para profundizar, ver Guía AGPD

Capítulo III Medidas de seguridad aplicables a ficheros y tratamientos automatizados

Sección 1.ª Medidas de seguridad de nivel básico

Artículo 89. Funciones y obligaciones del personal.

Artículo 90. Registro de incidencias.

Artículo 91. Control de acceso.

Artículo 92. Gestión de soportes y documentos.

Artículo 93. Identificación y autenticación.

Artículo 94. Copias de respaldo y recuperación.

Sección 2.ª Medidas de seguridad de nivel medio

Artículo 95. Responsable de seguridad.

Artículo 96. Auditoría.

Artículo 97. Gestión de soportes y documentos.

Artículo 98. Identificación y autenticación.

Artículo 99. Control de acceso físico.

Artículo 100. Registro de incidencias.

Sección 3.ª Medidas de seguridad de nivel alto

Artículo 101. Gestión y distribución de soportes.

Artículo 102. Copias de respaldo y recuperación.

Artículo 103. Registro de accesos.

Artículo 104. Telecomunicaciones.

Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Capítulo IV Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados

Sección 1.ª Medidas de seguridad de nivel básico

Artículo 105. Obligaciones comunes.

1. Además de lo dispuesto en el presente capítulo, a los ficheros no automatizados les será de aplicación lo dispuesto en los capítulos I y II del presente título en lo relativo a:

- a) Alcance.*
- b) Niveles de seguridad.*
- c) Encargado del tratamiento.*
- d) Prestaciones de servicios sin acceso a datos personales.*
- e) Delegación de autorizaciones.*
- f) Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.*
- g) Copias de trabajo de documentos.*
- h) Documento de seguridad.*

2. Asimismo se les aplicará lo establecido por la sección primera del capítulo III del presente título en lo relativo a:

- a) Funciones y obligaciones del personal.*
- b) Registro de incidencias.*
- c) Control de acceso.*
- d) Gestión de soportes.*

Artículo 106. Criterios de archivo.

Artículo 107. Dispositivos de almacenamiento.

Artículo 108. Custodia de los soportes.

Artículo 109. Responsable de seguridad.

Artículo 110. Auditoría.

Sección 3.ª Medidas de seguridad de nivel alto

Artículo 111. Almacenamiento de la información.

Artículo 112. Copia o reproducción.

Artículo 113. Acceso a la documentación.

Artículo 114. Traslado de documentación.

Ley

Deber de secreto

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.

Comentario ley: El incumplimiento del deber de secreto puede ser constitutivo de una sanción leve, en los términos del artículo 44.2.e), o de infracción grave de acuerdo con lo previsto en el artículo 44.3.g) en virtud del cual, '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.'

La vulneración del deber de guardar secreto sobre los datos de carácter personal especialmente protegidos a que hacen referencia los apartados 2 y 3 del artículo 7, así como de aquellos que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas, puede ser constitutivo de una sanción muy grave en los términos del artículo 44.4.g) de la Ley Orgánica 15/1999.

Derechos de las personas (ver reglamento arts. 23 y ss.)

Elementos generales (reglamento)

Artículo 23. Carácter personalísimo.

1. Los derechos de acceso, rectificación, cancelación y oposición son personalísimos y serán ejercidos por el afectado.

2. Tales derechos se ejercitarán:

a) Por el afectado, acreditando su identidad, del modo previsto en el artículo siguiente.

b) Cuando el afectado se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de estos derechos, podrán ejercitarse por su representante legal, en cuyo caso será necesario que acredite tal condición.

c) Los derechos también podrán ejercitarse a través de representante voluntario, expresamente designado para el ejercicio del derecho. En ese caso, deberá constar claramente acreditada la identidad del representado, mediante la aportación de copia

de su Documento Nacional de Identidad o documento equivalente, y la representación conferida por aquél.

Cuando el responsable del fichero sea un órgano de las Administraciones públicas o de la Administración de Justicia, podrá acreditarse la representación por cualquier medio válido en derecho que deje constancia fidedigna, o mediante declaración en comparecencia personal del interesado.

3. Los derechos serán denegados cuando la solicitud sea formulada por persona distinta del afectado y no se acredite que la misma actúa en representación de aquél.

Artículo 24. Condiciones generales para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

1. Los derechos de acceso, rectificación, cancelación y oposición son derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

2. Deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

3. El ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición será gratuito y en ningún caso podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar sus derechos el envío de cartas certificadas o semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.

4. Cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, podrá concederse la posibilidad al afectado de ejercer sus derechos de acceso, rectificación, cancelación y oposición a través de dichos servicios. En tal caso, la identidad del interesado se considerará acreditada por los medios establecidos para la identificación de los clientes del responsable en la prestación de sus servicios o contratación de sus productos.

5. El responsable del fichero o tratamiento deberá atender la solicitud de acceso, rectificación, cancelación u oposición ejercida por el afectado aún cuando el mismo no hubiese utilizado el procedimiento establecido específicamente al efecto por aquél, siempre que el interesado haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud, y que ésta contenga los elementos referidos en el párrafo 1 del artículo siguiente.

Ley

TÍTULO III

Derechos de las personas

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 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.

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 podrán ejercitarlo antes.

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.

2. Serán rectificadas 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 o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la 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 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.

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.

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.

Derecho de oposición y su desarrollo reglamentario

Ley

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 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.

Reglamento

Artículo 34. Derecho de oposición.

El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos:

a) Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.

b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, en los términos previstos en el artículo 51 de este reglamento, cualquiera que sea la empresa responsable de su creación.

c) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el artículo 36 de este reglamento.

Artículo 35. Ejercicio del derecho de oposición.

1. El derecho de oposición se ejercitará mediante solicitud dirigida al responsable del tratamiento.

Cuando la oposición se realice con base en la letra a) del artículo anterior, en la solicitud deberán hacerse constar los motivos fundados y legítimos, relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho.

Artículo 36. Derecho de oposición a las decisiones basadas únicamente en un tratamiento automatizado de datos.

1. Los interesados 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 automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta.

2. No obstante, los afectados podrán verse sometidos a una de las decisiones contempladas en el apartado 1 cuando dicha decisión:

a) Se haya adoptado en el marco de la celebración o ejecución de un contrato a petición del interesado, siempre que se le otorgue la posibilidad de alegar lo que estimara pertinente, a fin de defender su derecho o interés. En todo caso, el responsable del fichero deberá informar previamente al afectado, de forma clara y precisa, de que se adoptarán decisiones con las características señaladas en el apartado 1 y cancelará los datos en caso de que no llegue a celebrarse finalmente el contrato.

b) Esté autorizada por una norma con rango de Ley que establezca medidas que garanticen el interés legítimo del interesado.

Derecho de exclusión de las guías telefónicas

De conformidad con el artículo 3.j de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, los datos telefónicos básicos que figuran en los repertorios telefónicos (tanto en papel como en soporte electrónico), constituyen una fuente que se considera como accesible al público, pudiéndose recabar tales datos sin el consentimiento expreso del interesado.

Concretamente, en los repertorios de abonados de servicios telefónicos, ya sean impresos en papel o disponibles por otros medios (Páginas blancas, CD-ROM, etc...), aparecen el nombre y apellidos así como la dirección y, salvo que Vd. se manifieste en sentido contrario exigiendo su exclusión, sus datos pueden ser consultados y utilizados por el público en general. La exclusión debe hacerse efectiva, en las guías formato papel, con la siguiente edición y, en las guías electrónicas, en el plazo de 10 días.

Frente a esta situación, y si no se quiere que los datos sean de dominio público, sería conveniente proceder a solicitar, con carácter preventivo, que se proceda gratuitamente a la exclusión total o parcial de los datos relativos a su persona que se encuentren en los repertorios telefónicos de abonados, de conformidad con lo establecido en el artículo 28 de la Ley Orgánica 15/1999 y en el artículo 67 del Reglamento por el que se desarrolla el Título III de la Ley General de

Telecomunicaciones (Real Decreto 1736/1998), porque de otro modo sus datos seguirán utilizándose legalmente sin su consentimiento.

Ficheros privados, creación, etc.

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 de Protección de Datos.

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

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

4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles. En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

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

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 personales que figuren en el censo promocional, o 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 personales no pueden utilizarse para fines de publicidad o prospección comercial. Los interesados tendrán derecho a exigir gratuitamente la exclusión de la totalidad de sus datos personales que consten en el censo promocional por las entidades encargadas del mantenimiento de dichas fuentes. 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 telemática 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 telemáticamente 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.

4. Los datos que figuren en las guías de servicios de telecomunicaciones disponibles al público se registrarán por su normativa específica.

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 acreedor 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, 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.

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.

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.

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 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 de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas.

RLOPD Creación y registro de ficheros

Artículo 55. Notificación de ficheros.

1. Todo fichero de datos de carácter personal de titularidad pública será notificado a la Agencia Española de Protección de Datos por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, en el plazo de treinta días desde la publicación de su norma o acuerdo de creación en el diario oficial correspondiente.

2. Los ficheros de datos de carácter personal de titularidad privada serán notificados a la Agencia Española de Protección de Datos por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación. La notificación deberá indicar la identificación del responsable del fichero, la identificación del fichero, sus finalidades y los usos previstos, el sistema de tratamiento empleado en su organización,

el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, la indicación del nivel de medidas de seguridad básico, medio o alto exigible, y en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales de datos.

3. Cuando la obligación de notificar afecte a ficheros sujetos a la competencia de la autoridad de control de una comunidad autónoma que haya creado su propio registro de ficheros, la notificación se realizará a la autoridad autonómica competente, que dará traslado de la inscripción al Registro General de Protección de Datos.

El Registro General de Protección de Datos podrá solicitar de las autoridades de control de las comunidades autónomas el traslado al que se refiere el párrafo anterior, procediendo, en su defecto, a la inclusión de oficio del fichero en el Registro.

4. La notificación se realizará conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento.

Artículo 56. Tratamiento de datos en distintos soportes.

1. La notificación de un fichero de datos de carácter personal es independiente del sistema de tratamiento empleado en su organización y del soporte o soportes empleados para el tratamiento de los datos.

2. Cuando los datos de carácter personal objeto de un tratamiento estén almacenados en diferentes soportes, automatizados y no automatizados o exista una copia en soporte no automatizado de un fichero automatizado sólo será precisa una sola notificación, referida a dicho fichero.

Artículo 57. Ficheros en los que exista más de un responsable.

Cuando se tenga previsto crear un fichero del que resulten responsables varias personas o entidades simultáneamente, cada una de ellas deberá notificar, a fin de proceder a su inscripción en el Registro General de Protección de Datos y, en su caso, en los Registros de Ficheros creados por las autoridades de control de las comunidades autónomas, la creación del correspondiente fichero.

Artículo 58. Notificación de la modificación o supresión de ficheros.

1. La inscripción del fichero deberá encontrarse actualizada en todo momento. Cualquier modificación que afecte al contenido de la inscripción de un fichero deberá ser previamente notificada a la Agencia Española de Protección de Datos o a las autoridades de control autonómicas competentes, a fin de proceder a su inscripción en el registro correspondiente, conforme a lo dispuesto en el artículo 55.

2. Cuando el responsable del fichero decida su supresión, deberá notificarla a efectos de que se proceda a la cancelación de la inscripción en el registro correspondiente.

3. Tratándose de ficheros de titularidad pública, cuando se pretenda la modificación que afecte a alguno de los requisitos previstos en el artículo 55 o la supresión del fichero deberá haberse adoptado, con carácter previo a la notificación la correspondiente norma o acuerdo en los términos previstos en el capítulo I de este título.

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 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 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, la 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 médicos, la prestación de asistencia sanitaria o tratamiento médicos 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 aquella 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 de Protección de Datos

Artículo 35. Naturaleza y régimen jurídico.

1. La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno.

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 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 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 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 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 de Protección de Datos dirige la Agencia y ostenta su representación. Será nombrado, de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un período de cuatro años.

2. Ejercerá sus funciones con plena independencia y objetividad y no estará sujeto a instrucción alguna en el desempeño de aquéllas. En todo caso, el Director deberá oír al Consejo Consultivo en aquellas propuestas que éste le realice en el ejercicio de sus funciones.

3. El Director de la Agencia de Protección de Datos sólo cesará antes de la expiración del período a que se refiere el apartado 1, a petición propia o por separación acordada por el Gobierno, previa instrucción de expediente, en el que necesariamente serán oídos los restantes miembros del Consejo Consultivo, por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso.

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

Artículo 37. Funciones.

1. Son funciones de la Agencia de Protección de Datos:

a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

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

c) Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos 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 al Ministerio de Justicia.

l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46.

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

2. *Añadido por Ley 62/2003, de 30 de diciembre.* 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.

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.

Artículo 39. El Registro General de Protección de Datos.

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

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

a) Los ficheros 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 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 de Protección de Datos podrá 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.

Artículo 42. Ficheros de las Comunidades Autónomas en materia de su exclusiva competencia.

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

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 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 Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos.

1) 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.

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 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 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 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.

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 de Protección de Datos dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

2. El Director de la Agencia podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones públicas.

3. Se deberán comunicar a la Agencia las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

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

Artículo 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 adquiriera 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 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 de Protección de Datos podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido, la Agencia de Protección de Datos podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas.

...

4. Protección de datos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones

extracto

CAPÍTULO III.

Secreto de las comunicaciones y protección de los datos personales y derechos y obligaciones de carácter público vinculados con las redes y servicios de comunicaciones electrónicas.

Artículo 33. Secreto de las comunicaciones.

VER NUEVA REDACCIÓN EN COMENTARIO SOBRE NUEVA LEY 25/2007

Artículo 34. Protección de los datos de carácter personal.

Sin perjuicio de lo previsto en el apartado 6 del artículo 4 y en el segundo párrafo del artículo anterior, así como en la restante normativa específica aplicable, los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar, en

el ejercicio de su actividad, la protección de los datos de carácter personal conforme a la legislación vigente.

Los operadores a los que se refiere el párrafo anterior deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar los niveles de protección de los datos de carácter personal que sean exigidos por la normativa de desarrollo de esta Ley en esta materia. En caso de que exista un riesgo particular de violación de la seguridad de la red pública de comunicaciones electrónicas, el operador que explote dicha red o preste el servicio de comunicaciones electrónicas informará a los abonados sobre dicho riesgo y sobre las medidas a adoptar.

Artículo 35. Interceptación de las comunicaciones electrónicas por los servicios técnicos. (NO REFORMADO POR LEY 25/2007)

1. Con pleno respeto al derecho al secreto de las comunicaciones y a la exigencia, conforme a lo establecido en la Ley de Enjuiciamiento Criminal, de autorización judicial para la interceptación de contenidos, cuando para la realización de las tareas de control para la eficaz utilización del dominio público radioeléctrico sea necesaria la utilización de equipos, infraestructuras e instalaciones técnicas de interceptación de señales no dirigidas al público en general, será de aplicación lo siguiente:

a. La Administración de las telecomunicaciones deberá diseñar y establecer sus sistemas técnicos de interceptación de señales en forma tal que se reduzca al mínimo el riesgo de afectar a los contenidos de las comunicaciones.

b. Cuando, como consecuencia de las interceptaciones técnicas efectuadas, quede constancia de los contenidos, los soportes en los que éstos aparezcan no podrán ser ni almacenados ni divulgados y serán inmediatamente destruidos.

2. Las mismas reglas se aplicarán para la vigilancia del adecuado empleo de las redes y la correcta prestación de los servicios de comunicaciones electrónicas.

3. Lo establecido en este artículo se entiende sin perjuicio de las facultades que a la Administración atribuye el artículo 43.2.

Artículo 36. Cifrado en las redes y servicios de comunicaciones electrónicas.

1. Cualquier tipo de información que se transmita por redes de comunicaciones electrónicas podrá ser protegida mediante procedimientos de cifrado.

2. El cifrado es un instrumento de seguridad de la información. Entre sus condiciones de uso, cuando se utilice para proteger la confidencialidad de la información, se podrá imponer la obligación de facilitar a un órgano de la Administración General del Estado o a un organismo público, los algoritmos o cualquier procedimiento de cifrado utilizado, así como la obligación de facilitar sin

coste alguno los aparatos de cifra a efectos de su control de acuerdo con la normativa vigente.

Artículo 38. Derechos de los consumidores y usuarios finales.[...]

3. En particular, los abonados a los servicios de comunicaciones electrónicas tendrán los siguientes derechos:

a. A que se hagan anónimos o se cancelen sus datos de tráfico cuando ya no sean necesarios a los efectos de la transmisión de una comunicación. Los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones podrán ser tratados únicamente hasta que haya expirado el plazo para la impugnación de la factura del servicio o para que el operador pueda exigir su pago.

b. A que sus datos de tráfico sean utilizados con fines comerciales o para la prestación de servicios de valor añadido únicamente cuando hubieran prestado su consentimiento informado para ello.

c. A recibir facturas no desglosadas cuando así lo solicitasen.

d. A que sólo se proceda al tratamiento de sus datos de localización distintos a los datos de tráfico cuando se hayan hecho anónimos o previo su consentimiento informado y únicamente en la medida y por el tiempo necesarios para la prestación, en su caso, de servicios de valor añadido, con conocimiento inequívoco de los datos que vayan a ser sometidos a tratamiento, la finalidad y duración del mismo y el servicio de valor añadido que vaya a ser prestado.

e. A detener el desvío automático de llamadas efectuado a su terminal por parte de un tercero.

f. A impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de su línea en las llamadas que genere o la presentación de la identificación de su línea al usuario que le realice una llamada.

g. A impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de la línea de origen en las llamadas entrantes y a rechazar las llamadas entrantes en que dicha línea no aparezca identificada.

h. A no recibir llamadas automáticas sin intervención humana o mensajes de fax, con fines de venta directa sin haber prestado su consentimiento previo e informado para ello.

4. Los usuarios de los servicios de comunicaciones electrónicas que no tengan la condición de abonados tendrán asimismo los derechos reconocidos en los párrafos a, b, d y en el primer inciso del párrafo f del apartado anterior.

5. Los usuarios finales no podrán ejercer los derechos reconocidos en los párrafos d y f del apartado 3 cuando se trate de llamadas efectuadas a entidades que presten servicios de llamadas de urgencia que se determinen reglamentariamente, en especial a través del número 112.

Del mismo modo, y por un período de tiempo limitado, los usuarios finales no podrán ejercer el derecho reconocido en el párrafo f del apartado 3 cuando el abonado a la línea de destino haya solicitado la identificación de las llamadas maliciosas o molestas realizadas a su línea.

Reformado: «Lo establecido en las letras a) y d) del apartado 3 de este artículo se entiende sin perjuicio de las obligaciones establecidas en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.»

6. La elaboración y comercialización de las guías de abonados a los servicios de comunicaciones electrónicas y la prestación de los servicios de información sobre ellos se realizará en régimen de libre competencia, garantizándose, en todo caso, a los abonados el derecho a la protección de sus datos personales, incluyendo el de no figurar en dichas guías. A tal efecto, las empresas que asignen números de teléfono a los abonados habrán de dar curso a todas las solicitudes razonables de suministro de información pertinente para la prestación de los servicios de información sobre números de abonados y guías accesibles al público, en un formato aprobado y en unas condiciones equitativas, objetivas, orientadas en función de los costes y no discriminatorias, estando sometido el suministro de la citada información y su posterior utilización a la normativa en materia de protección de datos vigente en cada momento.

7. El Ministerio de Ciencia y Tecnología podrá introducir cláusulas de modificación de los contratos celebrados entre los operadores y los consumidores que sean personas físicas y usuarios finales, para evitar el trato abusivo a éstos.

8. Lo establecido en este artículo se entiende sin perjuicio de la aplicación de la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios.

Derechos de abonados y usuarios de servicios de telecomunicaciones

Según dispone el art. 38.3 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, los abonados y los usuarios a los servicios de telecomunicaciones, tienen los siguientes derechos:

- A que se hagan anónimos o se cancelen sus datos de tráfico cuando ya no sean necesarios a los efectos de la transmisión de una comunicación. Los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones podrán ser tratados únicamente hasta que haya expirado el plazo para la impugnación de la factura del servicio o para que el operador pueda exigir su pago.

- A que sus datos de tráfico sean utilizados con fines comerciales o para la prestación de servicios de valor añadido únicamente cuando hubieran prestado su consentimiento informado para ello.

- A recibir facturas no desglosadas cuando así lo solicitasen (*).

- A que sólo se proceda al tratamiento de sus datos de localización distintos a los datos de tráfico cuando se hayan hecho anónimos o previo su consentimiento informado y únicamente en la medida y por el tiempo necesarios para la prestación, en su caso, de servicios de valor añadido, con conocimiento inequívoco de los datos que vayan a ser sometidos a tratamiento, la finalidad y duración del mismo y el servicio de valor añadido que vaya a ser prestado.

- A detener el desvío automático de llamadas efectuado a su terminal por parte de un tercero (*).

- A impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de su línea en las llamadas que genere.

- A impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de su línea al usuario que le realice una llamada (*).

- A impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de la línea de origen en las llamadas entrantes y a rechazar las llamadas entrantes en que dicha línea no aparezca identificada (*).

(*) Estos derechos sólo están reconocidos por la LGT para los abonados a servicios de comunicaciones electrónicas.

Derechos de los destinatarios de servicios de comunicaciones electrónicas

Los arts. 21 y 22 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, conforme a la nueva redacción, dada por la disposición final primera de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, establecen los siguientes derechos para los destinatarios de servicios de comunicaciones electrónicas

- Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas. Éste precepto no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.

- El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente.

A tal efecto, los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el

consentimiento que hubieran prestado, y deberán facilitar información accesible por medios electrónicos sobre dichos procedimientos.

- Cuando los prestadores de servicios empleen dispositivos de almacenamiento y recuperación de datos en equipos terminales (cookies), informarán a los destinatarios de manera clara y completa sobre su utilización y finalidad, ofreciéndoles la posibilidad de rechazar el tratamiento de los datos mediante un procedimiento sencillo y gratuito.

Lo anterior no impedirá el posible almacenamiento o acceso a datos con el fin de efectuar o facilitar técnicamente la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.