

# 1. GARANTIA DE DERECHOS Y LIBERTADES

## 1.1. CLASES DE GARANTÍAS

### *1.1.1. La aplicación directa de los derechos y libertades*

Se enuncia en el artículo 53.1, al afirmar que los derechos y libertades del Capítulo II del Título 1 vinculan a todos los poderes públicos. Ello quiere decir que los derechos y libertades de los artículos 14 a 38 no necesitan ser desarrollados por una ley para ser aplicables, aunque tampoco se prohíba dicho desarrollo por vía legislativa.

### *1.1.2. Las garantías legislativas*

Se deducen de los arts. 53.1 y 81.1 de la Constitución. Por un lado, el art. 53.1 exige que **el desarrollo** de los derechos y libertades del Capítulo II (arts. 15-38) se haga **por ley**, pero sin que ésta pueda desnaturalizar el contenido del derecho o libertad que regula. La Constitución, en su art. 81.1, establece una garantía procedimental adicional cuando se trata del desarrollo legislativo de alguno de los derechos considerados fundamentales (arts. 15-29), En estos casos el legislador, además de respetar el "contenido esencial" del derecho que pretende regular, habrá de utilizar el procedimiento de Ley Orgánica.

Por otro lado, el art. 82.1 de la Constitución establece la posibilidad de que las Cortes deleguen en el Gobierno la potestad de dictar normas con rango de ley sobre materias que no sean derechos fundamentales,

Estatutos de Autonomía, régimen electoral general, etc. Es decir, que mediante la delegación legislativa los derechos de los artículos 30 a 38 y otros pueden ser regulados mediante Reales Decretos-Legislativos.

### ***1.1.3. Las garantías jurisdiccionales***

El art. 53.2 y la Legislación vigente establecen que los derechos comprendidos en los arts. 14 a 29, más el de la objeción de conciencia del art. 30.2, podrán ser protegidos ante los Tribunales ordinarios **"por un procedimiento** basado en los **principios de preferencia y sumariedad"**, así como en caso necesario "a través del recurso de **amparo ante el Tribunal Constitucional"**.

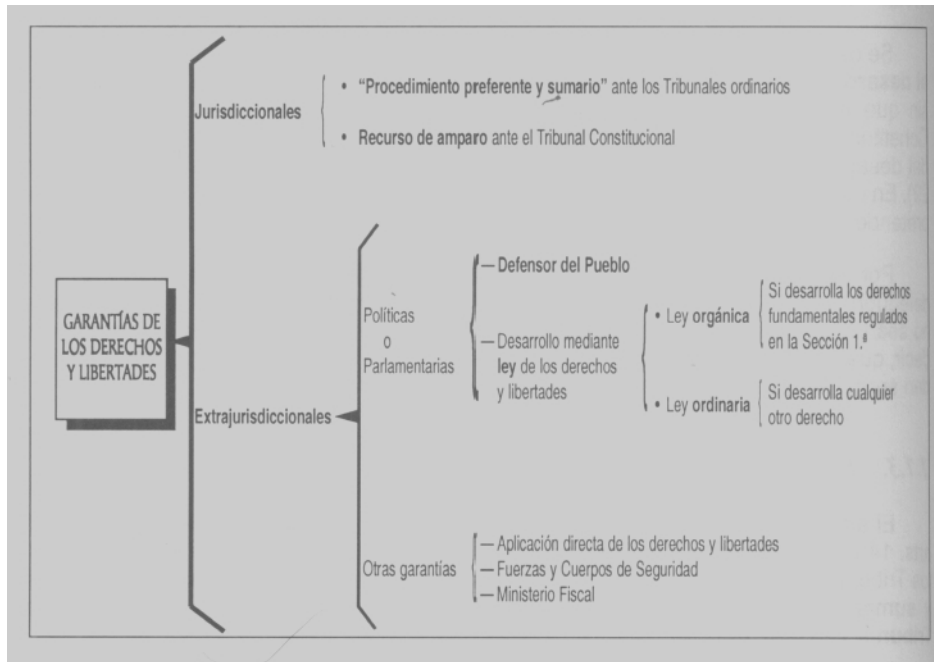
La Ley 62/1978, de 26 de diciembre, regulaba la tutela de los derechos fundamentales con el procedimiento especial en los ámbitos civil, penal y contencioso-administrativo, a que se refiere el art. 53.2 de la Constitución. En el ámbito contencioso-administrativo, la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, establece un procedimiento especial de protección de los derechos fundamentales, derogando el establecido en la Ley 62/1978, para dicho ámbito. Asimismo, la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil derogó los artículos referentes a la garantía jurisdiccional civil.

Por último la Ley 38/2002, de 24 de octubre ha derogado los que hacían referencia a la garantía jurisdiccional penal.

#### **1.1.4. Las garantías extrajudiciales**

Están integradas por ciertas instituciones que se encuentran constitucionalmente legitimadas para la protección y defensa de los derechos y libertades del ciudadano. Entre ellas podemos destacar:

- Las Fuerzas y Cuerpos de Seguridad del Estado bajo dependencia del Gobierno a las que el art. 104 habilita para proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana.
- El Ministerio Fiscal, a quien el artículo 124.1 encomienda, entre otras funciones, la de promover la defensa de los derechos de los ciudadanos. De aquí que el art. 162.1.b) le capacite para interponer recurso de amparo en defensa de los derechos fundamentales de los ciudadanos.
- El Defensor del Pueblo, que es una institución garantizadora de los derechos y libertades de los ciudadanos. En este sentido el art. 54 le encomienda la defensa de los derechos comprendidos en el Título 1 y el art. 162.1 b) le legitima para interponer recurso de amparo en defensa de los derechos fundamentales de los individuos.



## 2. LA LEGISLACIÓN DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

### 2.1. TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL. LEY 15/1999, SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

#### 2.1.1. Introducción

La protección jurídica de los programas informáticos tiene por objeto limitar el uso de la informática para garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente el de su honor, y la intimidad personal y familiar.

La legislación que regula la protección de los datos de carácter personal está contenida, en la actualidad, por **la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD)**, que ha derogado la anterior, **Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de los datos de carácter personal (LORTAD)**. Aunque el programa de la convocatoria alude a esta última, no tiene mucho sentido estudiar una Ley derogada por lo que vamos a desarrollar la vigente ley. La estructura de ambas leyes es idéntica. La Ley 15/1999 actualiza, completa y regula con más detalle muchos de los artículos de la ley derogada.

### ***2.1.2. Ámbito de aplicación***

La LOPD se aplicará a los datos de carácter personal registrados en soporte físico, que sean susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público (administraciones públicas) y privado (empresas y particulares).

La LOPD no se aplicará:

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

- A los ficheros sometidos a la normativa sobre protección de materias clasificadas (secretos oficiales).
- A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.

Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por la LOPD los siguientes tratamientos de datos personales:

- A) Los ficheros regulados por la legislación 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 mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

### **2.1.3. Definiciones**

- **Datos de carácter personal:** cualquier información concerniente a personas físicas, identificadas o identificables.
- **Fichero:** conjunto organizado de datos de carácter personal que sea objeto de tratamiento automatizado (creación, almacenamiento, organización y acceso).
- **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.
- **Responsable del fichero o tratamiento:** persona física o persona jurídica, de naturaleza pública o privada, u órgano administrativo, que tome decisiones sobre la finalidad, el contenido y el uso del tratamiento.
- **Afectado o interesado:** persona física titular de los datos que sean objeto de tratamiento.
- **Procedimiento de disociación:** información que no pueda

asociarse a persona identificada o identificable, obtenida a través de un tratamiento de datos personales.

- **Encargado del tratamiento:** persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otras, realice tratamiento de datos por cuenta del responsable del tratamiento.
- **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.
- **Cesión o comunicación de datos:** toda revelación de datos realizada a persona distinta del interesado.
- **Fuentes accesibles al público:** el censo promocional, los repertorios de teléfonos, listados de profesionales, los diarios y boletines oficiales y los medios de comunicación.

#### ***2.1.4. Principios de la protección de datos***

##### **A) Calidad de los datos**

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.

Los datos personales no podrán usarse para finalidades incompatibles con aquellas para las que fueron recogidos. Serán fines compatibles los históricos, estadísticos o científicos.

Los datos serán exactos y puestos al día; caso de resultar inexactos o incompletos, serán cancelados y sustituidos de oficio por datos rectificadas o completados.

Los datos personales serán cancelados cuando hayan dejado de ser necesarios para los fines para los que fueron recogidos.

Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

**B) Derecho de información en la recogida de datos** Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

- De que existe un fichero o un tratamiento de datos personales.
- De si deben responder o pueden no responder a las preguntas que les sean planteadas.
- De la finalidad de la recogida de datos.
- De los destinatarios de la información.

- De las consecuencias de la obtención de los datos o de la negativa a suministrarles.
- De que pueden ejercitar sus derechos de acceso a los datos, de rectificación, cancelación y de oposición a los mismos.
- De la identidad y la dirección del responsable del tratamiento o su representante.

Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, estas advertencias. Todo esto no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones Públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas.

En el caso de que los datos recogidos no se hayan solicitado al interesado este deberá:

- Ser informado de manera expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento de registro de los datos, de los extremos a los que hemos hecho referencia anteriormente.

- Esto será así excepto cuando así lo prevea una ley, cuando el tratamiento tenga fines históricos, estadísticos o científicos o cuando esta información resulte imposible o exija esfuerzos desproporcionados, a juicio de la Agencia de Protección de Datos (APD).
- Tampoco registrará lo dispuesto en el primer guión cuando los datos proceden de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial.

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

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 comercial, 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.

- 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 tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

Este consentimiento podrá ser revocado, cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

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 oponerle 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.

### **C) Datos especialmente protegidos**

1. Nadie puede ser obligado a declarar sobre su ideología, su religión o sus creencias.
2. Sólo con el consentimiento expreso y por escrito del afectado se pueden procesar datos sobre su ideología, religión o creencias, o su

afiliación sindical. Se exceptúan los ficheros que de sus propios afiliados mantengan los partidos políticos, sindicatos, confesiones religiosas y entes sin ánimo de lucro, pero necesitarán el consentimiento del afectado para ceder estos datos.

3. Se prohíbe crear ficheros con la finalidad exclusión de almacenar datos personales sobre ideología, afiliación sindical, religión, creencias, origen racial o étnico o vida sexual. Sólo cuando el afectado lo consienta expresamente, o una ley lo disponga por razones de interés general, podrán recogerse datos sobre origen racial, salud o vida sexual.

Contravenir los puntos 2 y 3 constituye falta muy grave, pero las Fuerzas y Cuerpos de Seguridad pueden hacerlo, **exclusivamente cuando sea absolutamente necesario para una investigación concreta.**

4. Los datos relativos a la comisión de infracciones penales o administrativas sólo pueden recogerse por las administraciones públicas en sus ficheros, de acuerdo con sus leyes especiales.
5. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento de datos de carácter personal a que se refieren los puntos 2 y 3, 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 personal sujeta asimismo a una obligación equivalente de secreto.

#### **D) Datos relativos a la salud**

Los centros sanitarios públicos y privados, y los profesionales de la medicina, podrán tratar datos relativos a la salud de sus pacientes, de acuerdo con las leyes sanitarias.

#### **E) Seguridad de los datos y deber de secreto**

El responsable del fichero y el encargado del tratamiento garantizarán la seguridad de los datos adoptando medidas que eviten su alteración, pérdida, o tratamiento o acceso no autorizado.

El responsable del fichero y quienes intervengan en el tratamiento de los datos están obligados a guardar secreto profesional, incluso después de terminar sus relaciones con el titular del fichero.

El personal al servicio de la Agencia de Protección de Datos tiene el mismo deber de guardar secreto profesional.

#### **F) Cesión (comunicación) de datos**

Sólo pueden cederse con consentimiento previo del interesado, y para fines directamente relacionados con las funciones legítimas del

cedente y del cesionario, con el previo consentimiento del interesado.

Por excepción, no se precisa el consentimiento del afectado:

- Cuando la cesión esté autorizada en una ley.
- Cuando los datos se recojan de una fuente accesible al público.
- 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 le justifique.
- Cuando la cesión se haga al Defensor del Pueblo, al Ministerio Fiscal o a los Jueces y Tribunales o al Tribunal de Cuentas o a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.
- En caso de cesión entre administraciones públicas cuando tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
- En caso de datos sobre la salud, cuya cesión resulte necesaria para solucionar una urgencia, o para realizar estudios sobre epidemias, conforme a las leyes de sanidad.

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 se destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.

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

### **G) Acceso a los datos por cuenta de terceros**

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.

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.

El contrato expresará:

a) Las obligaciones del encargado:

- Seguir las instrucciones del responsable del tratamiento.
- Aplicar los datos a las finalidades previstas en el contrato.
- Guardar secreto sobre los datos.



b) Las medidas de seguridad.

Una vez cumplido el contrato, se destruirán o devolverán al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

### ***2.7.5. Derechos de las personas afectadas***

#### **A) Impugnación de valoraciones**

El afectado puede impugnar los actos administrativos y las decisiones privadas que valoren su comportamiento cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.

Para conseguirlo, tiene derecho a que el responsable del fichero le informe sobre los criterios de valoración y el programa utilizado.

#### **B) Derecho de consulta al Registro General de Protección de Datos (RGPD)**

El RGPD es de consulta pública y gratuita. Cualquiera puede conocer la identidad del responsable y la finalidad de los ficheros de datos de carácter personal.

### **C) Derecho de acceso**

El interesado puede consultar gratuitamente los ficheros de sus datos personales, mediante su visualización; también puede obtener una comunicación de ellos mediante escrito, copia, fotocopia o telecopia, certificada o no, en forma legible e inteligible, sin tener que utilizar códigos o claves que requieran el uso de dispositivos mecánicos específicos, excepto cuando medien razones de interés público, o ante intereses de terceros más dignos de protección. En este caso, el responsable del fichero informará al afectado de su derecho a dirigirse a la Agencia de Protección de Datos.

Salvo que acredite interés legítimo, el afectado sólo puede ejercitar este derecho cada doce meses.

### **D) Derecho de rectificación y cancelación**

El responsable del tratamiento hará efectivo el derecho de rectificación o cancelación del interesado en plazo de diez días.

Serán rectificadas o canceladas los datos inexactos o incompletos.

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.

### **E) Tutela de los derechos y derecho de indemnización**

Los afectados pueden reclamar contra los autores de actos contrarios a esta ley, ante la Agencia de Protección de Datos.

Al interesado al que se denieguen, 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.

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

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

### **F) Derecho a indemnización**

Los afectados que sufran daño o lesión en sus bienes o derechos tienen derecho a ser indemnizados. La acción se ejercitará ante la jurisdicción ordinaria si los ficheros son de titularidad privada, y por las leyes que regulan la responsabilidad de las Administraciones públicas, si

los ficheros son de titularidad pública.

### **2.1.6. Disposiciones sectoriales**

#### **A) Ficheros de titularidad pública**

1. Las Administraciones públicas, para **crear, modificar o suprimir** ficheros automatizados necesitan una ley o reglamento publicado en los boletines oficiales (BOE, BOJA,..), en cuyas disposiciones conste:

- Fines del fichero y los usos previstos para el mismo.
- Personas o colectivos sobre los que se pretenda obtener los datos o que deben suministrar los datos.
- Procedimiento de recogida de datos.
- Estructura básica del fichero y descripción de los tipos de datos incluidos en el mismo.
- Cesiones y transferencias de datos que se prevean a países terceros.
- Órganos de las administraciones responsables del fichero.
- Órganos ante los que pueda ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
- Las medidas de seguridad.

2. Podrán **cederse los datos** que una Administración Pública obtenga con

destino a otra.

Pero no podrán cederse para el ejercicio de competencias diferentes o sobre materias distintas de las previstas, salvo que una disposición, ley o reglamento, así lo autorice o cuando tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

Un caso concreto es la cesión de los datos del padrón municipal de habitantes y del censo electoral que consten en los ficheros del Instituto Nacional de Estadística, organismo que podrá cederlos al Estado y a las Comunidades Autónomas que se lo soliciten para el ejercicio de sus competencias.

Para estas cesiones no será necesario el consentimiento del afectado (interesado).

## **B) Ficheros de titularidad privada**

Podrán crearse ficheros automatizados de datos de propiedad privada:

- Con respeto a las garantías de la ley.
- Cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular.

➤ Previa notificación a la Agencia de Protección de Datos (APD).

Esta notificación debe contener necesariamente:

- El responsable del fichero.
- La finalidad del fichero.
- Su ubicación.
- Tipo de datos que contiene.
- Medidas de seguridad.
- Cesiones de datos previstas: cuando se efectúe la primera, el responsable lo comunicará a los afectados, excepto cuando la cesión venga impuesta por la ley.
- Transferencias de datos que se prevean a países terceros.

La Agencia de Protección de Datos inscribirá el fichero en el Registro General de Protección de Datos, 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.

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.

### **C) Censo promocional**

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

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

Los procedimientos mediante los que los interesados podrán solicitar no aparecer en el censo promocional se regularán reglamentariamente. Entre estos procedimientos, que serán gratuitos para los interesados, se incluirá el documento de empadronamiento. Trimestralmente se editará una lista actualizada del censo promocional, excluyendo los nombres y domicilios de los que lo hayan solicitado.

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



### **2.1.7. Movimiento internacional de datos**

No podrán cederse datos automatizados a países que no proporcionen un nivel de protección equiparable al de la LOPD. Excepto, entre otros casos:

- Cuando se cedan en aplicación de tratados internacionales firmados por España.
- Para prestar o solicitar auxilio judicial internacional.
- Para intercambio de datos médicos.
- Cuando se refieran a transferencias de dinero, según sus leyes especiales.

### **2.1.8. La Agencia de Protección de Datos**

1. **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 la LOPD y su propio Estatuto.

2. **Son sus funciones** entre otras:

- 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.

- Atender las peticiones y reclamaciones de los afectados.
- Informar de sus derechos a los afectados.
- Ejercer la potestad sancionadora.
- Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publica periódicamente una relación de los ficheros de datos personales.
- Controlar y autorizar las autorizaciones que proceden en relación con los movimientos internacionales de datos.
- Vigilar la recogida de datos estadísticos y el secreto estadístico.
- Las que le atribuyan otras disposiciones.

Contra las Resoluciones del Director de la APD se puede interponer recurso contencioso-administrativo.

### **3. Órganos de la Agencia de Protección de Datos:**

#### **a) El Director:**

- La dirige y representa.

- Es elegido entre los miembros del Consejo Consultivo, mediante Real Decreto, por 4 años.
- Ejercerá sus funciones con plena independencia y objetividad y no estará sujeto a instrucción alguna en el desempeño de aquéllas.
- Puede ser cesado a petición propia o por separación acordada por el Gobierno por incumplimiento grave, por incapacidad, por incompatibilidad o, por condena por delito doloso.

**b) El Consejo Consultivo:**

- Es el órgano asesor del Director.
- Está compuesto por un diputado, un senador y representantes de la Administración Central del Estado, de las Comunidades Autónomas, de la Administración Local, de la Real Academia de la Historia, de los usuarios y consumidores, y del sector de ficheros privados y por un experto en la materia.

**c) El Registro General de Protección de Datos (RGPD)** es un órgano integrado en la APD, donde se inscribirán:

- Los ficheros automatizados de las administraciones públicas y los de titularidad privada.

- Los Códigos Tipo.
- Los datos necesarios para el ejercicio de los derechos de información, acceso, rectificación y cancelación.
- Las autorizaciones previstas en la ley.

**d) Órganos de las Comunidades Autónomas:**

- Las CC.AA. podrán crear y mantener sus propios registros de ficheros públicos para el ejercicio de sus competencias.
- A los órganos de las CC.AA. se les garantiza plena independencia y objetividad en el ejercicio de su cometido, pero el Director de la APD podrá convocarlos a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación. Y podrá requerir a las CC.AA. que tengan algún fichero ilegal para que los corrijan, y si desatienden este requerimiento, el Director de la APD podrá impugnar la resolución que adopte la Comunidad Autónoma.

**2.1.9. Infracciones y sanciones**

La LOPD establece un régimen sancionador para los responsables de los ficheros, y para los encargados del tratamiento.

## **A) Infracciones: tipos**

### **a) Leves:**

- Recoger datos de los interesados sin darles la información a que tienen derecho.
- No atender, por motivos formales, la solicitud del afectado para cancelar o rectificar sus datos.
- No dar la información solicitada por la Agencia de Protección de Datos (APD) en cuestiones no sustantivas.
- No solicitar la inscripción del fichero de datos de carácter personal en el Registro cuando no sea infracción grave.
- Incumplir el deber de secreto, cuando no sea infracción grave.

### **b) Graves:**

- Crear ficheros de titularidad pública sin autorización de una disposición general publicada en el BOE o Diario oficial correspondiente, o recoger datos para aquellos.
- Crear ficheros privados, o recoger datos para ellos, con finalidades distintas de las que constituyan el objeto legítimo de la empresa o entidad.
- Recoger datos sin el consentimiento expreso de los afectados.

- Tratar los datos, o usarlos, sin las garantías de la Ley.
- Obstaculizar o impedir el ejercicio del derecho de acceso y oposición y la negativa a facilitar la información que sea solicitada.
- Mantener datos inexactos o no efectuar las rectificaciones o cancelaciones cuando resulten afectados los derechos de las personas amparados por la ley.
- Vulnerar el deber de guardar secreto.
- Mantener los ficheros, locales, programas o los equipos sin las debidas condiciones de seguridad.
- No remitir a la APD dentro de plazo las informaciones o documentos que le sean requeridos, así como no remitir las notificaciones previstas.
- Obstruir el ejercicio de la función inspectora.
- No inscribir el fichero de datos en el Registro (RGPD) cuando así lo requiera el Director de la Agencia (APD).
- Incumplir el deber de información establecido en esta ley, cuando los datos hayan sido recogidos de persona distinta del afectado.

c) **Muy graves:**

- Recoger datos con engaño y fraude.
- Ceder o comunicar los datos fuera de los casos en que está permitido.
- No cesar en el uso ilegítimo de los tratamientos de datos, cuando sea requerido por el Director de la APD o por los afectados.
- Transferir datos a países que no garanticen su protección, sin autorización del Director de la APD.
- Tratar los datos de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando se atente contra el ejercicio de los derechos fundamentales de las personas.
- No atender u obstaculizar de manera sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.
- No atender, de forma sistemática, el deber legal de notificar la inclusión de los datos personales en un fichero.
- Vulnerar el deber de guardar secreto en datos especialmente protegidos, así como los que hayan sido recabados para fines policiales, sin consentimiento de las personas afectadas.

## **B) Infracciones de las Administraciones Públicas**

Cuando las infracciones se cometan en ficheros de las Administraciones Públicas, el Director de la APD dictará una resolución con las medidas necesarias:

- Para corregir o cesar los efectos de la infracción.
- También podrá proponer la apertura de un expediente sancionador al responsable del fichero, conforme al Reglamento de régimen disciplinario de las Administraciones Públicas.
- Y comunicará al Defensor del Pueblo estas actuaciones.

## **C) Sanciones: tipos**

Las infracciones se sancionarán con multas, en cuantía de:

- **Leves**, de 601,01 a 60.101,21 euros.
- **Graves**, de 60.101,21 a 300.506,05 euros.
- **Muy graves**, de 300.506,05 a 601.012,10 euros.

La cuantía de cada sanción se graduará con arreglo a estos criterios:

- Naturaleza de los derechos personales afectados.
- Volumen de los tratamientos efectuados.



- Beneficios obtenidos.
- Intencionalidad.
- Reincidencia.
- Daños y perjuicios causados a los afectados y a terceras personas.
- Y cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

#### **D) Procedimiento sancionador**

Las Resoluciones de la Agencia de Protección de Datos u órgano correspondiente de la Comunidad Autónoma agotan la vía administrativa, razón por la cual pueden ser recurridas directamente ante la jurisdicción contencioso-administrativa.

#### **E) Inmovilización de ficheros**

En los casos de infracciones muy graves, de utilización o cesión ilícita de los datos de carácter personal en que se impide gravemente o se atente igualmente contra el ejercicio de los derechos de los

ciudadanos y el libre desarrollo de la personalidad que garantizan la Constitución y las leyes, el Director de la APD podrá:

- Además de sancionar a los responsables de los ficheros, tanto públicos como privados.
- Requerirles a que cesen en su utilización o cesión ilícita de datos.
- Si el requerimiento fuera desatendido la APD podrá **inmovilizar los ficheros**, mediante Resolución motivada.

## **F) Prescripción**

Las infracciones cometidas, y las sanciones impuestas, prescriben:

- Muy graves, a los tres años.
- Graves, a los dos.
- Leves, al año.

El plazo de prescripción comienza a contarse desde el día en que la infracción se comete, y desde el día siguiente a aquél en que adquiera firmeza la resolución por la que se impone la sanción.

La prescripción se interrumpe, por iniciación del procedimiento (sancionador o de ejecución) con conocimiento del infractor.

La prescripción se reanuda si el expediente se paraliza más de 6 meses por causa no imputable al infractor.