

LA PROTECCIÓN DE DATOS EN EL ÁMBITO DE LA RELACIÓN JURÍDICO-ADMINISTRATIVA

ALFONSO RODRÍGUEZ PALENCIA
Profesor Asociado de Derecho Civil
Universidad de Alcalá

Resumen: La protección de datos de carácter personal constituye un sistema de protección de la intimidad y de la dignidad del titular de los mismos arbitrado por el legislador en cumplimiento del mandato del artículo 18.4 de la Constitución e incardinable en el esquema teórico del derecho subjetivo clásico. Sentado lo anterior, se ha tratado de exponer como opera dicho derecho en la interacción de su titular con la Administración Pública –relación jurídico-administrativa- con las limitaciones provenientes de la prerrogativa administrativa y en el marco tanto del Procedimiento Administrativo Común como del procedimiento electrónico en el que se concreta la actuación de la denominada Administración electrónica.

Palabras clave: Protección de datos, Procedimiento Administrativo Común, Administración electrónica

Abstract: The protection of private data is a system for protection of the privacy and dignity of people. The article 18.4 of the Spanish Constitution (1978), related with the new technology and privacy, has been implemented by a specific Act passed by the Spanish Parliament (Cortes Generales). This legal protection has adopted the technique of the classic private right. This paper focuses on the scope of the right mentioned above in the relationship between citizens and Public Administration (administrative relations). The paper examines the limits of the right as a consequence of the special powers that has the Public Administration. The study focuses on the common Administrative procedure and the electronic procedure; in the latest acts the so called Electronic Administration.

Keywords: Protection of private data, Common Administrative Procedure, Electronic Administration

SUMARIO: I. INTRODUCCIÓN. II. CONCEPTO DE LA PROTECCIÓN DE DATOS. III. NATURALEZA JURÍDICA DE LA PROTECCIÓN DE DATOS. 1 La protección de datos como derecho de la personalidad y derecho fundamental. 2 La protección de datos como derecho subjetivo. IV. LAS ADMINISTRACIONES PÚBLICAS EN EL MARCO DE LA RELACIÓN JURÍDICO-ADMINISTRATIVA. V. LA PROTECCIÓN DE DATOS EN EL ÁMBITO DE SU REGULACIÓN ESPECÍFICA. 1 La especial situación jurídica de las Administraciones Públicas. 1.1. Ficheros de las Administraciones Públicas excluidos del régimen general de la protección de datos. 1.2. Exclusión del consentimiento del afectado para el tratamiento de datos de carácter personal. 1.3. Datos sobre infracciones penales o administrativas. 1.4. Exclusión del consentimiento del interesado para comunicación de datos a un tercero. 1.5. Aplazamiento del derecho de cancelación. 1.6. Creación, modificación o supresión de los ficheros de titularidad pública. 1.7. Ficheros de las Fuerzas y Cuerpos de Seguridad. 1.8. Excepciones a los derechos de acceso, rectificación y cancelación. 1.9. Otras excepciones a los derechos de los afectados. 1.10. Excepción a las restricciones al movimiento internacional de datos. 1.11. Infracciones de las Administraciones públicas. 2. Las matizaciones introducidas por el Tribunal Constitucional. 3. La caracterización de la protección de datos como derecho subjetivo. 3.1. La protección de datos como un derecho subjetivo unitario. 3.2. La integración, como meras facultades, en el derecho subjetivo a la protección de datos, de los denominados derechos contemplados por la L.O. 15/99. 4. El contenido del derecho subjetivo a la protección de datos. 5. En particular, el consentimiento del afectado. 5.1. Consentimiento para el tratamiento de los datos de carácter personal. 5.1.1. Definición de consentimiento del interesado. 5.1.2. Derecho de información en la recogida de datos. 5.1.3. Prestación del consentimiento. 5.1.4. Revocación del consentimiento. 5.1.5. Datos especialmente protegidos. 5.1.6. Desarrollo de relaciones jurídicas. 5.2 Consentimiento para la comunicación de datos. 5.2.1. Definición de cesión. 5.2.2. Sustantividad normativa propia. 5.2.3. Supuestos de consentimiento para cesión de datos. 5.2.4. Ficheros públicos. 5.3 Consentimiento para el tratamiento de datos de menores de edad. VI. CRONOLOGÍA DE LA INCOR-

PORACIÓN DE LA PROTECCIÓN DE DATOS A LA RELACIÓN JURÍDICO-ADMINISTRATIVA. VII PROTECCIÓN DE DATOS Y PROCEDIMIENTO ADMINISTRATIVO COMÚN. VIII. PROTECCIÓN DE DATOS Y ADMINISTRACIÓN ELECTRÓNICA. 1. El procedimiento administrativo-electrónico. 2. La superación de temores y recelos ante la utilización de las nuevas tecnologías. 3. Protección de datos y Administración electrónica. IX. EN RESUMEN

I. INTRODUCCIÓN

Con este artículo se pretende la presentación de la Protección de Datos personales como constitutiva de un verdadero derecho subjetivo que se inserta en la esfera jurídica de su titular el cual puede, por tanto, ejercitarlo en sus relaciones con las Administraciones públicas. Como tal derecho subjetivo, cabe distinguir en el mismo entre una actividad de ejercicio del poder jurídico en que el derecho consiste sobre el objeto del mismo –los datos personales- y una actividad de defensa y protección frente a eventuales agresiones o intromisiones indebidas; todo ello enmarcado en el ámbito específico de la relación jurídico-administrativa, esto es, en el ámbito de las relaciones que el titular de los datos y, correlativamente, del derecho subjetivo, mantiene, en su condición de ciudadano/administrado, con las Administraciones Públicas. En el marco de la relación jurídica las partes gestionan entre sí sus derechos y obligaciones recíprocos; en la relación jurídico-administrativa esta gestión se produce entre ciudadano y Administración y, en ese proceso, el ciudadano puede recurrir al ejercicio de su derecho subjetivo a la protección de datos. Se trata, pues, de demostrar en primer lugar la naturaleza jurídica de derecho subjetivo de la protección de datos y de determinar su contenido. Y seguidamente analizar la operatividad de dicho derecho en las relaciones de su titular con la Administración. A tal efecto observaremos el desenvolvimiento de la relación jurídico-administrativa dentro de los marcos normativos más habituales para el ejercicio del derecho subjetivo de protección de datos:

- La propia legislación de protección de datos.
- El procedimiento administrativo común.
- El procedimiento administrativo electrónico.

II. CONCEPTO DE LA PROTECCIÓN DE DATOS

Curiosamente, aunque la Ley Orgánica 15/1999 se denomina de Protección de Datos de Carácter Personal, ni en ella ni en su Reglamento, aprobado por Real Decreto 1720/2007, de 21 de diciembre, se hace constar una definición de la protección de datos. A partir del artículo 1 de la Ley Orgánica 15/1999 puede decirse que la protección de datos consiste en la garantía y protección, en lo que concierne al tratamiento de los datos personales, de las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar. Se distinguen en este concepto tres elementos sobre los que conviene fijar especialmente la atención, a saber:

- Las personas físicas
- El tratamiento
- Los datos personales

Ya se ve en el concepto expuesto como el ámbito personal de la protección de datos se refiere exclusivamente a las personas físicas. Ítem más, el artículo 3.e) de la Ley Orgánica define al afectado o interesado como la persona física titular de los datos que sean objeto del tratamiento. En los mismos términos se expresa el artículo 5.1.a) del Reglamento, cuyo artículo 2.2 excluye expresamente de su ámbito de aplicación a los tratamientos de datos referidos a personas jurídicas. En cuanto al tratamiento, conviene disipar un cierto lugar común que tiende a creer que esta legislación se refiere exclusivamente a los tratamientos y ficheros automatizados o informatizados. No es así. La protección de datos se extiende tanto a los ficheros y tratamientos automatizados como a los no automatizados. El ámbito de aplicación está definido con la suficiente generalidad como para incluir en el mismo los ficheros y tratamientos automatizados o no: *“aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento”* (art.2.1, L.O. 15/99). Lo mismo cabe decir respecto a la definición de fichero (art. 3.b) y, en cuanto al tratamiento de datos, se especifica que se trata de *“operaciones y procedimientos técnicos de carácter automatizado o no”* (art. 3.c). En la Exposición de Motivos del Reglamento se hace constar que la Ley Orgánica 15/1999 comprende el tratamiento automatizado y el no automatizado de los datos de carácter personal. A lo largo del texto se encuentran otras varias referencias en este mismo sentido. Por último, hemos apuntado una acotación respecto al contenido de los datos personales. También en este punto hay que desmentir un lugar común acerca del carácter íntimo o reservado de los datos personales objeto de tratamiento. No cabe deducir esta interpretación de la definición de datos de carácter personal

contenida en el artículo 3.a) de la Ley y, con más amplitud, en el artículo 5.1.f) del Reglamento: “*Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables*”. Ya en una sentencia del Tribunal Constitucional de 4 de mayo de 1998, en relación con el artículo 18.4 de la Constitución, fundamento parcial (relativo a los ficheros y tratamientos automatizados) de la protección de datos, se hacía mención al control del flujo de informaciones que conciernen a cada persona, pertenezcan o no al ámbito más estricto de la intimidad.

III. NATURALEZA JURÍDICA DE LA PROTECCIÓN DE DATOS

La protección de datos participa de un doble carácter:

- Derecho de la personalidad / Derecho fundamental.
- Derecho subjetivo.

1. La protección de datos como derecho de la personalidad y derecho fundamental

Los derechos de la personalidad se configuran como aquellos poderes jurídicos conferidos al individuo, bien para defender su personalidad y los bienes inherentes a la misma; bien para proyectar hacia el exterior, de una manera eficaz, su propia personalidad con arreglo a sus aspiraciones y legítimos intereses. Los bienes de la personalidad son “*atributos que integran su esencia [de la persona] y que le son indispensables para el desarrollo de su personalidad. Derechos de la personalidad serán los instrumentos ideados por el Ordenamiento jurídico para que el hombre satisfaga aquellas necesidades, esto es, para conseguir el pleno goce y disfrute de aquellas manifestaciones esenciales de su personalidad*”.¹ La asimilación entre derechos de la personalidad y derechos fundamentales está aceptada con bastante generalidad por nuestra doctrina científica. En todo caso, al estar el bien jurídico protegido (bien de la personalidad) a nivel constitucional, se sitúa automáticamente a este nivel el derecho protector correspondiente. Así ha sido declarado, a la vista de la L.O. 15/99, por la Sentencia 292/2000 del Tribunal constitucional, la cual manifiesta que cabe entender sin dificultad que dicha Ley da cumplimiento al mandato del artículo 18.4 de la Constitución, lo que se traduce en el derecho fun-

1 BUSTOS (2008): 19.

damental a la protección de datos que persigue garantizar a la persona un poder de control y disposición sobre sus datos personales, sobre su uso y destino.

2. La protección de datos como derecho subjetivo

El precedente enunciado implica la consideración, no absolutamente pacífica, de que los derechos de la personalidad son subsumibles en el molde clásico del derecho subjetivo. No es esta la ocasión para terciar a fondo en esta cuestión, si bien no cabe eludir un intento de justificación, siquiera sea somero, del porque de la consideración de dichos derechos como derechos subjetivos. *“En principio no hay ciertamente razones decisivas para negar la existencia de la categoría jurídica constituida por los derechos subjetivos de la personalidad. Si el derecho subjetivo presupone siempre un deber jurídico que haga posible una pretensión o exigencia, hay que reconocer que el derecho a la vida, a la integridad física, al honor, a la identidad personal, etc., penetran en el círculo del deber jurídico que pesa sobre todos, en el sentido de que no han de ser ilegítimamente lesionados. Y si el concepto del derecho subjetivo presupone un poder al que el ordenamiento jurídico conceda una cierta autonomía, no puede negarse la posibilidad técnica de que sean objetivados por el Derecho, separándolos y destacándolos de la personalidad, determinados atributos suyos, que sean así elevados a bienes jurídicos y, consiguientemente, a objetos de derecho protegidos con una específica acción civil.*

*En los derechos esenciales de la personalidad, en conclusión, pueden concurrir las cualidades propias de los derechos subjetivos, en cuanto se dé en ellos la atribución, por el ordenamiento positivo, de un poder jurídico a un titular frente a otra u otras personas, puesto a su libre disposición y tutelado por una acción judicial”.*² Pues bien, ese poder jurídico, esencia del derecho subjetivo, al que hace referencia el profesor CASTÁN, tiene una clara manifestación en la sentencia del Tribunal Constitucional antes mencionada en la que, tras repetidas alusiones a la protección de datos como poder de control y de disposición, se concluye y resume: *“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 ese tercero recabar,*

2 CASTÁN TOBENAS (1984): 366.

y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso". Quizá, la principal dificultad para admitir la subsunción de los derechos de la personalidad en el esquema de los derechos subjetivos clásicos (derechos reales y derechos de crédito u obligación) es que en estos predomina el aspecto de poder jurídico –uso, disfrute, disposición- sobre el aspecto puramente defensivo, que solo se activa cuando se produce alguna perturbación indebida que, por definición, siempre presentará un cierto carácter anómalo en el contexto global de la funcionalidad del derecho. Las cosas son distintas en el contexto de los derechos de la personalidad. Estos ostentan una serie de caracteres, como son la extrapatrimonialidad o la intransmisibilidad que los hace extraños al tráfico patrimonial clásico basado en el uso, disfrute y disposición; mientras que una parte muy importante de su funcionalidad radica en los aspectos puramente defensivos. Pero, ya sea que predomine la patrimonialidad, ya sea que prime la protección, ello no excluye en ninguno de los dos casos el que nos encontremos ante genuinos derechos subjetivos, integrados, en una u otra medida y proporción, por un ámbito de poder jurídico y por un elenco de instrumentos de protección. Si consideramos al derecho subjetivo desde un punto de vista institucional, vemos que constituye el reconocimiento por el ordenamiento de un ámbito de poder y libertad que permita al individuo el cabal desarrollo de su personalidad y el logro de sus legítimos intereses. Este sería el aspecto genérico -sustantivo y fundamental- del derecho subjetivo, aplicable tanto a los derechos patrimoniales clásicos como a los derechos de la personalidad. Si nos fijamos en el aspecto técnico-jurídico, el derecho subjetivo articula el conjunto de facultades y medidas de protección para la puesta en práctica de ese desarrollo personal que acabamos de ver reconocido en términos generales. Por su carácter instrumental, el aspecto técnico-jurídico tiene un valor secundario respecto al carácter institucional y constituye la configuración específica -especie- de cada tipo de derecho subjetivo: real, de obligación o de la personalidad. Pero todos, en fin, y el derecho fundamental a la protección de datos entre ellos, derechos subjetivos.

IV. LAS ADMINISTRACIONES PÚBLICAS EN EL MARCO DE LA RELACIÓN JURÍDICO-ADMINISTRATIVA

Las Administraciones públicas no son un sujeto más de los que operan en el marco de la realidad social. En realidad, se trata del sujeto más importante, el más grande y el más poderoso. Y, además de eso, en su relación con

el resto de los sujetos del marco social y, por consiguiente, en su relación con los ciudadanos/administrados -relación jurídico-administrativa- actúa ostentando las facultades exorbitantes propias de la prerrogativa administrativa. La prerrogativa administrativa encuentra su fundamento en la circunstancia de que la Administración, por definición:

- Actúa siempre conforme a Derecho.

- Gestiona y promueve los intereses generales. "La Administración Pública sirve con objetividad los intereses generales y actúa de acuerdo con los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación con sometimiento pleno a la ley y al Derecho". (Art.103.1 C.E.).

En el mismo sentido:

- Art. 3.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.- Art. 2.1 de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado. Este es el interlocutor con el que debe interrelacionar el ciudadano cuando actúa en su condición de administrado el cual, para equilibrar su relación con tan impresionante combinación de poder y prerrogativa, cuenta en su haber con los instrumentos legales que pone a su disposición el Estado de Derecho. Y, entre esos instrumentos, uno de ellos es el derecho subjetivo de la protección de datos. Seguidamente, vamos a tratar de poner de manifiesto como se ejerce ese derecho en los siguientes ámbitos concretos de la actuación administrativa:

- Protección de datos.
- Procedimiento administrativo.-
Administración electrónica.

V. LA PROTECCIÓN DE DATOS EN EL ÁMBITO DE SU REGULACIÓN ESPECÍFICA

1. La especial situación jurídica de las Administraciones Públicas

Ya se ha apuntado con anterioridad que la especial situación de prerrogativa de las Administraciones Públicas en el marco de la relación jurídico-administrativa se debe a que las mismas se caracterizan por gestionar y promover los intereses generales actuando siempre conforme a

Derecho. En la Ley Orgánica 15/99 esta prerrogativa se traduce en un régimen especial de las AA.PP concretado en varios aspectos de su articulado que pasamos a examinar seguidamente.

1.1. Ficheros de las Administraciones Públicas excluidos del régimen general de la protección de datos

Ficheros meramente excluidos:

- Ficheros sometidos a la normativa sobre protección de materias clasificadas. (Art. 2.2.b).
- Ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. (Art. 2.2.c).

Ficheros regidos por sus disposiciones específicas:

- Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública. (Art. 2.3.b).
- 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. (Art. 2.3.e).

1.2. Exclusión del consentimiento del afectado para el tratamiento de datos de carácter personal

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. (Art. 6.2).

1.3. Datos sobre infracciones penales o administrativas

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. (Art. 7.5)

1.4. Exclusión del consentimiento del interesado para comunicación de datos a un tercero

Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. (Art. 11.2.e)

1.5. Aplazamiento del derecho de cancelación

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. (Art. 16.3).

1.6. Creación, modificación o supresión de los ficheros de titularidad pública

Mediante disposición general publicada en el Boletín Oficial del Estado o Diario oficial correspondiente. (Art. 20.1)

1.7. Ficheros de las Fuerzas y Cuerpos de Seguridad

- La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto. (Art.22.2).

- La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos que hagan referencia a la ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta. (Art.22.3).

1.8. Excepciones a los derechos de acceso, rectificación y cancelación

- Los responsables de determinados ficheros (art.22.2, 3 y 4) de las Fuerzas y Cuerpos de Seguridad podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando. (Art.23.1).

- Los responsables de los ficheros de la Hacienda Pública podrán denegar el ejercicio de dichos derechos cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y cuando el afectado esté siendo objeto de actuaciones inspectoras. (Art.23.2).

1.9. Otras excepciones a los derechos de los afectados

- El derecho de información en la recogida de datos no será aplicable cuando con ello se 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. (Art.24.1). Subrayado: anulado por el Tribunal Constitucional.

- La efectividad de los derechos de acceso, rectificación y cancelación no será de aplicación si, ponderados los intereses en presencia, resultase que dichos derechos hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección. (Art.24.2). Anulado por el Tribunal Constitucional.

1.10. Excepción a las restricciones al movimiento internacional de datos

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. (Art.34.h)

1.11. Infracciones de las Administraciones públicas

En el caso de infracciones en ficheros de titularidad pública, el Director de la Agencia Española de Protección de Datos dictará una Resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. (Art.46.1).

2. Las matizaciones introducidas por el Tribunal Constitucional

En este régimen jurídico especial conferido por la legislación de protección de datos a las Administraciones públicas, se introdujo un matiz restrictivo por medio de la Sentencia 292/2000, de 30 de noviembre, del Tribunal Constitucional.

El Defensor del Pueblo interpuso recurso de inconstitucionalidad contra los siguientes incisos de la Ley Orgánica 15/1999, los cuales, a su juicio, lesionan el contenido esencial del derecho fundamental a la intimidad frente al uso de la informática, al imponerle restricciones injustificadas y desproporcionadas que lo hacen impracticable y lo despojan de su necesaria protección. Junto a cada objeción del Defensor del Pueblo hacemos constar, por claridad expositiva, los correlativos pronunciamientos del Tribunal Constitucional.

-Art.21.1: “o por disposición de superior rango que regule su uso”. Aduce el Defensor del Pueblo que al considerar dicho precepto, que autoriza la comunicación de datos entre Administraciones públicas, en relación

con el artículo 20.1 (Disposición de creación del fichero, vid. ut supra 1.6) se posibilitan los siguientes efectos:

Que puedan hacerse cesiones de datos entre Administraciones públicas para fines distintos a los que motivaron su recogida.

Que el titular de los datos no sea informado, cuando se recaban, de la posibilidad de dicha cesión, al no estar prevista en la norma que crea y regula el fichero.

Que la propia cesión se efectúe sin el consentimiento del afectado.

Que la autorización para efectuar esas cesiones puede contenerse en una norma de rango inferior a la Ley.

La Sentencia manifiesta, a este respecto, que el motivo de la inconstitucionalidad del artículo 21.1 de la L.O. resulta claro puesto que la Ley en este punto no ha fijado por sí misma, como le impone la Constitución (art.53.1 C.E), los límites al derecho a consentir la cesión de datos personales entre Administraciones públicas para fines distintos a los que motivaron originariamente su recogida, y a los que alcanza únicamente el consentimiento inicialmente prestado por el afectado (art.11 en relación con lo dispuesto en los arts. 4, 6 y 34.e de la L.O.), sino que se ha limitado a identificar la norma que puede hacerlo en su lugar.

Norma que bien puede ser reglamentaria, ya que con arreglo al precepto impugnado será una norma de superior rango, y con mayor razón para el caso de que la modificación lo sea por una norma de similar rango, a la que crea el fichero (y ésta basta con que sea una disposición general, que no una Ley, publicada en un Boletín o Diario oficial –art.20.1 de la L.O.) la que pueda autorizar esa cesión inconstituida de datos personales, lo que resulta ser, desde luego, contrario a la Constitución.

- Ar.24.1. Vid. ut supra 1.9, primer guión. Arguye el Defensor del Pueblo que el inciso mencionado exime a la Administración de cumplir con sus obligaciones de información y advertencia del artículo 5.1 y 2 (facultades de acceso a los datos, de rectificación y cancelación de los mismos y de oponerse a su tratamiento automatizado) si tal cosa pudiere impedir o dificultar gravemente las funciones de control y verificación de las Administraciones públicas o cuando afecte a la persecución de infracciones administrativas; lo que constituiría infracción de los artículos 18.1 y 4 y 53.1 de la Constitución. Respecto a este punto, la sentencia hace constar que la expresión “*funciones de control y verificación*” abre un espacio de incertidumbre tan amplio que al habilitar a la Administración para que restrinja derechos fundamentales invocando semejante expresión está renunciando a fijar ella misma los límites, apoderando a la Administración para hacerlo. Y de un modo tal que permite reconducir a la misma prácticamente toda actividad adminis-

trativa, ya que toda actividad administrativa que implique entablar una relación jurídica con un administrado conllevará de ordinario la potestad de verificar y controlar que ese administrado ha actuado conforme al régimen jurídico administrativo de la relación jurídica entablada con la Administración.

Lo que, a la vista del motivo de restricción del derecho a ser informado del art. 5 de la L.O. deja en la más absoluta incertidumbre al ciudadano sobre en qué casos concurrirá esa circunstancia (si no en todos) y sume en la ineficacia cualquier mecanismo de tutela jurisdiccional que deba enjuiciar semejante supuesto de restricción de derechos fundamentales sin otro criterio complementario que venga en ayuda de su control de la actuación administrativa en esta materia. Las mismas tachas merece la restricción, contenida en el mismo precepto, relativa a la persecución de infracciones administrativas.

- Art.24.2. Vid. ut supra 1.9, segundo guión. En este caso, considera el Defensor del Pueblo que se priva a los individuos de sus derechos de acceso a sus datos en poder de las Administraciones públicas y a que, en su caso, se proceda obligatoriamente por esas Administraciones a su rectificación y cancelación de ser requeridas por el interesado para ello; lo que constituiría asimismo infracción de los artículos 18.1 y 4 y 53.1 de la Constitución. Los mismos reproches que en el punto anterior merece al Tribunal Constitucional la invocación, en este art. 24.2, del “*interés público*” y de la garantía de “*intereses de terceros más dignos de protección*” como fundamento de la imposición de límites a los derechos fundamentales del artículo 18.1 y 4 de la Constitución.

En conclusión, el Tribunal Constitucional declaró contrarios a la Constitución y nulos los siguientes incisos de la Ley Orgánica 15/1999:

- Art. 21.1: “*cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso o*”.

- Art. 24.1: “*impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas*” y “*o administrativas*”.

- Art. 24.2, completo. Por lo tanto, hemos podido comprobar en este apartado como, a iniciativa del Defensor del Pueblo, el Tribunal Constitucional ha introducido algún matiz restrictivo en la situación de prerrogativa que, en materia de protección de datos, ostentan las Administraciones públicas en sus relaciones jurídico-administrativas con los ciudadanos.

3. La caracterización de la protección de datos como derecho subjetivo

La caracterización que en este epígrafe se pretende configurar tropieza con la inicial dificultad de que la Ley Orgánica 15/1999 no contiene una definición específica de un derecho a la protección de datos; enumerando y caracterizando, además, una serie de denominados derechos que inducen la duda razonable de si se está en presencia de un solo derecho subjetivo de protección de datos o de una pluralidad de derechos encaminados a la finalidad común de proteger la privacidad de la persona.

En efecto, la Ley Orgánica enumera y regula los siguientes denominados derechos:

- Derecho de información en la recogida de datos. (Art. 5).
- Consentimiento inequívoco del afectado. (Art. 6.1).
- Derecho de consulta al Registro General de Protección de Datos. (Art.14).
- Los denominados por cierta "praxis" "Derechos ARCO": Acceso, rectificación, cancelación y oposición. (Arts.15 a 17).

La concepción de la protección de datos como un derecho subjetivo, y por tanto, unitario, implica considerar a los derechos enumerados, a pesar de su denominación, no como tales auténticos derechos, sino como meras facultades integradas orgánicamente en aquél. Este punto de vista ha quedado avalado por la Sentencia 292/2000 del Tribunal Constitucional, de la que venimos haciendo mérito. Son dos los aspectos de dicho pronunciamiento judicial los que en esta ocasión conviene poner especialmente de manifiesto, puesto que de ellos se puede deducir lo siguiente:

El carácter de la protección de datos como un derecho subjetivo unitario, y la integración orgánica en el mismo, como meras facultades, de los derechos meramente instrumentales a que venimos haciendo referencia.

3.1. La protección de datos como un derecho subjetivo unitario

Esta es la conclusión que lógicamente cabe extraer de los siguientes pronunciamientos de la Sentencia:

"...el art.18.4 C.E. contiene, en los términos de la [jurisprudencia constitucional] 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...y que se traduce en un derecho de control sobre los datos relativos a la propia persona...

Este derecho fundamental a la protección de datos...consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos... persigue garantizar a [la] 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... El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos... [Su] contenido...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 quien posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso”.

3.2. La integración, como meras facultades, en el derecho subjetivo a la protección de datos, de los denominados derechos contemplados por la L.O. 15/99

Se trata de una conclusión que también cabe extraer con razonable evidencia del contenido de la Sentencia:

“...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 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, -[art.6.1]- el derecho a saber y ser informado sobre el destino y uso de esos datos -[arts.5 y 14]-, y el derecho a acceder, rectificar y cancelar dichos datos -[arts.15 a 17]-.

En definitiva, el poder de disposición sobre los datos personales. 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”.

De manera que, como acabamos de exponer, el Tribunal Constitucional ha contribuido decisivamente a perfilar la dogmática de la protección de datos permitiendo configurarla como un derecho subjetivo en el que se integran orgánicamente, constituyendo “*un haz de facultades*”, los denominados impropiedades derechos de los artículos 5, 6.1, 14 y 15 a 17 de la L.O. 15/99. Este punto de vista ha sido asumido por el propio legislador quién, en el preámbulo del Reglamento, aprobado por Real Decreto 1720/2007, manifiesta que estos derechos de acceso, rectificación, cancelación y oposición al tratamiento, según ha afirmado el Tribunal Constitucional en su sentencia número 292/2000, constituyen el haz de facultades que emanan del derecho fundamental a la protección de datos y sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales.

4. El contenido del derecho subjetivo a la protección de datos

Como acabamos de ver, el contenido del derecho a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que se articula en un correlativo haz de facultades. Aunque ya hemos hecho varias alusiones a estas facultades o derechos -en la terminología de la L.O- proponemos a continuación un examen más pormenorizado de las mismas.

- 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, entre otros extremos, de la existencia y finalidad del fichero, de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición y de la identidad y dirección del responsable del fichero. (Art.5.1).

- Consentimiento del afectado. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, el cual podrá ser revocado con causa justificada. (Art. 6.1 y 3).

- Oposición fundada y legítima a un tratamiento de datos que no requiera consentimiento previo. (Art.6.4).

- No declaración: Nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. (Art.7.1).

- Derecho de impugnación de valoraciones. 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. (Art.13.1).

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. (Art.13.2).

- 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. (Art.14).

- Derecho de acceso. El derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos. (Art. 27.1 del Reglamento). Esencialmente ha sido el derecho de acceso el elemento principal sobre el que se ha basado el concepto doctrinal del “*habeas data*”.

- Derecho de rectificación. El derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos. (Art. 31.1 del Reglamento).

- Derecho de cancelación. El ejercicio del derecho de cancelación dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos. (Art. 31.2 del Reglamento).

- 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:

* Cuando no sea necesario su consentimiento previo, con motivo legítimo y fundado.

* Ficheros para publicidad y prospección comercial.

* 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. (Art. 34 del Reglamento).

- Tutela de los derechos. Las actuaciones contrarias a lo dispuesto en la L.O. 15/99 pueden ser objeto de reclamación por los interesados ante la Agencia Española de Protección de Datos. (Art. 18.1 L.O. 15/99).

- Derecho a indemnización. (Art. 19.1 L.O.15/99)

* En caso de daño o lesión por incumplimiento de la L.O. 15/99.

* Ficheros públicos: Aplicación del régimen de responsabilidad de las Administraciones Públicas. (Art.19.2 L.O.15/99).

- Movimiento internacional de datos. No podrán realizarse transferencias 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 de la L.O. 15/99. (Art. 33.1 L.O.15/99).

- Funciones de la Agencia Española de Protección de Datos.

* Atender las peticiones y reclamaciones formuladas por las personas afectadas.(Art. 37.d) L.O.15/99).

* Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal. (Art. 37.e) L.O.15/99).

5. En particular, el consentimiento del afectado

El poder de disposición y control sobre los propios datos personales en que el derecho subjetivo de protección de datos consiste, implica la realización de diferentes negocios jurídicos, bien para el establecimiento de relaciones jurídicas -relaciones jurídico-administrativas cuando el interlocutor es la Administración-, bien para el mero ejercicio de alguna de las facultades que el derecho atribuye a su titular.

En todas estas actividades resulta obvia la importancia que tiene la prestación por el interesado de un consentimiento libre e informado. El legislador, consciente de ello -“*reviste particular importancia la regulación del modo de captación del consentimiento*” manifiesta el Preámbulo del Reglamento- se ha preocupado, efectivamente, de regular con extensión y detalle las cuestiones relativas a la prestación del consentimiento por los titulares de los datos de carácter personal. Seguidamente vamos a tratar de exponer dicha regulación con cierto pormenor.El tratamiento del consentimiento en el marco de la protección de datos se puede deslindar conceptualmente en tres aspectos diferenciados:

5.1 Consentimiento para el tratamiento de los datos de carácter personal.

5.2 Consentimiento para la comunicación de datos.

5.3 Consentimiento para el tratamiento de datos de menores de edad.

5.1. Consentimiento para el tratamiento de los datos de carácter personal

Dentro de este epígrafe pueden distinguirse, a su vez, varios subapartados:

- 5.1.1. Definición de consentimiento del interesado.
- 5.1.2. Derecho de información en la recogida de datos.
- 5.1.3. Prestación del consentimiento.
- 5.1.4. Revocación del consentimiento.
- 5.1.5. Datos especialmente protegidos.
- 5.1.6. Desarrollo de relaciones jurídicas.

5.1.1. Definición de consentimiento del interesado

Se define como consentimiento del interesado toda manifestación de voluntad:

- Libre
- Específica e
- Inequívoca
- Informada

mediante la que el interesado consienta el tratamiento de datos personales que le conciernen. (Arts .3.h) L.O. 15/99 y 5.1.d) del Reglamento).

Evidentemente, el legislador ha tenido presentes los cuatro vicios clásicos del consentimiento -error, dolo, violencia e intimidación- y con los requisitos impuestos trata de neutralizar la posibilidad de que dichas tachas se materialicen:

- Frente a violencia e intimidación, libertad.
- Frente a error, voluntad inequívoca y específica.
- Frente a dolo, información.

5.1.2. Derecho de información en la recogida de datos

Un consentimiento informado se basa en la información, valga el juego de palabras. Por esa razón, la norma hace especial hincapié en el derecho de información en la recogida de datos. Los interesados a los que se soliciten datos personales deberán ser previamente informados:

- De la existencia del fichero
- De la finalidad de la recogida de datos.
- De los destinatarios de la información.

- Del carácter obligatorio o facultativo de las respuestas.
- De las consecuencias de la obtención de datos o de la negativa a suministrarlos.
- De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- De la identidad y dirección del responsable del tratamiento. (Art. 5.1 L.O. 15/99).

La información que se proporcione, deberá ser *expresa, precisa e inequívoca*; el legislador insiste en ello por dos veces. (Art. 5.1 y 4 L.O. 15/99).

El derecho de información en la recogida de datos tiene su reverso, lógicamente, en el deber de información al interesado. A tal efecto, se formulan dos exigencias reglamentarias:

- Acreditación del cumplimiento y
- Conservación de dicha acreditación mientras persista el tratamiento de datos. (Art. 18 del Reglamento).

5.1.3. *Prestación del consentimiento*

Como sabemos, es en la prestación del consentimiento donde radica la esencia del negocio jurídico y de ahí que el legislador se haya ocupado de ella con cierto pormenor. En concreto, se regulan específicamente los siguientes aspectos de la prestación del consentimiento:

- Solicitud del consentimiento.
- Prestación del consentimiento, propiamente dicha y
- Prueba del consentimiento.

Solicitud del consentimiento. El responsable del tratamiento deberá obtener el consentimiento del interesado para el tratamiento de sus datos de carácter personal. La solicitud del consentimiento deberá concretar:

- El tratamiento o tratamientos que se pretende realizar.
- Finalidad de los mismos.
- Otras condiciones importantes. (Art. 12.1 del Reglamento). El artículo 14 del Reglamento se refiere a la forma de recabar el consentimiento. Nosotros nos ocuparemos de ello seguidamente, en relación con la prestación del consentimiento.

Prestación del consentimiento. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa. (Art. 6.1 L.O. 15/99).

Es muy importante tener presente que, para el tratamiento de los datos de carácter personal, se requiere que el consentimiento sea inequívoco,³ como acabamos de ver, pero de ningún modo se requiere que el consentimiento sea expreso. Con vistas a asegurar el consentimiento inequívoco establece el artículo 12.1 del Reglamento los extremos que debe concretar la solicitud del consentimiento, según antes quedó expuesto. En realidad, la normativa presta poca o ninguna atención al consentimiento expreso y se centra en la regulación del consentimiento tácito, deducido de la inactividad o silencio del interesado. El artículo 14.1 del Reglamento admite esta posibilidad con carácter general, salvo exigencia legal.

Por consiguiente, el responsable podrá dirigirse al afectado cumplimentando el deber de información (Arts. 5 L.O. 15/99 y 18 del 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. (Art. 14.2 del Reglamento). Para salvaguardar las garantías con las que se quiere proteger el consentimiento del interesado, se establecen las siguientes cautelas:

- Certeza de que la comunicación no ha sido devuelta. (Art. 14.3 del Reglamento).

- Proporcionar al interesado un medio sencillo y gratuito para manifestar su negativa. V.gr.:

* Envío prefranqueado al responsable del tratamiento.

* Llamada a un número telefónico gratuito. (Art. 14.4 del Reglamento).

* Servicios de atención al público del responsable del tratamiento.

No se considerarán conformes a lo dispuesto en la Ley los supuestos en que el responsable establezca como medio para que el interesado pueda manifestar su negativa al tratamiento:

1) el envío de cartas certificadas o envíos semejantes,

2) la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o

3) cualesquiera otros medios que impliquen un coste adicional al interesado. (Art. 17.1, segundo párrafo, del Reglamento). Aunque esta

3 Además de libre, específico e informado, como se vio al tratar de su definición.

regla se encuadra en la revocación del consentimiento, consideramos que, según una razonable interpretación gramatical y sistemática, es también aplicable a la negativa al tratamiento de los datos.

Como supuestos en los que se requiere el consentimiento expreso se señalan en la L.O. 15/99 los siguientes:

- Tratamiento de los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se requiere el consentimiento expreso y por escrito del afectado. (Art. 7.2 L.O. 15/99).

- Datos relativos al origen racial, salud y vida sexual. Se requiere consentimiento expreso para su recogida y tratamiento. (Art. 7.3 L.O. 15/99).

- Podría asimilarse a estos casos de consentimiento expreso el supuesto del art. 13.4 L.O. 15/99, según el cual la valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

Prueba del consentimiento. Corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en Derecho. (Art. 12.3 del Reglamento).

5.1.4. Revocación del consentimiento

El consentimiento del afectado para el tratamiento de sus datos de carácter personal podrá ser revocado cuando:

- exista causa justificada y
- no se le atribuyan efectos retroactivos. (Art. 6.3 L.O. 15/99).

El afectado podrá revocar su consentimiento a través de un medio:

- sencillo
- gratuito y
- que no implique ingreso alguno para el responsable del fichero.

En particular, se consideran medios adecuados para vehicular la revocación del consentimiento:

- envío prefranqueado al responsable del tratamiento.
- llamada a un número telefónico gratuito y
- servicios de atención al público del responsable del fichero.

No se consideran, en cambio, procedimientos adecuados:

- el envío de cartas certificadas o similares.
- la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado y
- cualesquiera otros medios que impliquen un coste adicional al interesado. (Art. 17.1 del Reglamento).

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. (Art. 17.2 del Reglamento).

5.1.5. Datos especialmente protegidos

El artículo 7 de la LO. 15/99 confiere una especial protección a los datos relativos a: Ideología, Origen racial, Religión, Salud, Creencias, Vida sexual y Afiliación sindical.

Ya hemos visto con anterioridad como se requiere consentimiento expreso para el tratamiento de varias de estas categorías de datos personales.

5.1.6. Desarrollo de relaciones jurídicas

Se contemplan en la normativa una serie de supuestos que, desde nuestro punto de vista, constituyen una manifestación del principio general resultante del artículo 1.258 del Código Civil que obliga a atenerse a las consecuencias que constituyan una derivación lógica o razonable del consentimiento inicialmente prestado.

Según la trasposición de este principio al ámbito de la protección de datos, no sería exigible el consentimiento para el tratamiento o la cesión de los datos cuando ello fuere la consecuencia lógica del desarrollo normal de relaciones jurídicas establecidas con anterioridad. Así:

- No será preciso el consentimiento para el tratamiento de datos personales cuando los mismos 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. (Art. 6.2 L.O. 15/99).

- No será preciso el consentimiento para una comunicación o cesión de datos 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. (Art. 11.2.c) L.O. 15/99).

- No serán de aplicación las precauciones y requisitos en materia de movimiento internacional de datos 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. (Art. 34.f) L.O. 15/99).

- Los datos de carácter personal podrán tratarse sin necesidad del consentimiento del interesado cuando 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. (Art. 10.3.b) del Reglamento).

- Será posible la cesión de datos de carácter personal sin contar con el consentimiento del interesado cuando la misma responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de los datos. (Art. 10.4.a) del Reglamento). Este consentimiento implícito no se debe entender aplicable a finalidades que no guarden relación directa con el mantenimiento, desarrollo o control de la relación jurídica, según resulta del artículo 15 del Reglamento.

5.2. Consentimiento para la comunicación de datos

El consentimiento para el tratamiento de datos de carácter personal no se debe confundir con el consentimiento para la comunicación de datos, que la normativa contempla con una sustantividad propia y diferenciada y en el que cabe apreciar los siguientes aspectos:

5.2.1. Definición de cesión

5.2.2. Sustantividad normativa propia

5.2.3. Supuestos de consentimiento para cesión de datos

5.2.4. Ficheros públicos

5.2.1. Definición de cesión o comunicación de datos

Tratamiento de datos que supone su revelación a una persona distinta del interesado. (Arts. 3.i) L.O. 15/99 y 5.1.c) del Reglamento).

5.2.2. Sustantividad normativa propia del consentimiento para la comunicación de datos respecto al consentimiento para el tratamiento de datos

Esto es algo que resulta de los siguientes preceptos y consideraciones:

- Distinta ubicación sistemática. Consentimiento para el tratamiento en el artículo 6.1 de la L.O. 15/99 y consentimiento para la cesión en el artículo 11.1.

En el Reglamento, consentimiento para el tratamiento en los artículos 10.3 y 12.1 y consentimiento para la cesión en los artículos 10.4 y 12.2.

- “*El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable*” (Art. 11.4 L.O. 15/99). El empleo del adverbio “*también*” denota la distinción entre ambos supuestos de consentimiento, a saber: consentimiento para el tratamiento y consentimiento para la cesión.

5.2.3. Supuestos de consentimiento para cesión de datos

La normativa contempla los siguientes:

- Regla general: Los datos de carácter personal únicamente podrán ser objeto de cesión si el interesado hubiera prestado previamente su consentimiento para ello. (Art. 10.1 del Reglamento). Esta formulación es más general que la de la Ley, que contempla la condición de que la cesión sea para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario. (Art. 11.1 L.O. 15/99).

- Datos relativos a la ideología, afiliación sindical, religión y creencias. Se requiere el consentimiento previo del afectado para la cesión de los mismos. (Art. 7.2 L.O. 15/99).

- Datos relativos al origen racial, salud, y vida sexual. Se precisa que el afectado consienta expresamente la cesión de los mismos. (Art. 7.3 L.O. 15/99).

- Los datos recogidos por las Administraciones públicas de fuentes accesibles al público no podrán comunicarse a ficheros de titularidad privada sin el consentimiento del interesado. (Art. 21.3 L.O. 15/99).

- Podrá prescindirse de la Norma general en materia de movimiento internacional de datos cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista. (Art. 34.e) L.O. 15/99 y 66.2.b) del Reglamento).

5.2.4. Ficheros públicos

Las disposiciones de creación de los ficheros de las Administraciones públicas deberán indicar, entre otros extremos, las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros. (Arts. 20.2.e) L.O. 15/99 y 54.1.d) y e) del Reglamento).

5.3. Consentimiento para el tratamiento de datos de menores de edad

Pueden distinguirse las siguientes reglas, todas ellas recogidas en el artículo 13 del Reglamento:

- Mayores de catorce años: Consentimiento de los mismos, salvo que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela.

- Menores de catorce años: Se requerirá el consentimiento de los padres o tutores.

- Prohibición de recabar del menor datos sobre su entorno familiar.

- Información dirigida a los menores con ocasión de un tratamiento de datos: En lenguaje fácilmente comprensible por los mismos.

- Comprobación garantizada de la edad del menor.

- Comprobación garantizada de la autenticidad del consentimiento prestado por los padres, tutores o representantes legales.

VI. CRONOLOGÍA DE LA INCORPORACIÓN DE LA PROTECCIÓN DE DATOS A LA RELACIÓN JURÍDICO-ADMINISTRATIVA

Con este epígrafe, breve inciso en realidad, se trata de mostrar, por razones de claridad expositiva, el “iter” de la incorporación de la protección de datos al procedimiento administrativo, núcleo y esencia de la relación jurídico-administrativa.

La integración de la protección de datos en la relación jurídico-administrativa va íntima e indisolublemente unida al proceso de incorporación de las nuevas tecnologías a la actuación de las Administraciones públicas. Desde esta perspectiva podemos distinguir dos fases claramente diferenciadas:

1ª) Desde la entrada en vigor de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Es una etapa que en su primera parte coincidió con la vigencia de la primitiva ley de protección de datos, la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal y que, coincidiendo prácticamente con el cambio de milenio, presenta una segunda parte bajo la vigencia de la actual L.O. 15/99.

2ª) La segunda fase se inicia con la promulgación de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios

Públicos. Es un momento en que ya está bastante “rodada” la L.O. 15/99 pero que presenta un hito muy importante con la entrada en vigor, en la primavera de 2008, del Reglamento, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

Veamos seguidamente el contenido de cada una de esas fases.

VII. PROTECCIÓN DE DATOS Y PROCEDIMIENTO ADMINISTRATIVO COMÚN

Ya hemos dicho como la incorporación de la normativa sobre protección de datos a la “praxis” del procedimiento administrativo común va indisolublemente unida a la incorporación de las nuevas tecnologías de la información y de la comunicación a la práctica de las Administraciones públicas. Vamos a exponer brevemente la evolución de este doble proceso a través de la Ley 30/92 y disposiciones subsiguientes y/o de desarrollo.

- Ley 30/92. Contempla la incorporación de las nuevas tecnologías al procedimiento administrativo.

En el derecho de acceso a Archivos y Registros (art.37) entremezcla disposiciones de carácter técnico con otras más propias de la protección de datos:

* Los ciudadanos tienen derecho a acceder a los registros y a los documentos que, formando parte de un expediente, obren en los archivos administrativos, cualquiera que sea la forma de expresión, gráfica, sonora o en imagen o el tipo de soporte material en que figuren.

* El acceso a los documentos que contengan datos referentes a la intimidad de las personas estará reservado a éstas, que, en el supuesto de observar que tales datos figuran incompletos o inexactos, podrán exigir que sean rectificadas o completadas.

* El ejercicio de los mencionados derechos podrá ser denegado cuando prevalezcan razones de interés público, por intereses de terceros más dignos de protección o por disposición legal.

* Se contemplan excepciones que recuerdan claramente a las de la normativa de protección de datos, tales como Defensa Nacional, Seguridad del Estado e investigación de delitos.

En materia de Registros de entrada y salida de documentos (art.38) se establece que el sistema garantizará la integración informática en el

registro general de las anotaciones efectuadas en los restantes registros del órgano administrativo. Mediante convenios de colaboración suscritos entre las Administraciones públicas se establecerán sistemas de intercomunicación y coordinación de registros que garanticen su compatibilidad informática así como la transmisión telemática de asientos y documentos. El artículo 45 se ocupa específicamente de la incorporación de medios técnicos, entretejiendo nuevamente disposiciones técnicas y garantistas.

Las Administraciones públicas impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y el ejercicio de sus competencias, con las limitaciones que a la utilización de estos medios establecen la Constitución y las Leyes. Asimismo se dispone que la gestión de documentos mediante estas técnicas estará sujeta al cumplimiento de las garantías legales.

- Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.

Tiene como criterio inspirador el recoger las garantías y derechos de los ciudadanos frente a la Administración cuando esta utiliza las tecnologías de la información. En el artículo 2 -derechos de los ciudadanos y limitaciones- se vela por la garantía del honor y la intimidad personal y familiar de los ciudadanos conforme a la entonces vigente L.O. 5/92; ateniéndose a las limitaciones sobre la utilización de estas técnicas establecidas por la Constitución.

- Real Decreto 772/1999, de 7 de mayo, por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias de documentos y devolución de originales y el régimen de las oficinas de registro.

En medio de una normativa de carácter predominantemente técnico-administrativo, figura alguna disposición más propia de la protección de datos, como es la denegación de copias auténticas de documentos públicos administrativos en supuestos tales como:

* Cuando concurren razones de protección del interés público o de protección de intereses de terceros.

* Investigación de delitos y peligro de los derechos y libertades de terceros.

* Defensa Nacional o Seguridad del Estado. (Art. 9.4).

- Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.

Tanto en el Preámbulo como en el articulado (art. 1.2) se resalta que el uso de los medios y técnicas telemáticas se hará de acuerdo con lo dispuesto en la L.O. 15/99. Se incluye asimismo una referencia en el mismo sentido en el R.D. 263/96 del que antes hemos hecho mérito. (Art. 2.2).

- Ley 59/2003, de 19 de diciembre, de firma electrónica.

En su artículo 17 -protección de los datos personales- se contienen tres referencias a la L.O.15/99:

* Remisión general de cumplimiento.

* Prohibición de incluir en los certificados electrónicos los datos especialmente protegidos del artículo 7 de la L.O. 15/99.

* Obligación de revelar la identidad de los firmantes cuando lo soliciten el Defensor del Pueblo, el Ministerio Fiscal, los Jueces o Tribunales o el Tribunal de Cuentas. (Vid. art. 11.2.d) L.O. 15/99).

VIII. PROTECCIÓN DE DATOS Y ADMINISTRACIÓN ELECTRÓNICA

La expresión “*Administración electrónica*” figura en el documento “PLAN DE CHOQUE PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA EN ESPAÑA”, de 8 de mayo de 2003, de los Ministerios de Ciencia y Tecnología y de Administraciones Públicas. En dicho documento se concibe a la Administración electrónica como “*una vía para avanzar hacia el desarrollo del “mejor gobierno” de las Administraciones Públicas, en donde la tecnología es fundamentalmente un medio...que debe responder a la optimización y reorganización de los esquemas del servicio público, de tal forma que permitan una mayor eficiencia y eficacia en las relaciones con los ciudadanos y empresas...*” (pág. 7). “*La Administración electrónica debe permitir una transformación en la forma de ofrecer los servicios de la Administración General del Estado...[tendiendo] hacia un modelo “integrador” centrado en el usuario*”. (pág. 8). Es en esta línea donde puede situarse la promulgación de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

En realidad, nada nuevo ofrece esta Ley en materia de protección de datos cuya regulación, en el momento de su entrada en vigor, constituía

una práctica ya firmemente asentada en la actividad de las Administraciones públicas. Ello no obstante, resulta evidente que, por la materia misma de la Ley, la aplicación de la normativa de protección de datos a esta innovadora manifestación del procedimiento administrativo es algo que debe tenerse muy presente. Por lo tanto, y desde el punto de vista de nuestro estudio, conviene fijar la atención en los siguientes aspectos:

1. El procedimiento administrativo-electrónico.
2. La superación de temores y recelos ante la utilización de las nuevas tecnologías y
3. Protección de datos y Administración electrónica.

1. El procedimiento administrativo-electrónico

Uno de los objetivos de la Ley 11/2007 es implantar el procedimiento electrónico, esto es, establecer la posibilidad de realizar todos los trámites y actuaciones propios del procedimiento administrativo común por medios electrónicos, sin merma de la eficacia administrativa ni de la seguridad jurídica. En la Exposición de Motivos ya se configura la relación con las Administraciones públicas por medios electrónicos como un derecho de los ciudadanos y como una obligación correlativa para dichas Administraciones. Y así, en el artículo 6.1 se reconoce a los ciudadanos el derecho a relacionarse con las Administraciones públicas utilizando medios electrónicos para el ejercicio de los derechos previstos en el artículo 35 de la Ley 30/92 -Derechos de los ciudadanos-, así como para:

- Obtener informaciones
- Entablar pretensiones
- Realizar consultas y alegaciones
- Efectuar pagos
- Formular solicitudes
- Realizar transacciones y
- Manifestar consentimiento
- Oponerse a las resoluciones y actos administrativos.

Todo ello sin merma del principio de legalidad en cuanto al mantenimiento de la integridad de las garantías jurídicas de los ciudadanos ante las Administraciones públicas establecidas en la Ley 30/92. (Art. 4.d) Ley 11/07).

Tras estas consideraciones de carácter general puede abordarse la definición de expediente electrónico, considerado como el conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan. (Art. 32.1 Ley 11/07).

La iniciación de un procedimiento administrativo a solicitud del interesado por medios electrónicos requerirá la puesta a disposición de los interesados de los correspondientes modelos o sistemas electrónicos de solicitud en la sede electrónica que deberán ser accesibles sin otras restricciones tecnológicas que las estrictamente derivadas de la utilización de estándares y criterios de comunicación y seguridad aplicables de acuerdo con las normas y protocolos nacionales e internacionales. (Art. 35.1 Ley 11/07).

En cuanto a la instrucción del procedimiento utilizando medios electrónicos, las aplicaciones y sistemas de información utilizados al efecto deberán garantizar el control de los tiempos y plazos, la identificación de los órganos responsables de los procedimientos así como la tramitación ordenada de los expedientes y facilitar la simplificación y la publicidad de los procedimientos. Cuando se utilicen medios electrónicos para la participación de los interesados en la instrucción del procedimiento a los efectos del ejercicio de su derecho a presentar alegaciones, se emplearán los medios de comunicación y notificación legalmente previstos a tal efecto. (Art. 36.1 y 3, en relación con 27 y 28, Ley 11/07). La resolución de un procedimiento utilizando medios electrónicos garantizará la identidad del órgano competente mediante el empleo de alguno de los instrumentos legalmente previstos a tal efecto, a saber, firma electrónica para la actuación administrativa automatizada y firma electrónica del personal al servicio de las Administraciones Públicas. (Art. 38.1, en relación con 18 y 19, Ley 11/07)

2. La superación de temores y recelos ante la utilización de las nuevas tecnologías

No tiene nada de extraño que las nuevas tecnologías, verdaderamente inusitadas para muchos de los potenciales usuarios, levanten temores y recelos entre los mismos en cuanto a la certeza y conservación de las actuaciones, seguridad jurídica, confidencialidad, etc.

El legislador fue consciente de este estado de cosas y ha tratado, al poner en marcha la Administración electrónica, de disipar temores y

recelos: *“...el principal reto que tiene la implantación de las Tecnologías de la Información y las Comunicaciones (TIC) en la sociedad en general y en la Administración en particular es la generación de confianza suficiente que elimine o minimice los riesgos asociados a su utilización. La desconfianza nace de la percepción, muchas veces injustificada, de una mayor fragilidad de la información en soporte electrónico, de posibles riesgos de pérdida de privacidad y de la escasa transparencia de estas tecnologías. Por otro lado, la legislación debe proclamar y erigirse sobre un principio fundamental como es la conservación de las garantías constitucionales y legales a los derechos de los ciudadanos y en general de las personas que se relacionan con la Administración Pública, cuya exigencia se deriva del artículo 18.4 C.E. Las anteriores consideraciones cristalizan en un Estatuto del ciudadano frente a la administración electrónica que recoge un elenco no limitativo de las posiciones del ciudadano en sus relaciones con las Administraciones Públicas, así como las garantías específicas para su efectividad”*. (E. de M. Ley 11/07).

En consecuencia, el artículo 3.3 de la Ley 11/07 señala como uno de los fines de la misma:

“crear las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos”.

Y, como principio general, se establece el de *“seguridad en la implantación y utilización de los medios electrónicos por las Administraciones Públicas, en cuya virtud se exigirá al menos el mismo nivel de garantías y seguridad que se requiere para la utilización de medios no electrónicos en la actividad administrativa”*. (Art. 4.f) Ley 11/07)

3. Protección de datos y Administración electrónica

Acabamos de ver como una de las vías que el legislador señala para fomentar la confianza en el uso de los medios electrónicos es la preservación de la protección de datos de carácter personal -(Art. 3.3 Ley 11/07)- en la línea de conservar las garantías constitucionales de los derechos de los ciudadanos derivados del artículo 18.4 de la Constitución.

Hemos dicho con anterioridad que la Ley 11/07 no introduce ninguna novedad en materia de protección de datos, lo cual no es óbice para que el legislador haga un llamamiento a su estricto cumplimiento: *“Las normas de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal deben bastar, y no se trata de hacer ninguna innovación al respecto, pero si de establecer previsiones que garanticen la utilización de los datos obtenidos de las comunicaciones electrónicas para el fin preciso para el que han sido remitidos a la Administración”*. (E. de M. Ley 11/07). Se establecen así el Principio general del respeto al derecho a la protección de datos de carácter personal en los términos establecidos por la L.O. 15/99, (Art. 4.a) Ley 11/07) y el correlativo Derecho de los ciudadanos a la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas. (Art. 6.2.i) Ley 11/07).

La misma sujeción a la L.O. 15/99 encontramos en la cesión de datos entre Administraciones Públicas del artículo 9.1 de la Ley 11/07.

IX. EN RESUMEN

La protección de datos de carácter personal constituye un sistema de protección de la intimidad y de la dignidad del titular de dichos datos arbitrado por el legislador en cumplimiento del mandato contenido en el artículo 18.4 de la Constitución. Según nuestro punto de vista, dicha protección es incardinable en el esquema teórico del derecho subjetivo clásico. Sentado lo anterior, hemos tratado de observar como opera dicho derecho subjetivo en el ámbito de la relación jurídico-administrativa, esto es, en la interacción del sujeto con la Administración Pública.

En dicho contexto, el derecho a la protección de datos de carácter personal queda sujeto a ciertas limitaciones provenientes de la prerrogativa administrativa; si bien dichas limitaciones han sido objeto de alguna matización por parte de la jurisprudencia constitucional.

Por último, hemos analizado la operatividad del derecho a la protección de datos de carácter personal en el marco normativo específico de la relación jurídico-administrativa: el procedimiento administrativo común y, más especialmente, el procedimiento electrónico, concreción sustancial de la denominada Administración electrónica.

BIBLIOGRAFÍA

- BUSTOS PUECHE, José Enrique (2008): “*Manual sobre bienes y derechos de la personalidad*”, 2ª ed., Madrid, Ed. Dykinson, pág.19.
- CASTÁN TOBEÑAS, José (1984): “*Derecho Civil español, Común y Foral*”, T.I, VOL.II, 14ª ed., Madrid, Ed. REUS, S.A., pág.366.