

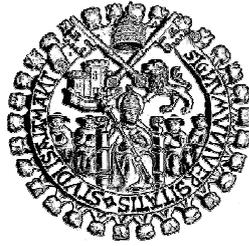


UNIVERSIDAD DE SALAMANCA
Facultad de Traducción y Documentación
DEPARTAMENTO DE BIBLIOTECONOMÍA Y DOCUMENTACIÓN

Protección de datos en archivos públicos: introducción a su estudio

Trabajo que presenta Francisco Fernández Cuesta,
para la obtención del Grado de Salamanca,
bajo la dirección del Dr. D. Luis Hernández Olivera

SALAMANCA, 2011



UNIVERSIDAD DE SALAMANCA
Facultad de Traducción y Documentación
DEPARTAMENTO DE BIBLIOTECONOMÍA Y DOCUMENTACIÓN

Protección de datos en archivos públicos: introducción a su estudio

Trabajo que presenta Francisco Fernández Cuesta,
para la obtención del Grado de Salamanca,
bajo la dirección del Dr. D. Luis Hernández Olivera

SALAMANCA, 2011

Protección de datos en archivos públicos: introducción a su estudio

Trabajo presentado para la obtención del Grado de Salamanca por la Universidad de Salamanca.

Elaborado por D. Francisco Fernández Cuesta, Licenciado en Historia por la Universidad de Cantabria.

Dirigido por el Dr. D. Luis Hernández Olivera, Profesor Titular de Universidad, del Departamento de Biblioteconomía y Documentación, de la Universidad de Salamanca.

Vº Bº

Índice	I
Siglas y abreviaturas empleadas	V
Introducción	3
Un fenómeno nuevo y unos presuntos implicados	3
Objetivos, metodología y estructura del trabajo	6
Agradecimientos	10
0. Ámbito de análisis: los archivos de la Administración General del Estado	11
0.1. Los archivos como servicio o institución. Los archivos públicos	11
0.2. Los sistemas de archivos	19
0.3. El sistema archivístico de la Administración General del Estado	23
1. La articulación de un derecho fundamental a la protección de datos	39
1.1. Ponerle vallas al campo. La amenaza informática y la necesidad de regular el tratamiento de datos de carácter personal	39
1.2. Un derecho europeo para la protección de datos de carácter personal	45
1.3. La configuración del derecho fundamental a la protección de datos en España	51
2. El régimen de la protección de datos en España	57
2.1. El objeto del derecho: los datos personales y su tratamiento en ficheros de datos. Datos especialmente protegidos	57
2.1.1. Los datos personales y su tratamiento	57
2.1.2. La importancia del concepto de fichero de datos	62
2.1.3. Datos sensibles o especialmente protegidos	65

2.2. El concepto de fichero y la delimitación del objeto de protección en los archivos públicos	67
2.2.1. La opinión de la doctrina jurídica. El criterio “totalizador”	68
2.2.2. La defensa del criterio totalizador por las autoridades de control	70
2.2.3. Jurisprudencia en torno a un caso paradigmático: la polémica de los Libros de Bautismo	72
2.3. El contenido del derecho: principios de la protección de datos y derechos de las personas	77
2.3.1. Principios de la protección de datos: calidad, consentimiento y finalidad	77
2.3.2. Derechos de las personas	81
2.4. La Agencia Española de Protección de Datos	89
2.5. Medidas de seguridad	93
2.5.1. Cuestiones generales y clasificación de las medidas	93
2.5.2. Medidas técnicas y organizativas	95
2.5.3. Instrumentos administrativos: documento de seguridad, auditorías y formación	100
2.6. Breve mención al régimen específico de los ficheros públicos	103
3. Ficheros y tratamientos de datos en los archivos públicos	107
3.1. El objeto de protección en los archivos	107
3.1.1. Los ficheros del archivo: propuesta de sistematización	107
3.1.2. Tratamientos de datos de los archivos públicos	110
3.2. Cuando los archivos crean ficheros: algunas cuestiones referidas a la recogida de datos	113
3.2.1. Protección de datos en la gestión de usuarios de los Archivos Estatales	113
3.2.2. Los sistemas descripción archivística como ficheros de datos	119
3.2.3. Algunas consideraciones sobre la importancia de los sistemas de descripción archivística desde la perspectiva de la protección de datos	122

3.3. ¿Conservación a largo plazo de los datos o cancelación?	125
3.3.1. Conservación a largo plazo: una excepción controlada por la AEPD	125
3.3.2. Implicaciones de la cancelación de datos sobre el patrimonio documental: el caso de los ficheros de la Dirección General de Instituciones Penitenciarias	130
3.3.3. La destrucción incontrolada de documentos: buena práctica para la AEPD	134
4. Comunicaciones de datos en los archivos de la AGE	137
4.1. Las transferencias como cesión de datos	137
4.2. Breve referencia a los préstamos	141
4.3. El acceso a los documentos como cesión de datos	143
4.3.1. Una necesaria habilitación legal	143
4.3.2. Regulación legal del acceso a los documentos en los archivos de la AGE	145
4.3.3. Acceso a los documentos y principio de calidad	149
4.4. Los problemas de la difusión de información archivística	153
4.4.1. El fichero "Guerra Civil y Franquismo"	153
4.4.2. El Portal de Víctimas de la Guerra Civil y Represaliados del Franquismo	157
5. Las medidas de seguridad como función archivística	165
5.1. Modelo básico de responsabilidades del archivo en materia de seguridad	165
5.2. Seguridad y acceso en las normas ISO 15.489:2001	167
6. Conclusiones	175

7. Fuentes	181
7.1. Bibliografía	181
7.2. Documentos de la AEPD mencionados en el texto	189
Anexos	193
Anexo 1. Formulario de recogida de datos para la apertura de expediente de usuario de los Archivos Estatales	193
Anexo 2. Oficio del Subdirector General de los Archivos Estatales, de 22 de abril de 2010, solicitando a la AEPD informe jurídico sobre la publicación en la Red de una base de datos sobre víctimas de la Guerra Civil y la represión franquista	197
Anexo 3. Anexo 3. Informe de la Agencia Española de Protección de Datos, de 25 de mayo de 2010 (ref. de entrada 142746/2010) sobre la consulta del Subdirector General de los Archivos Estatales	203

SIGLAS Y ABREVIATURAS EMPLEADAS

AEPD	Agencia Española de Protección de Datos
AGA	Archivo General de la Administración
AGE	Administración General del Estado
AHN	Archivo Histórico Nacional
AHP	Archivo Histórico Provincial / archivos históricos provinciales
APDCM	Agencia de Protección de Datos de la Comunidad de Madrid
CE	Constitución Española
CSCDA	Comisión Superior Calificadora de Documentos Administrativos
DTA-SGAE	<i>Diccionario de Terminología Archivística</i> de la Subdirección General de los Archivos Estatales, 2ª ed. (SGAE 1995)
ICA	International Council on Archives (Consejo Internacional de Archivos)
IJ	Informe jurídico de la Agencia Española de Protección de Datos
LMH	Ley 52/2007, de 26 diciembre, por la que se reconocen y amplían derechos y se establecen medidas en favor de quienes padecieron persecución o violencia durante la guerra civil y la dictadura (Ley de la Memoria Histórica)
LOFAGE	Ley 6/1997, de 14 abril, de organización y funcionamiento de la Administración General del Estado
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
LORTAD	Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal
LPAC	Ley 30/1992, de 26 de noviembre, de régimen jurídico de las Administraciones Públicas y del procedimiento administrativo común
LPHE	Ley 16/1985, de 25 junio, del Patrimonio Histórico Español
Reglamento	Real Decreto 1720/2007, de 21 de diciembre, por el se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
SAN	Sentencia de la Audiencia Nacional
STC	Sentencia del Tribunal Constitucional

Los recursos del ordenador para el tratamiento de datos han despertado temores sobre la incidencia de esta nueva técnica en las libertades individuales. Se cuestiona sobre la posibilidad, en estas circunstancias, de mantener las garantías actuales del secreto de datos y el respeto de las reglas protectoras de la vida privada, de las libertades privadas y públicas. Y se exagera, sin duda alguna.

SERRA NAVARRO, P. 1980. Los archivos y el acceso a la documentación. Lección de clausura del curso académico 1977-1978 de la Escuela de Documentalistas. Madrid: Subdirección General de Archivos

INTRODUCCIÓN

Un fenómeno nuevo y unos presuntos implicados

La existencia de una normativa destinada a proteger los datos de carácter personal es un fenómeno relativamente nuevo. Su corta trayectoria provoca que aún en la actualidad –cuando se han cumplido 30 años del primer texto internacional sobre la materia, inspirador de los posteriores desarrollos legislativos nacionales europeos, el Convenio 108 del Consejo de Europa¹, y casi 20 de la primera ley específica en nuestro país, la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (en adelante, LORTAD)- sea algo poco conocido, tanto por parte de los ciudadanos en general² como por aquellos responsables de tratar de una u otra forma con información de carácter personal. Y, a mayor abundamiento, supone que aún sea poco uniforme su interpretación –y, por tanto, su aplicación- por parte de las autoridades de control y los órganos judiciales. Esta circunstancia, como ha señalado Messía de la Cerda (2008), “ha obligado a los diversos agentes involucrados a realizar un esfuerzo de análisis, adaptación y aplicación”.

¿Forman parte los archivos de estos agentes? Y, en caso afirmativo, ¿en qué medida están involucrados? ¿Se ha realizado el esfuerzo de análisis,

¹ Convention (ETS nº 108) for the protection of individuals with regard to automatic processing of personal data. El instrumento de su ratificación por parte de España, así como la traducción al castellano de este Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, se publicó en el BOE nº 274, de 15 de noviembre de 1985.

² Muchos autores, como M.A. Davara (cit. en Serrano 2003, p. 18, n. 1), han llamado la atención sobre la ausencia general de una cultura de la protección de datos y el desconocimiento de la normativa que regula esta materia por parte de la ciudadanía. No obstante, las Memorias anuales de la Agencia Española de Protección de Datos vienen destacando la progresiva concienciación de los ciudadanos con los riesgos asociados a sus datos personales y los derechos al respecto que les amparan.

adaptación y aplicación necesario para cumplir con la normativa vigente sin menoscabo de las funciones atribuidas a los archivos? A pesar de que no existe mucha bibliografía profesional al respecto³, en algunos Manuales de Archivística se ha empezado a considerar que la normativa de protección de datos sí afecta a los archivos, especialmente a los públicos, concretamente en lo referido a la accesibilidad legal⁴ de los documentos.

- Así, Duplá (1997) considera que esta normativa afecta “muy directamente a la accesibilidad de los documentos” (p. 209) y, por tanto, ha de ser tenida en cuenta por los archivos al determinar la accesibilidad en los procesos de análisis, identificación y valoración de series documentales (p. 200).
- Alberch (2003) apenas menciona la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal al analizar la

³ Basta consultar la principal base de datos bibliográfica especializada en Archivística de nuestro país, el Catálogo Colectivo de la Red de Bibliotecas de los Archivos Estatales, coordinado por el Centro de Información Documental de Archivos (CIDA) del Ministerio de Cultura (Subdirección General de los Archivos Estatales). Disponible en: <http://www.mcu.es/ccbae/es/inicio/inicio.cmd> [Consulta: 13 junio 2011]. Los resultados que arroja la búsqueda por el término “protección de datos” –tanto en título como en materia– son desalentadores: la única referencia de un archivero español que aparece es la de Hernández (2007), con un breve artículo en el que comenta la necesidad de destruir adecuadamente los documentos par evitar fraudes e infracciones, a la luz de diversos informes sobre seguridad de la información. Dicho artículo se publicó en *Archivamos*, revista archivística de actualidad de la Asociación de Archiveros de Castilla y León, en la que periódicamente aparecen noticias sobre estas cuestiones. Desde un punto de vista más doctrinal, encontramos algunas referencias a la normativa de protección de datos en la bibliografía relativa al derecho de acceso a los archivos. Destacan en este sentido los trabajos de Gómez-Llera (por ejemplo, 2009), quien aborda la cuestión desde un punto de vista práctico y relativamente novedoso (al aplicarlos a los archivos históricos, muchas veces olvidados en la bibliografía profesional a pesar de ser el tipo de centro que cuenta con más personal técnico). No obstante, no se ha realizado aún un estudio integral de la relación protección de datos – archivos.

⁴ De acuerdo con el Diccionario de Terminología Archivística (en adelante, DTA-SGAE), la accesibilidad es la posibilidad de consulta de los documentos de archivo, determinada por la normativa vigente, su control archivístico y su estado de conservación. Dada esta triple vertiente, y para evitar la confusión con su acepción general de grado en el que todas las personas pueden utilizar un objeto, visitar un lugar o acceder a un servicio, independientemente de sus capacidades técnicas, cognitivas o físicas (véase “Accesibilidad”. En: *Wikipedia* [sitio web]. [Consulta: 28 nov. 2010]. Disponible en: <<http://es.wikipedia.org/wiki/Accesibilidad>>), preferimos emplear el término “accesibilidad legal”. Término que, por otra parte, viene siendo utilizado por el propio Ministerio de Cultura (véase su Portal de Víctimas de la Guerra Civil y Represaliados del Franquismo <<http://pares.mcu.es/victimasGCFPortal/staticContent.form?viewName=copia>> [Consulta: 28 nov. 2010]).

Por otro lado, la especial consideración en este sentido de los archivos públicos viene dada por ser los únicos que, en principio, se encuentran obligados legalmente a ofrecer servicio al conjunto de los ciudadanos, a quienes también legalmente se les reconoce el derecho de acceder a los mismos y a los documentos que conservan. Sobre este tipo de archivos, especialmente los integrados en el sistema archivístico de la Administración General del Estado, centraremos nuestro trabajo.

normativa que afecta de forma sectorial a los archivos, destacando que ésta y otras leyes “inciden claramente en la operatividad de los archivos y refuerzan su carácter democrático y de servicio a los ciudadanos”⁵ (p. 43). También, cuando aborda el derecho de acceso a los archivos y documentos (p. 195), hace mención a esta Ley, que introduce

una serie de cautelas dirigidas a preservar el uso de los datos personales que figuren en ficheros automatizados, tanto del sector público como del privado. Los miles de expedientes de sanción incoados por la Agencia de Protección de Datos a empresas privadas e instituciones públicas a causa del uso indebido de datos personales evidencian la magnitud y la gravedad del problema.

- Cruz Mundet (2003) resume brevemente -apenas unos párrafos- el contenido de la LOPD, al concluir un capítulo sobre la legislación estatal que regula el derecho de acceso a la documentación pública. Aunque considera que “no posee una relación tan directa con los archivos” como otras normas (p. 335), cree que

su ámbito de actuación es confluyente en buena manera con el nuestro, ya que desarrolla el artículo 18.4 de la Constitución y en parte también el 105 b), en tanto tiene la misión de proteger la intimidad de las personas en relación con el uso de los datos de carácter personal, especialmente mediante sistemas informáticos.

- Más importancia le otorgará este mismo autor en su manual de 2006 - que sigue las directrices de las ISO 15489⁶-, en el que encuadra la legislación sobre protección de datos entre la normativa que influye directamente en los archivos y que, por tanto, ha de ser analizada y tomada en cuenta a la hora de planificar y poner en marcha un sistema de gestión de documentos en una organización (p. 90); para formar

⁵ Sin embargo, señala a continuación Alberch, la efectividad de estas leyes “que estipulan unos derechos ciudadanos [...] sólo se pueden garantizar en el marco de una función pública que disponga de unos procesos administrativos eficientes y con unos archivos ordenados correctamente”, situación que -como dice este autor- está lamentablemente lejos de la realidad.

⁶ ISO 15489-1:2001. *Información y documentación. Gestión de documentos. Parte 1: Generalidades*; completada con la ISO/TR 15489-2:2001. *Información y documentación. Gestión de documentos. Parte 2: Directrices*, guía de implementación de la anterior para su uso por parte de los profesionales de la gestión de documentos y de aquellas personas encargadas de gestionar documentos en sus respectivas organizaciones. Ambas han sido traducidas y publicadas por AENOR como normas UNE en 2006.

parte, finalmente, del reglamento del sistema⁷, ya que determina uno de los puntos críticos del mismo, el del acceso a la información y a los documentos (pp. 276-279).

A pesar de ello, la Archivística española no ha analizado aún en profundidad la relación entre la normativa de protección de datos y los archivos. Tampoco lo ha hecho el mundo del Derecho, aunque en los últimos años hayan sido numerosas las monografías y artículos, ponencias y comunicaciones, que han elaborado distintos juristas sobre la protección de los datos de carácter personal y sobre el derecho de acceso a la información pública⁸, y que tocan de alguna manera los archivos públicos. Aunque cuando esto sucede, en raras ocasiones se realiza desde una concepción integral de los mismos, abarcando todo el ciclo de vida de los documentos -de las oficinas a los archivos históricos- y los distintos aspectos relacionados con su gestión y la administración de los centros encargados (al menos en teoría) de la misma, de su custodia y de su servicio⁹.

Objetivos, metodología y estructura del trabajo

Retomando las preguntas que nos hacíamos arriba, podemos adelantar, por tanto, que, si bien para algunos autores los archivos –en especial los públicos- forman parte de los agentes afectados por la normativa de protección de datos -al menos en lo que se refiere a su papel como proveedores de información pública-, aún no se ha realizado un análisis

⁷ Norma básica interna, aprobada al más alto nivel de la organización, “que establece y garantiza el pleno desarrollo funcional del sistema: su ubicación, estructura, recursos y régimen de funcionamiento” (Cruz 2006, p. 267).

⁸ Si bien, como ha señalado Guichot (2009, p. 198), “no hay estudios monográficos relevantes conocidos por nosotros que analicen el encaje entre ambos derechos”. Quizás destaque la propia obra de Guichot, la de Castillo (2007a) y el extenso artículo de Troncoso (2008).

⁹ Remitimos a la Bibliografía para una selección de la doctrina jurídica sobre estas cuestiones. Hemos de advertir, no obstante –aunque no es nuestra intención entrar en ello-, que algunos textos que se refieren expresamente a los archivos desprenden cierto desconocimiento acerca de sus funciones, su funcionamiento y la situación actual de los mismos, así como un mal uso de la terminología archivística. Fruto, quizás, del generalizado olvido social de los archivos al que no es ajeno el mundo del Derecho.

Un ejemplo de este hecho nos lo ofrecen Fernández y Valero (2005, p. 309), quienes señalaron hace unos años “que hoy día la mayor parte de los datos que obran en los archivos y registros públicos se encuentran digitalizados”. Circunstancia que, a nuestro pesar, dista mucho de ser realidad.

sistemático de las implicaciones que puede tener esta circunstancia. Éste será el propósito principal de nuestro trabajo: estudiar el impacto del derecho a la protección de datos en los archivos públicos e intuir, si fuera posible, futuras vías de investigación y análisis en profundidad de la cuestión. De acuerdo con ello, los objetivos específicos que pretendemos alcanzar con este trabajo son, fundamentalmente:

- Encontrar posibles zonas de fricción, así como áreas de confluencia, entre las prescripciones de la legislación de protección de datos de carácter personal, y el funcionamiento de los archivos públicos y la normativa que lo regula.
- Proponer, en la medida de lo posible, soluciones a alguno de los problemas que pudieran detectarse en dicha relación.
- Por último, y como ya se ha avanzado, vislumbrar futuras líneas de investigación en esta materia que permitan desarrollar en trabajos posteriores, un modelo de análisis, adaptación y aplicación de la normativa de protección de datos en este ámbito.

Para realizarlo, hemos acotado nuestro ámbito de análisis al sistema archivístico de la Administración General del Estado (en adelante, AGE)¹⁰, conscientes de que su estudio nos permitirá ofrecer una imagen extrapolable en buena medida a otras Administraciones. Contamos, sin amargo, con un *handicap* importante: los archivos siguen siendo los grandes desconocidos de nuestras administraciones. Cuáles son, para qué sirven y cómo llevan a cabo sus funciones, siguen siendo cuestiones desconocidas para los ciudadanos, pero también para los responsables políticos de la Administración Pública. Por este motivo –y aún a riesgo de dedicar bastantes páginas de nuestro trabajo en el intento- hemos decidido incluir un Capítulo 0 con el pretendemos caracterizar a los archivos como servicio necesario para el buen funcionamiento de las organizaciones; y poner en contexto a aquellos que constituyen el ámbito

¹⁰ La especial referencia que haremos a los archivos gestionados por el Ministerio de Cultura –que en ningún caso se trata de un estudio de caso- responde a nuestro mejor conocimiento de esta organización, para la que trabajamos, en el Archivo General de la Administración.

de análisis de nuestro trabajo –los archivos de la Administración General del Estado–, en torno al concepto de sistema archivístico.

La estructura que da forma, finalmente, al trabajo es fruto principalmente de la metodología empleada para llevarlo a cabo. Ésta constó básicamente de tres fases:

- En un primer momento, analizamos de forma detallada la legislación vigente en materia de protección de datos¹¹. Para orientar, organizar e interpretar los resultados de este análisis, nos apoyamos en el estudio de una reducida selección de bibliografía jurídica: buscamos aquella que, a nuestro criterio, abordaba de forma más próxima a nuestros objetivos y ámbito de estudio dicha legislación¹².
- El siguiente paso consistió en examinar el marco definido como ámbito de estudio, estudiando, por un lado, la legislación reguladora del funcionamiento del sistema archivístico de la Administración General del Estado; y, por otro, la práctica profesional en los centros que lo integran, recurriendo para ello a la bibliografía, documentos y normas técnicas archivísticas.
- Por último, tratamos de relacionar los resultados de uno y otro análisis, para lo que resultó imprescindible recurrir a la doctrina de las autoridades de control, especialmente de la Agencia Española de Protección de Datos (en adelante, AEPD)¹³, buscando y seleccionando aquellos documentos que se ocuparan de forma más o menos directa de las cuestiones que pudieran afectar a los archivos.

De acuerdo con este esquema, y una vez delimitado nuestro ámbito de estudio, el trabajo se desarrolla en torno a dos grandes bloques: en el primero (capítulos 1 y 2), se examinará el derecho a la protección de datos y su régimen jurídico en España; mientras que en el segundo

¹¹ Hemos obviado, dado nuestro ámbito específico de estudio, las disposiciones relativas a ficheros de titularidad privada. Tampoco analizamos lo referente a las transferencias internacionales de datos, quizás de interés a tenor de los diferentes proyectos de sistemas globales de información archivística existentes.

¹² Véase la bibliografía en el capítulo de fuentes.

¹³ Véase el apartado correspondiente en el capítulo de Fuentes.

(capítulos 3 a 5) se abordará más detalladamente la aplicación de este régimen en los archivos de la Administración General del Estado.

Así, en el Capítulo 1 resumimos las principales etapas que condujeron al reconocimiento de este derecho en nuestro país e influyeron decisivamente en la configuración del régimen legal que se ha articulado al efecto. Comenzamos, para ello, indagando sus orígenes: el momento en que se hace patente la necesidad de regular el tratamiento de datos de carácter personal frente a la creciente "amenaza informática". Proseguimos con su desarrollo en Europa, de la mano del Consejo de Europa y de la Unión Europea, como derecho fundamental autónomo, a través de un modelo normativo que influyó de forma decisiva en su plasmación en nuestro país, que brevemente repasamos para concluir el capítulo.

El Capítulo 2, por su parte, estudia la regulación vigente en España de este derecho: la Ley Orgánica de protección de datos de carácter personal (LOPD)¹⁴ y su Reglamento de desarrollo¹⁵. A partir del estudio de sus coordenadas básicas (el objeto y el contenido del derecho) desgranaremos las principales disposiciones de la normativa de protección de datos vigente en nuestro país y las garantías institucionales que contempla para hacer efectivo este derecho. Aunque su análisis específico se realizará en capítulos posteriores, procuraremos no perder de vista el ámbito de análisis que hemos definido al comienzo del trabajo: los archivos de la Administración General del Estado. Para ello, delimitaremos el objeto de protección de esta normativa en los mismos y haremos una breve referencia a las disposiciones destinadas a los ficheros de titularidad pública en los que se inscribe dicho objeto.

En el segundo bloque del trabajo analizamos, como dijimos, las implicaciones de este régimen en el funcionamiento de los archivos de la Administración General del Estado. En primer lugar, delimitamos la zona de impacto de la normativa de protección de datos en los mismos, tanto

¹⁴ Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (BOE nº 298, de 14 de diciembre). En el texto se citará como "LOPD".

¹⁵ Real Decreto 1720/2007, de 21 de diciembre, por el se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (BOE nº 17, de 19 de enero). En el texto se citará como "Reglamento".

en lo que se refiere a los ficheros presentes en su trabajo, como a los diferentes tratamientos que se realizan sobre ellos. Como hace la LOPD, trataremos de forma separada el grueso de los tratamientos, a los que dedicamos el Capítulo 3, de las cesiones o comunicaciones de datos, estudiadas en el Capítulo 4. Por último, el Capítulo 5 estudia la responsabilidad de los archiveros en la implementación de las medidas de seguridad exigidas en el Reglamento de la LOPD, como recomienda la normativa técnica archivística.

Las referencias normativas y jurisprudenciales recogidas en el texto se han desarrollado para facilitar su identificación y localización. Aunque se cita únicamente la publicación original de las normas, hemos empleado versiones consolidadas de las mismas, obtenidas de distintas bases de datos jurídicas (principalmente las de Westlaw y el BOE).

Por su parte, el estilo empleado para las referencias bibliográficas se basa en la norma ISO/FDIS 690, al igual que las citas, en su versión autor-fecha (estilo Harvard).

Agradecimientos

Este trabajo de investigación ha sido posible gracias, en primer lugar, a la infinita paciencia y los sabios consejos de su director, el profesor Luis Hernández Olivera. Agradecemos también la colaboración del Subdirector General de los Archivos Estatales, Severiano Hernández Vicente, que nos facilitó interesante documentación para realizar este estudio y que ha sido incorporada como anexos. Del mismo modo hemos de mencionar al Centro de Información Documental de Archivos (CIDA), dependiente de dicha Subdirección General, especialmente a nuestro compañero Javier Fernández Fernández, que nos prestó inestimable ayuda en la búsqueda de bibliografía y recursos. Y, por último, a mis compañeros de promoción en los Cuerpos Facultativo y de Ayudantes de archivos del Estado y al Departamento de Referencias del Archivo General de la Administración, especialmente a Daniel Gozalbo, Ricard Pérez y Juan José Villar, de cuyo trabajo aprendo cada día.

0. ÁMBITO DE ANÁLISIS: LOS ARCHIVOS DE LA ADMINISTRACIÓN GENERAL DEL ESTADO

0.1. Los archivos como servicio o institución. Los archivos públicos

El término "archivo", entendido como servicio o institución, sirve para designar distintas realidades, fruto de una larga trayectoria histórica que se remonta al origen mismo de la escritura¹⁶. Tres elementos fundamentales, sin embargo, permiten caracterizar un modelo general:

- En primer lugar, su objeto: los documentos (documentos de archivo¹⁷), que podríamos definir como la "información registrada producida o recibida durante la iniciación, desarrollo o terminación de una actividad personal o institucional y que incluye contenido¹⁸, contexto¹⁹ y

¹⁶ Especialmente polisémico, este término se emplea para designar distintas realidades –con mayor o menor arraigo social– en función del contexto de su uso. Incluso desde el punto de vista estrictamente archivístico, doctrina y legislación lo suelen emplear en tres sentidos: en primer lugar, para designar a la institución o servicio responsable de los documentos de una organización (sentido que emplearemos en nuestro trabajo); en segundo lugar, para denominar al conjunto de documentos que tiene a su dicho servicio o institución; y, por último, para referirse al local o edificio que alberga los anteriores. Puede verse un análisis de distintas definiciones y una propuesta integradora para el término "archivo", en la monografía que Antonia Heredia dedicó a este concepto (2007). Por otro lado, resulta destacable también el acercamiento al concepto de archivo que se está realizando en los últimos tiempos desde otras disciplinas, en lo que se ha venido a llamar "giro archivístico" (*archival turn*). Véase a este respecto el artículo de Alexandrina Buchanan [2001. Strangely unfamiliar: ideas of the archive from outside the discipline. En: Hill, J. (ed.). *The future of archives and recordkeeping: a reading*. Londres: Facet Publishing, pp. 36-62].

¹⁷ La Archivística hispanoparlante emplea la expresión "documentos de archivo" para diferenciar éstos de otros tipos de documentos, objeto de otras disciplinas. En nuestro trabajo emplearemos indistintamente los términos "documentos" y "documentos de archivo".

¹⁸ Sustancia intelectual de un documento. En los documentos tradicionales, el contenido está indisolublemente ligado al soporte (elemento estructural), hasta el punto de que la destrucción del soporte supondría la desaparición del propio documento. En los documentos electrónicos –al igual que los documentos analógicos registrados en nuevos soportes (por oposición a los tradicionales, generalmente en papel, y a los "novísimos", referidos a los electrónicos)–, el contenido no es autoevidente, sino que requiere unas herramientas de hardware y software para su visualización. Por otro lado, es posible la separación entre contenido y soporte: el contenido de un documento electrónico puede residir en diferentes partes de un mismo soporte e, incluso, en diferentes soportes (documentos distribuidos).

estructura²⁰ suficientes para servir como testimonio de esa actividad” (ICA 1997, p. 22). Esta definición hace hincapié en el origen funcional de los documentos de archivo: así, algunos autores (Yeo 2008, p. 337) los han definido como representaciones permanentes de actividades, creadas por participantes u observadores de las mismas o por sus representantes autorizados. Pero también, en su carácter testimonial, como evidencia o prueba de dichas actividades para poder servir de apoyo a las funciones de la organización y permitir, en su caso, la rendición de cuentas o la exigencia de responsabilidades a una organización o una persona (ICA 2005, p.20). Se trata de una definición, por tanto, ligada al objetivo que podríamos denominar “primario” de los documentos de archivo y vinculada a su dimensión

¹⁹ Circunstancias organizacionales, funcionales y operativas que rodean a la creación, recepción, almacenamiento o uso de los documentos, y su relación con otros materiales. La información contextual puede formar parte del propio documento, de sus elementos internos (por ejemplo, el membrete en un documento textual) o residir en elementos externos (por ejemplo, en la carpetilla de un expediente, en los instrumentos de control y en los instrumentos de descripción). El glosario InterPARES (INTERNational Research on Permanent Authentic Records in Electronic Systems) distingue:

- Contexto jurídico-administrativo: sistema legal y organizativo.
- Contexto de procedencia: entorno administrativo y funcional.
- Contexto procedimental: procedimiento en el curso del cual se crea el documento.
- Contexto documental: el fondo y su estructura interna.
- Contexto tecnológico: componentes técnicos del sistema o sistemas informáticos en que se crean, procesan, difunden y conservan los documentos.

Véase: InterPARES. 2001. *The InterPARES Glossary* [en línea]. Vancouver (Canadá): InterPARES. [Consulta: 10 de junio de 2011]. Disponible en: http://www.interpares.org/book/interpares_book_q_gloss.pdf

²⁰ Manera en que los elementos (de contenido y de contexto) de un documento se organizan, se interrelacionan y se presentan. Siguiendo el *Glosario de terminología archivística y documental* de la SAA (PEARCE-MOSES 2005), podemos diferenciar entre:

- Estructura interna, relacionada con la forma en que se registra el documento e incluye: la organización y disposición física de las partes que componen el contenido del documento (así como la información contextual presente en el propio documento); la utilización de signos; el soporte y el formato; etc.
- Estructura externa, que sitúa un documento de archivo en el contexto de un orden, una serie, un fondo, etc. En los documentos tradicionales se materializa en su ordenación física e instalación.

Para los documentos electrónicos, la *Guía para gestionar documentos electrónicos desde una perspectiva archivística* del Consejo Internacional de Archivos (ICA 1997) -y, con ella, el *Manual para archiveros* (ICA 2005)- distingue:

- Estructura física: no es evidente para el usuario e inmutable a priori como en los documentos tradicionales, sino que es variable y depende del hardware y el software. La estructura física está basada en una serie de componentes digitales registrados en un medio o soporte de almacenamiento: un componente digital es un objeto o cadena de bits diferenciada (fichero o file en terminología informática) que puede constituir un documento electrónico (la cadena de bits representa la información contenida en el documento); formar parte de un documento electrónico, junto con otros componentes; contener una o más partes de uno o varios documentos electrónicos.
- Estructura lógica: es propiamente la relación entre las partes que componen el documento, e incluye básicamente: el formato de fichero de cada componente digital, esto es, la codificación utilizada para que el software correspondiente traduzca esa cadena de bits en forma legible o interpretable para el ser humano; y la relación entre el contenido de los distintos componentes digitales o ficheros del documento (si es que está compuesto de varios)

jurídica y administrativa o de gestión²¹, con independencia del interés cultural que pueden tener desde el momento mismo de su creación.

- Un segundo elemento que permite caracterizar a los archivos es su función: la gestión de los documentos que acabamos de identificar. Una gestión que debería abarcar todo el ciclo de vida²² de los documentos, incluyendo tanto la función de la gestión de documentos (*records management*) como la archivística. La gestión de documentos de archivo es el "área de gestión responsable del control eficaz y sistemático de la creación, la recepción, el mantenimiento, el uso y la disposición de documentos, incluidos los procesos para incorporar y mantener, en forma de documentos, la información y prueba de las actividades y operaciones de la organización"²³. Así se define en la norma ISO 15.489-1:2001 sobre gestión de documentos (3.15), completada con el informe técnico ISO/TR 15.489-2:2001 -guía de implementación de la anterior para su uso por parte de los profesionales de la gestión de documentos y de aquellas personas

²¹ Otras definiciones, sin embargo, enfatizan otras dimensiones de los documentos de archivo, dependiendo del punto de vista desde el que se realiza. Así, se realza su carácter informativo cuando se realiza desde la óptica de las Ciencias de la Información –destacando sus elementos comunes con otras clases de documentos-. O se relaciona con el concepto de memoria, cuando se aborda desde la óptica de la Historia y las identidades culturales (Yeo 2008). En cualquier caso, hemos de recordar, siguiendo a Heredia (2011) que para los documentos de archivo "no cabe la exclusiva dimensión de histórica, de cultural, de memoria" (p. 76), ya que es su dimensión administrativa, de gestión, la que los imprime carácter, "porque los documentos de archivo no son tales porque estén en un Archivo, ni porque sean muy antiguos, sino porque han nacido como algo obligado y son testimonio y prueba de transacciones y relaciones necesarias y establecidas por la sociedad y los seres humanos" (p. 73).

²² Periodo comprendido entre la producción de un documento –incluido su diseño- y su eliminación o, en su caso, conservación permanente (Cruz 2011, p. 109).

²³ Este control debe asegurar que los documentos se crean y mantienen a lo largo del tiempo con las siguientes características: autenticidad, fiabilidad, integridad y disponibilidad.

Según la ISO 15.489-1:2001 (7.2.2), un documento auténtico es aquél del que se puede probar que es lo que afirma ser; que ha sido creado o enviado por la persona de la cual se afirma que lo ha creado o enviado; y que ha sido creado en el momento en que se afirma. Por su parte, la Guía del ICA (1997) entiende la autenticidad como la persistencia a lo largo del tiempo de las características del documento respecto al contenido, contexto y estructura. Uniendo ambas ideas, se puede decir que la autenticidad –como han señalado los hallazgos del Proyecto InterPARES 1– se basa en la identidad del documento y en su integridad.

Un documento fiable es aquél cuyo contenido puede ser considerado una representación completa y precisa de las operaciones, las actividades o los hechos de los que da testimonio (ISO 15.489-1:2001, 7.2.3). Es decir, es la capacidad de un documento para servir de prueba fidedigna (ICA 1997), aspecto que hace referencia a la autoridad y veracidad de los documentos como prueba.

La integridad es el mantenimiento del carácter completo e inalterado de los documentos.

Por último, la disponibilidad es la capacidad de localizar, recuperar, presentar e interpretar un documento.

encargadas de gestionar documentos en sus respectivas organizaciones-. La función archivística, por su parte, "es aquel grupo de actividades interrelacionadas que contribuyen a (y son necesarias para) lograr los objetivos de salvaguardia y conservación de los documentos de valor permanente, y garantizar que sean accesibles e inteligibles" (ICA 2005, p.19). Dentro de este marco general, las distintas funciones específicas que puede llevar a cabo cada archivo dependen de la especificidad de la organización en la que está integrado (titularidad, tamaño, funciones, estructura) y su marco normativo y reglamentario, así como de la sistematización del servicio de archivo en la misma, que puede suponer la división del servicio en distintas unidades en función del ciclo vital de los documentos²⁴ u otros criterios que dependen también de dicha especificidad y de los propios documentos²⁵.

- La gestión de documentos y la función archivística pueden existir con independencia de los archivos como institución²⁶. Por ello, necesitamos un tercer elemento para identificar a los archivos: su servicio por parte

²⁴ Así, se suele hablar de archivos centrales, archivos intermedios y archivos históricos.

²⁵ De esta forma se fueron articulando a lo largo de la historia distintos archivos históricos "nacionales" en nuestro país: Archivo de la Corona de Aragón, Archivo General de Simancas, Archivo General de Indias, Archivo Histórico Nacional, Sección Nobleza del Archivo Histórico Nacional, Centro Documental de la Memoria Histórica...

²⁶ Es frecuente que no sólo los archivos se ocupen de estas funciones: por un lado, la gestión de documentos implica también a directivos, administradores de sistemas y empleados en general de una organización; por otro, otros servicios o instituciones (generalmente bibliotecas y museos) pueden custodiar y administrar documentos de archivo de valor permanente. A pesar de ello, coincidimos con los cuatro principios establecidos en la *Guía para gestionar documentos electrónicos desde una perspectiva archivística* del Consejo Internacional de Archivos (ICA 1997) que remarcan el papel principal que deberían desempeñar los archivos en este contexto (cit en ICA 2005, p. 15):

- *Los archivos deberían facilitar el establecimiento de políticas, procedimientos, sistemas, normas y prácticas diseñadas para ayudar a los productores de documentos a crear y conservar documentos auténticos, fiables y susceptibles de conservación a largo plazo.*
- *Los archivos deberían participar en todo el ciclo de vida de los documentos (concepción, producción, conservación) para garantizar la incorporación al sistema de archivo, conservación y disponibilidad de los documentos de valor permanente.*
- *Los archivos deberían ser responsables de la valoración de los documentos para identificar aquellos que tengan valor permanente.*
- *Los archivos deberían articular los requisitos de conservación y accesibilidad para garantizar que los documentos de archivo sigan estando disponibles y sigan siendo accesibles e inteligibles a lo largo del tiempo.*

de un personal técnico especializado, los archiveros²⁷, a través de unos procesos, metodologías, requisitos y normas técnicas propias, definidas por la Archivística, que abarcan –de forma extremadamente sucinta–:

- El llamado “tratamiento archivístico de los documentos”²⁸: la identificación²⁹, descripción³⁰ y valoración³¹ de los mismos.
- Los procesos técnicos que permiten controlar el ingreso³², el almacenamiento³³ y la manipulación³⁴ y la conservación³⁵ a largo plazo o eliminación³⁶ de los documentos.
- El servicio de los documentos, incluyendo el control del acceso y las funciones de referencia³⁷ y difusión³⁸ de los documentos.

²⁷ Como bien destaca Antonia Heredia (2011, p. 81), “[u]n Archivo no será tal, por muchos documentos valiosos que guarde, si no rinde servicio [...] y este servicio es difícil que se articule sin archiveros”.

²⁸ Conjunto de operaciones realizadas en cada una de las fases que componen el proceso de control intelectual y físico de los fondos a lo largo del ciclo vital de los documentos (DTA-SGAE).

²⁹ Fase del tratamiento archivístico que consiste en la investigación y sistematización de las categorías administrativas y archivísticas en que se sustenta la estructura de un fondo. El resultado de la misma permite la organización (clasificación y ordenación) de dicho fondo (DTA-SGAE).

³⁰ Fase del tratamiento archivístico que consiste en la elaboración de representaciones de documentos de archivo y, en su caso, de otras entidades archivísticas (agentes, funciones, etc) (Comisión de Normas Españolas de Descripción Archivística. 2008. *Modelo conceptual de descripción archivística y requisitos de datos básicos de las descripciones de documentos de archivo, agentes y funciones. Parte 1: Tipos de entidad*. Madrid: Ministerio de Cultura, p.22). Se realiza mediante la recopilación, análisis, organización y registro de la información que sirve para identificar, gestionar, localizar y explicar los documentos de archivo, así como su contexto y el sistema que los ha producido (ICA. 2000. *ISAD(G): Norma Internacional General de Descripción Archivística*. 2ª ed. Madrid: Ministerio de Educación, Cultura y Deporte, p. 16).

³¹ Fase del tratamiento archivístico que consiste en analizar y determinar los valores primarios y secundarios de las series documentales, fijando los plazos de transferencia, acceso, y conservación o eliminación total o parcial (DTA-SGAE).

³² Entrada de documentos en un archivo para su custodia, control y conservación, por la vía regular de transferencia o la extraordinaria de adquisición, por compra, por pago de impuestos, donación, depósito, etc. (DTA-SGAE)

³³ Incluyendo el acondicionamiento e instalación de los soportes analógicos como los procesos relacionados con el almacenamiento digital.

³⁴ Incluyendo los movimientos de entrada y salida. Cruz Mundet (2011, p. 239) define “manipulación” (2) como el “procedimiento establecido para el adecuado uso y traslado de los documentos, que incluye instrucciones escritas, contenedores adecuados y reproducción digital o por otros medios para preservar su integridad”. Véase ISO 15.489-1:2001, 9.6.

³⁵ Procesos y operaciones realizados para garantizar la permanencia intelectual y técnica de documentos auténticos a lo largo del tiempo (ISO 15.489-1:2001, 3.14).

³⁶ Procedimiento archivístico que consiste en la identificación de los documentos que se van a destruir conforme a los plazos establecidos en la fase de valoración (DTA-SGAE). Incluimos en este procedimiento la propia destrucción de los documentos por cualquier método que garantice la imposibilidad de reconstrucción de los mismos.

³⁷ Función archivística cuya finalidad es informar a los usuarios sobre la naturaleza de los documentos conservados en cada archivo sobre el o los temas elegidos, las condiciones de

Bajo las coordinadas que acabamos de señalar, los archivos públicos³⁹ - respecto a los cuales hemos decidido orientar nuestro trabajo- ejercen un papel esencial al servicio de la sociedad en general. Permiten a las instituciones de las que nos hemos dotado todos los ciudadanos desarrollar sus funciones de forma segura, responsable y transparente, en términos de eficacia y economía; son un instrumento fundamental para permitir el ejercicio del derecho de acceso a la información pública y, con él, el control democrático de dichas instituciones, así como el ejercicio de otros derechos reconocidos constitucionalmente. Finalmente, pretenden salvaguardar una importante parte de nuestra memoria colectiva y del patrimonio cultural. Como ha destacado Luis Martínez (1999, p. 91):

difícilmente podríamos encontrar unas instituciones que afecten de manera tan directa a un número tan considerable de derechos constitucionales. La gestión de los archivos atañe a la eficacia de las Administraciones Públicas, al derecho de los ciudadanos a acceder a la información que les interesa, al acceso de todos los españoles a la cultura y a la identidad de nacionalidades y regiones.

Aparte de esto, los archivos públicos cuentan con unas características propias que podemos resumir en torno a los tres elementos con los que caracterizábamos al conjunto de los archivos:

- En primer lugar, los documentos que gestionan se encuentran sujetos a un régimen jurídico especial, en tanto que forman parte, desde el momento de su creación, del patrimonio documental, bien del Estado, bien de las distintas Comunidades Autónomas. En el caso de los archivos de la Administración General del Estado⁴⁰ -a los que especialmente nos referiremos en este estudio-, dicho régimen se

accesibilidad, los instrumentos de consulta que permitan identificarlos y los medios de obtener reproducciones (DTA-SGAE).

³⁸ Función archivística cuya finalidad es por una parte, promover y generalizar la utilización de los fondos documentales de los archivos, y por otra, hacer partícipe a la sociedad del papel que desempeñan los archivos en ella (DTA-SGAE).

³⁹ Aquellos integrados en el sector público y cuyos documentos provienen y emanan del ejercicio de las competencias propias de los distintos Poderes del Estado; sin perjuicio de que archivos públicos puedan gestionar fondos y colecciones de origen privado.

⁴⁰ Forman parte del Patrimonio Documental los documentos de cualquier época generados, conservados o reunidos en el ejercicio de su función por cualquier organismo o entidad de carácter público, por las personas jurídicas en cuyo capital participe mayoritariamente el Estado u otras entidades públicas y por las personas privadas, físicas o jurídicas, gestoras de servicios públicos en lo relacionado con la gestión de dichos servicios (art. 49.2 LPHE).

encuentra recogido en el Título VII de la Ley 16/1985, de 25 junio, del Patrimonio Histórico Español (BOE nº 155, de 29 de junio) –en adelante, LPHE-.

- Buena parte de sus funciones se encuentran también reguladas en textos normativos (leyes, reglamentos), y suelen ejercerse en el marco de sistemas (sistemas de archivos) definidos de forma más o menos precisa y extensa en dichos textos. En el apartado siguiente desarrollaremos el concepto de sistema de archivos para contextualizar nuestro ámbito de estudio: el sistema archivístico de la Administración General del Estado.

- Por último, estos archivos son servidos generalmente a través de cuerpos específicos de funcionarios. En el caso que nos ocupará, suelen formar parte de las secciones de archivos de los Cuerpos Facultativo de Archiveros, Bibliotecarios y Arqueólogos, y de Ayudantes de Archivos, Bibliotecas y Museos y, en menor número, de la Escala de Auxiliares de Archivos, Bibliotecas y Museos.

0.2. Los sistemas de archivos

El concepto de sistema de archivos⁴¹ comenzó a desarrollarse en la década de 1960 en el sentido de "Sistemas Nacionales de Archivos", concebidos como "conjunto de todos los archivos de un país, reunidos en virtud de una ley bajo una unidad de régimen, [entendiendo que ésta] era la mejor forma de organizarlos, para la mayor eficacia y eficiencia de sus funciones y servicios"⁴². En estos entes, configurados bajo un régimen jurídico común a través de una legislación específica que actúa como verdadero motor del sistema, habrían de integrarse, en primer lugar, la totalidad de los archivos públicos del país, estableciéndose mecanismos para incorporar al mismo a los archivos privados. Por encima de todos ellos, la institución archivística central (denominada generalmente Archivo Nacional) debería ejercer como órgano rector o coordinador del sistema, asumiendo "un destacado papel como órganos de autoridad y de coordinación a lo largo de todo el ciclo documental, en sus fases administrativa e histórica" (Llansó 2006a, p. 63).

En este sentido, la LPHE previó en su artículo 66 el desarrollo de un Sistema Español de Archivos integrado por los archivos y los servicios de carácter técnico o docente directamente relacionados con los mismos, que se incorporen en virtud de lo que se disponga reglamentariamente. Por su parte, el art. 6.h del Real Decreto 1132/2008, de 4 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Cultura (BOE nº

⁴¹ Como ha señalado J. Llansó –a quien seguimos principalmente en este apartado- el de "sistema de archivos" o "sistema archivístico" es un "término discutido en el ámbito doctrinal iberoamericano –singularmente en España-" (2006a, p. 55). Ámbito que, por otra parte, es el único en el que se ha desarrollado este concepto (p. 57).

⁴² A esta conclusión se llegó en el marco del Seminario Multinacional sobre Planificación y Reorganización de Archivos Nacionales, organizado por la Organización de Estados Americanos (OEA) en 1973 en Lima (Perú), destacado por Llansó (2006a, p. 62) como uno de los hitos en la construcción de este concepto.

165, de 9 de julio) confiere a este departamento, a través de la Dirección General del Libro, Archivos y Bibliotecas (concretamente, a la Subdirección General de los Archivos Estatales) la función de coordinación del Sistema Español de Archivos. Sin embargo, al no existir una Ley estatal de archivos ni el Reglamento que habría que desarrollar la mencionada previsión de la LPHE, que sirva de marco general y motor de desarrollo de este Sistema Español de Archivos, podría afirmarse que dicho sistema aún no existe o no se ha configurado⁴³. Sí lo han hecho, sin embargo, los Sistemas Nacionales o Regionales constituidos –aunque en algunos casos sólo sobre el papel– en las distintas Comunidades Autónomas en virtud de sus respectivas competencias⁴⁴.

En cualquier caso, el concepto de sistema archivístico ha evolucionado de esta idea de Sistema Nacional a la más moderna de sistema institucional, aproximación “más modesta y a la vez más próxima a las realidades del panorama archivístico” (Llansó 2006a, p. 58), en contraposición con aquellos “metasistemas”. Definido por Eduardo Núñez como el “sistema propio de una institución, organización o administración para llevar a cabo la planificación, organización y gestión de sus fondos” (cit. en Llansó 2006a, p. 59), estaría conformado por los siguientes componentes:

⁴³ Uno de los pocos elementos “aglutinadores” previsto en la legislación vigente es el Consejo del Patrimonio Histórico –regulado en los arts. 2 a 6 del Real Decreto 111/1986, de 10 de enero, de desarrollo parcial de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español (BOE de 28 de enero)–, si bien limitado a la comunicación y el intercambio de programas de actuación e información relativos al Patrimonio Histórico Español entre las Administraciones del Estado y de las Comunidades Autónomas y que, además, ha resultado hasta el momento –que sepamos– inoperante en el ámbito archivístico. Más activa está resultando la Comisión de Normas Españolas de Descripción Archivística (CNEDA) –creada por la Orden CUL/1524/2007, de 25 de mayo (BOE nº 131, de 1 de junio) en virtud de la mencionada función de coordinación del Sistema Español de Archivos–, aunque limitada a un ámbito muy específico: la elaboración de unas normas archivísticas que, por otro lado, no podrán imponerse por parte del Estado más que a sus propios archivos.

Otro elemento aglutinador, aunque de carácter instrumental, es el Censo de los bienes integrantes del Patrimonio Documental que el art. 51 de la LPHE dispone que habrá de confeccionar “la Administración del Estado, en colaboración con las demás Administraciones competentes”. Este instrumento, que ha evolucionado hacia el actual Censo-Guía de los Archivos de España e Iberoamérica, se realiza bajo la coordinación del Ministerio de Cultura (a través del Centro de Información Documental de Archivos, integrado en la Subdirección General de los Archivos Estatales), con desigual colaboración por parte de las distintas Comunidades Autónomas.

⁴⁴ Fernández Ramos (2002, pp- 47 y 48) llega a cuestionarse la viabilidad constitucional de un Sistema Nacional de Archivos a tenor de la distribución competencial en esta materia, y concluye que “la conexión entre el sistema estatal de archivos y los sistemas autonómicos [...] no puede definirse unilateralmente por el Estado, sino que ésta tendrá que acudir a las vías más delicadas de la cooperación interadministrativa”. En nuestra opinión, la configuración del sistema podría venir a partir de la integración voluntaria de otros sistemas a través de convenio.

- Un marco normativo (normas legales y reglamentarias), que defina el sistema y determine su funcionamiento y las responsabilidades de los diferentes actores dentro del mismo.
- La administración de archivos o institución archivística, encabezada por una dirección política, encargada de la planificación, organización y gestión del sistema; e integrada por los distintos archivos que componen las fases o estadios del sistema: "archivos de gestión o de oficina"⁴⁵, archivos centrales⁴⁶ y, al menos, un archivo intermedio⁴⁷ y otro histórico⁴⁸. Así mismo, puede contar con servicios técnicos que atiendan necesidades específicas del conjunto de archivos del sistema; y con órganos de asesoramiento integrados por representantes de los distintos centros y de los propios productores de los documentos.
- Sus recursos (personal, infraestructuras, recursos tecnológicos), que dependerán del posicionamiento institucional de la institución archivística.
- Por último, Llansó –siguiendo a Carol Couture y Jean-Yves Rousseau– introduce un elemento que considera fundamental: el programa⁴⁹, compuesto básicamente por un conjunto de normas que regulen la creación y el tratamiento de documentos a lo largo de todo su ciclo de vida y de los instrumentos necesarios para ponerlas en práctica.

⁴⁵ Se emplea este término para designar los documentos en trámite o sometidos a continua utilización y consulta administrativa por las mismas oficinas productoras. De acuerdo con lo señalado en el apartado anterior, no podríamos considerarlo propiamente como un archivo, si bien hay que señalar que, generalmente, estos "archivos de oficina" suelen ser responsabilidad de los archivos centrales.

⁴⁶ Aquellos que coordinan y controlan el funcionamiento de los distintos archivos de gestión y reúnen los documentos transferidos por los mismos, una vez finalizado su trámite y cuando su consulta no es constante (DTA-SGAE).

⁴⁷ Aquél al que se han de transferir los documentos de los archivos centrales cuando su consulta por los organismos productores es esporádica y en el que permanecen hasta su eliminación o transferencia al archivo histórico (DTA-SGAE).

⁴⁸ Aquél al que se ha de transferir desde el archivo intermedio la documentación que deba conservarse permanentemente, y que puede conservar también otros documentos históricos recibidos por donación, depósito, adquisición, etc. (DTA-SGAE).

⁴⁹ Para Llansó supone el nexo de unión entre sistema archivístico y modelo de gestión de documentos. "El sistema archivístico definido hasta ahora en Iberoamérica no ha incorporado el «programa» como un componente más del sistema [...] que caracteriza la gestión de documentos" (2006b, p. 65).

0.3. El sistema archivístico de la Administración General del Estado

¿Cómo se estructura archivísticamente la gestión de los documentos producidos por los distintos órganos de la AGE y sus organismos autónomos (actuales y extintos) en el ejercicio de sus funciones⁵⁰? Resulta difícil sistematizar los archivos que serán nuestro objeto de atención en un marco como el que acabamos de describir debido a varias peculiaridades:

- En primer lugar, como consecuencia de que “la legislación estatal relativa a los propios archivos estatales es aún, a pesar de los lustros transcurridos desde la LPHE, incompleta, asistemática y dispersa” (Fernández 2002, p. 157), el sistema archivístico de la Administración General del Estado no ha encontrado aún su definición y regulación normativa.
- Además –como veremos- no se adapta perfectamente al modelo de sistema archivístico institucional que hemos definido anteriormente, debido especialmente a los principios de descentralización y desconcentración que rigen la organización y el funcionamiento de la AGE⁵¹, de acuerdo con la Constitución (art. 103 CE). Más bien podríamos hablar –como veremos- de un “metasistema”.
- Pero a pesar de ser un “metasistema” –esto es, un sistema que engloba a otros sistemas-, no abarca al conjunto de la Administración

⁵⁰ Los archivos de la AGE gestionan también fondos, colecciones y documentos de personas e instituciones privadas –especialmente los archivos históricos gestionados por el Ministerio de Cultura-, que han ingresado en los mismos mediante distintas fórmulas (donación, depósito, compra...), generalmente para su explotación con fines culturales, cumpliendo con el mandato constitucional de enriquecer el patrimonio histórico, cultural y artístico de los pueblos de España (art. 46 CE).

⁵¹ Ley 6/1997, de 14 abril, de Organización y Funcionamiento de la Administración General del Estado (LOFAGE), art. 3.

General del Estado, sino únicamente la "Administración civil": al margen del mismo se encuentra el Sistema de Archivos de la Defensa (SAD) –incluido el propio Ministerio de Defensa- tradicionalmente independiente y que en los últimos años ha venido configurándose en torno a una completa normativa⁵².

A pesar de esta compleja situación de partida –para algunos, "un auténtico galimatías de unidades independientes y autónomas entre sí sin apenas ningún lazo en común" (Martínez 1999, p. 116)-, creemos que podría ser perfilado como sistema –al menos "en construcción", hasta la promulgación de una ley de archivos estatales- a partir de una serie de componentes. Así, distintas normas⁵³ permiten vislumbrar un extremadamente flexible (Fernández 2002, p. 157) régimen de transferencias⁵⁴ -a través del cual se pueden definir los distintos tipos o fases de archivo- y un procedimiento único para la eliminación de

⁵² Real Decreto 2598/1998, de 4 de diciembre, por el que se aprueba el Reglamento de Archivos Militares (BOE nº 303, de 19 de diciembre); Real Decreto 1816/2009, de 27 de noviembre, por el que se aprueba el Reglamento de los Archivos Judiciales Militares (BOE nº 13, de 15 de enero); Orden PRE/447/2003, de 27 de febrero, por la que se determinan los órganos de dirección, planificación y ejecución del Sistema Archivístico de la Defensa, se modifica la dependencia y composición de la Junta de Archivos Militares y se establece la dependencia y composición de la Comisión Calificadora de Documentos de la Defensa (BOE nº 54, de 4 de marzo); Instrucción General 03/06, Sistema de Acción Cultural del Ejército de Tierra (organiza el Subsistema Archivístico del Ejército de Tierra); Instrucción 15/2010, de 30 de marzo, del Jefe de Estado Mayor de la Armada, por la que se establece la organización del Subsistema Archivístico de la Armada (BOD nº 73, de 16 de abril); Instrucción General 10-22, de 15 de septiembre de 2004, del Jefe de Estado Mayor del Ejército del Aire, sobre organización y funciones del Subsistema Archivístico del Ejército del Aire; Orden Ministerial 38/2002, de 19 de febrero, por la que el Subdirector General de Régimen Interior del Ministerio de Defensa asume las Funciones de Director del Subsistema Archivístico del Órgano Central (BOD nº 53, de 15 de marzo); Orden DEF/486/2011, de 9 de febrero, por la que se establecen los precios públicos para la reproducción de documentos custodiados en los archivos dependientes del Ministerio de Defensa (BOE nº 59, de 10 de marzo).

⁵³ La LPHE (art. 65); el Decreto 914/1969 de 8 de mayo, de creación del Archivo General de la Administración Civil (BOE nº 125, de 26 de mayo); el Real Decreto 1164/2002, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y la conservación de documentos administrativos en soporte distinto al original (BOE nº 274, de 15 de noviembre); y las distintas normas por las que se crean y regulan las Comisiones Calificadoras de Documentos Administrativos de los distintos Ministerios y organismos autónomos.

⁵⁴ Las transferencias son el procedimiento habitual de ingreso de fondos en un archivo mediante traslado de las fracciones de series documentales, una vez que éstas han cumplido el plazo de permanencia fijado por las normas establecidas en la valoración para cada una de las etapas del ciclo vital de los documentos (DTA-SGAE). La "flexibilidad" del régimen establecido por el Decreto 914/1969 se basa en las excepciones contempladas en las primeras fases; unas excepciones que se han convertido en norma y hacen que el circuito documental no sea sistemático sino, más bien, testimonial en algunos casos, provocando la saturación de oficinas y archivos centrales (y, lo que es peor, la posible destrucción incontrolada de documentos). En ello incide también el colapso del archivo que pone fin al sistema, el Archivo Histórico Nacional, incapaz de recibir más transferencias; y la tardanza en llevar a cabo procedimientos controlados de eliminación de documentos, lo que provocó aún más la acumulación de documentos en los archivos centrales.

documentos⁵⁵. A ello debemos unir la sujeción a un mismo régimen jurídico de sus documentos y del acceso a los mismos⁵⁶ y a “algunos fundamentos básicos de la actuación de los archivos” (Martínez 1999, p. 101) que establece la LPHE.

Dado que hablamos de un “metasistema”, no existe una única institución archivística. No obstante, el papel de dirección política le corresponde en cierta medida al Ministerio de Cultura a través de la Subdirección General de los Archivos Estatales (dependiente de la Dirección General del Libro, Archivos y Bibliotecas). Así, el Real Decreto 1132/2008, de 4 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Cultura (BOE nº 165, de 9 de julio) confiere a dicha unidad, en su art. 6, funciones de gestión de los archivos de titularidad y gestión estatal adscritos al Departamento, y de asesoramiento respecto de los archivos de titularidad estatal dependientes de otros Ministerios (art. 6.f); así como la creación, dotación y fomento de archivos de titularidad estatal (art. 6.g)⁵⁷.

Cómo órganos comunes de asesoramiento se encuentra, en primer lugar, la Junta Superior de Archivos, órgano consultivo de la Administración General del Estado en materia de patrimonio documental y archivos, previsto en el art. 10.b del Real Decreto 111/1986, de 10 de enero, de desarrollo parcial de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español (BOE nº 24, de 28 de enero)⁵⁸. No obstante, sus funciones han sido hasta el momento mínimas, sin apenas trascendencia para el funcionamiento del sistema. Mucha mayor importancia está teniendo la Comisión Superior Calificadora de Documentos Administrativos (CSCDA). Creada por la LPHE en su artículo 58, su composición, funcionamiento y competencias específicas fueron establecidas en el Real Decreto 139/2000, de 4 de febrero y, posteriormente, del Real Decreto 1401/2007, de 29 de octubre, que derogó al anterior. Adscrito al Ministerio

⁵⁵ Regulado en el ya señalado Real Decreto 1164/2002, de 8 de noviembre.

⁵⁶ Básicamente a través de los artículos 37 de la Ley 30/1992, de 26 de noviembre, de régimen jurídico de las Administraciones Públicas y del procedimiento administrativo común (LPAC); y 57 de la LPHE.

⁵⁷ A ello deberíamos sumar su papel, ya referido, de coordinador respecto del Sistema Español de Archivos (art. 6.h), inoperativo hasta que no se desarrolle normativamente.

⁵⁸ Su composición y funciones se encuentran reguladas en la Orden de 25 de noviembre de 1996 (BOE nº 289, de 30 de noviembre). La última vez que se nombraron vocales fue por Orden CUL/4292/2005, de 22 de diciembre (BOE nº 23, de 27 de enero de 2006).

de Cultura a través de la Dirección General del Libro, Archivos y Bibliotecas, este órgano colegiado tiene la misión de estudiar y dictaminar sobre la calificación y utilización de los documentos de la Administración del Estado y del sector público estatal, así como sobre su integración en los archivos y el régimen de acceso e inutilidad administrativa de los mismos, si bien sus funciones se encuentran en la actualidad limitadas al dictamen final en los procedimientos de eliminación de documentos y, en su caso, de conservación del contenido de los mismos en soporte distinto del original⁵⁹.

Como servicios técnicos de apoyo, la Subdirección General de los Archivos Estatales cuenta con el Centro de Información Documental de Archivos (CIDA)⁶⁰ y el Servicio de Reproducción de Documentos (SRD)⁶¹. Aunque creados inicialmente con el propósito de atender las necesidades del Sistema Archivístico Español, atienden principalmente a los centros de la AGE y, de forma especial, a los archivos dependientes del Ministerio de Cultura, desempeñando un papel bastante discreto en el sistema (Martínez 1999, p. 129).

Los archivos, "elemento básico, sobre el que gira cualquier sistema" (Martínez 1999, p. 130), se articulan -debido a este débil marco que brevemente hemos descrito- en lo que podríamos denominar varios subsistemas, correspondientes a la Administración central, a la Administración periférica y a la Administración institucional de la AGE⁶².

⁵⁹ Real Decreto 1164/2002, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y la conservación de documentos administrativos en soporte distinto al original (BOE nº 274, de 15 de noviembre).

⁶⁰ El CIDA funciona como centro de documentación especializado en información archivística (coordinando para ello el Censo Guía de Archivos de España e Iberoamérica, <http://censoarchivos.mcu.es>) y bibliográfica -principalmente sobre archivos y fuentes documentales- (para lo que cuenta con una importante biblioteca, amén de coordinar el Catálogo Colectivo de la Bibliotecas de los Archivos Estatales, <http://www.mcu.es/ccbae/>).

⁶¹ EL SRD (<http://www.mcu.es/archivos/MC/SRD/index.html>) se ocupa del asesoramiento y apoyo técnico a los archivos en materia de reproducción de documentos, y ejerce además funciones de archivo de seguridad, conservando para ello copias de conservación de documentos de distintos archivos españoles.

⁶² No haremos mención a los archivos de los órganos de la AGE en el exterior, que entendemos incardinado en el subsistema central a través del Ministerio de Asuntos Exteriores.

El subsistema de la Administración central estaría formado por la confluencia -dada la relativa independencia de cada uno de ellos- del flujo documental de los "sistemas" propios⁶³ de los órganos centrales de cada Ministerio (véase tabla resumen en páginas siguientes) en las últimas fases de archivo -intermedio e histórico-, concentradas en los centros dependientes de Cultura (Archivo General de la Administración, Archivo Histórico Nacional y resto de archivos históricos estatales⁶⁴).

Cada uno de dicho sistemas se articula en torno a un archivo central o general, generalmente adscrito a la Secretaría General Técnica de su departamento -que constituiría, por tanto, el órgano directivo de cada sistema-. Estos archivos centrales son -de acuerdo con el citado régimen de transferencias establecido en los artículos 2 y 3 del Decreto 914/1969⁶⁵- los encargados de recoger anualmente los documentos de las distintas unidades administrativas (archivos de oficina)⁶⁶ que integran los

⁶³ Estos sistemas propios o subsistemas departamentales se encuentran muy desigualmente desarrollados: en algunos casos asistimos a la configuración de verdaderos sistemas institucionales de archivos, prácticamente autónomos y con una completa normativa reguladora, como es el caso del Ministerio del Interior; de otros -como Sanidad, Política Social e Igualdad-, apenas tenemos información.

⁶⁴ Archivo de la Corona de Aragón, Archivo General de Simancas, Archivo General de Indias, Archivo de la Real Chancillería de Valladolid, Sección Nobleza del Archivo Histórico Nacional y Centro Documental de la Memoria Histórica.

⁶⁵ *Artículo 2. Anualmente, en las fechas y forma que se determine por el Subsecretario de cada Departamento, las dependencias de la Administración Pública Central e Institucional, remitirán al Archivo Central del Ministerio a que pertenezcan la totalidad de los expedientes en que se hayan dictado actos administrativos de resolución que afecten de algún modo a derechos o intereses del Estado o de los administrados, cuando dichos actos hayan devenido firmes y se hayan practicado por la Administración las actuaciones conducentes a la total ejecución de sus pronunciamientos. Cuando se trate de expedientes o documentos en que no proceda dictar actos administrativos de resolución del carácter expresado, así como informes, estudios, etc., pasarán al Archivo General cuando hayan producido en la dependencia que los ha elaborado o tramitado la totalidad de sus efectos. No obstante, cuando la índole de los documentos así lo aconseje podrán conservarse en la respectiva dependencia administrativa previa resolución del Subsecretario del Departamento correspondiente. El mismo régimen se seguirá con aquellas series documentales que por razón de su frecuente consulta convenga conservar en la dependencia que las produce o tramita.*

Artículo 3. La documentación de los Archivos Centrales de los Ministerios se trasladará al Archivo General de la Administración Civil al cumplirse los quince años de su ingreso en los mismos. Aquellas series documentales, sin embargo, que tengan poco uso y se consulten raramente podrán ser enviadas al Archivo General antes de cumplir el indicado plazo, a propuesta del Archivo del Ministerio, con aprobación del Subsecretario del Departamento. Por el Archivo General de la Administración Civil se formulará propuesta a la Dirección General de Archivos y Bibliotecas para remitir al Archivo Histórico Nacional aquella documentación que con más de veinticinco años de antigüedad carezca, a su juicio, de validez administrativa y tenga valor histórico. La Dirección General resolverá en cada caso, previa consulta a los Departamentos interesados.

⁶⁶ Algunos Ministerios cuentan, además, con otros archivos más o menos independientes del Central. Por ejemplo, en el ámbito del Ministerio de Economía y Hacienda, nos encontramos con los Archivos de las Direcciones Generales de Costes de Personal y Pensiones Públicas (antigua Dirección General de Clases Pasivas) y de la Dirección General del Tesoro y Política

órganos centrales de cada Ministerio; así como de transferir al Archivo General de la Administración (AGA) las fracciones de serie⁶⁷ correspondientes tras quince años de su ingreso en los mismos y desde el cual se habrán de transferir al correspondiente archivo histórico aquellos documentos sobre los que se ha determinado su conservación permanente. A pesar de ello, son pocos los archivos centrales que transfieren regularmente documentos al AGA y aquellos que si lo hacen, no lo realizan de forma sistemática.

Algunos de estos sistemas departamentales han desarrollado su propia normativa (Asuntos Exteriores, Justicia y, sobre todo, Interior) relativa a las transferencias –especialmente de las oficinas al archivo central- y al procedimiento de acceso a los documentos. Además, prácticamente todos cuentan con su propia Comisión Calificadora⁶⁸, que eleva sus propuestas sobre eliminación o conservación en soporte distinto al original⁶⁹ a la Superior. La intensa actividad desarrollada hasta el momento por alguna de estas Comisiones (por ejemplo, la del Ministerio de Economía y

Financiera; y, dentro del propio Ministerio de Cultura, con el Archivo General del Instituto del Patrimonio Cultural de España. Por otro lado, no está claro qué sucede con los archivos centrales de Ministerios extinguidos y su relación con los del departamento en el que se integran (por ejemplo, el Archivo Central de la Secretaría de Estado de Vivienda y Actuaciones Urbanas –antiguo Archivo Central del Ministerio de la Vivienda- con respecto al Archivo General del Ministerio de Fomento).

⁶⁷ Cada una de las divisiones cronológicas de una serie, que resultan del establecimiento de plazos concretos de transferencia y eliminación y que constituyen, por tanto, la base de las operaciones de transferencia y selección (DTA-SGAE).

⁶⁸ El artículo 58 LPHE previó la creación de Comisiones Calificadoras “en los Organismos públicos que así se determine”, lo que dio lugar a la creación de Comisiones Calificadoras ministeriales, hecho generalizado como consecuencia de la disposición transitoria única del Real Decreto 1164/2002: *1. En todos los Departamentos ministeriales y en el plazo de tres meses desde la entrada en vigor del presente Real Decreto se crearán, en su caso, mediante Orden, las Comisiones Calificadoras de Documentos Administrativos previstas en el artículo 58 de la Ley 16/1985, de 25 de junio, con la aprobación previa del Ministro de Administraciones Públicas en los términos previstos en el artículo 67.4 de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado. 2. Respecto de los Organismos públicos se podrá proceder a la creación, mediante Orden ministerial, de una Comisión distinta de la del Departamento al que estén vinculados cuando la gestión documental que tenga lugar en los mismos lo aconseje. En otro caso, si se hubiese constituido la Comisión en el Ministerio correspondiente, los Organismos públicos estarán representados en la misma. 3. La constitución y el funcionamiento de la Comisión serán atendidos con los actuales medios personales y materiales del Departamento u Organismo sin que la aprobación de esta norma suponga incremento de gasto público.* A pesar de ello, aún no se ha creado la Comisión Calificadora de Documentos Administrativos del Ministerio de Medio Ambiente y Medio Rural y Marino.

⁶⁹ Ya que, como hemos dicho, se trata del único procedimiento relativo a las funciones de estas comisiones que ha sido regulado. La ausencia de una norma que desarrolle las funciones que, al respecto del establecimiento de plazos de transferencia entre los distintos tipos de archivo tienen las Comisiones Calificadoras de Documentos Administrativos es una de las razones del deficiente régimen de transferencias del sistema archivístico de la AGE.

Hacienda) contrasta sin embargo con la de otras que ni siquiera han llegado aún a reunirse.

Por otro lado, algunos autores han criticado el abandono por parte de los archivos centrales del papel fundamental que debería corresponderles como canalizadores de una parte esencial de la información administrativa de los departamentos, tanto para la propia Administración como para los ciudadanos. Como señaló en su momento Luis Martínez (1999, p. 117):

Esta misión de informar se está confundiendo en algún Ministerio, o en casi todos, con la investigación histórica. El archivo central de los organismos públicos pierde su sentido cuando se dedica al servicio de la investigación o a la promoción y difusión cultural. Existen ejemplos sangrantes como el del Ministerio de Asuntos Exteriores, que todavía posee documentación del siglo XVI, pero podemos incluir casi todos, puesto que entre sus papeles mantienen auténticos nidos para la Historia.

El subsistema de los órganos centrales es, en definitiva, una amalgama compuesta por sistemas heterogéneos, más o menos independientes del sistema general, cuyas "funciones primordiales (la información administrativa, el control de los archivos de oficina, la valoración y las transferencias) son, salvo excepciones, meramente testimoniales" –como continuaba Martínez en la cita anterior–.

Subsistema	Archivo cabecera y adscripción orgánica del mismo		Normas internas
Asuntos Exteriores	Archivo General del Ministerio de Asuntos Exteriores	Secretaría General Técnica. Vicesecretaría General Técnica RD 1748/2010, de 23 de diciembre (BOE nº 12, de 14 de enero de 2011)	Acceso, régimen de transferencias y Comisión Calificadora ⁷⁰
Ciencia e Innovación	Archivo General del Ministerio de Ciencia e Innovación	sin datos	Comisión Calificadora ⁷¹

⁷⁰ Orden de 2 de abril de 1991 por la que se regula el acceso a los archivos del Ministerio de Asuntos Exteriores (BOE nº 87, de 11 de abril).

⁷¹ Orden CTE/2211/2003, de 23 de julio, por la que se crea la Comisión Calificadora de Documentos Administrativos del Ministerio de Ciencia y Tecnología (BOE nº 186, de 5 de agosto).

Subsistema	Archivo cabecera y adscripción orgánica del mismo		Normas internas
Cultura	Archivo Central del Ministerio de Cultura	Dir. Gral. del Libro, Archivos y Bibliotecas. Subdir. Gral. de los Archivos Estatales RD 1132/2008, de 4 de julio (BOE nº 165, de 9 de julio)	Comisión Calificadora ⁷²
Economía y Hacienda	Archivo General / Central del Ministerio de Economía y Hacienda	Secretaría General Técnica. Subdir. General de Información, Documentación y Publicaciones RD 1127/2008, de 4 de julio (BOE nº 165, de 9 de julio)	Comisión Calificadora ⁷³
Educación	Archivo Central del Ministerio de Educación	Subsecretaría. Oficialía Mayor RD 189/2011, de 18 de febrero (BOE nº 43, de 19 de febrero)	Comisión Calificadora ⁷⁴
Fomento	Archivo General / Central del Ministerio de Fomento	Subsecretaría. Inspección General de Fomento. Oficialía Mayor RD 30/2011, de 14 de enero (BOE nº 16, de 19 de enero)	Comisión Calificadora ⁷⁵
Industria, Turismo y Comercio	Archivo Central del Ministerio de Industria, Turismo y Comercio	Secretaría Gral. Técnica. Subdir. Gral. de Desarrollo Normativo, Informes y Publicaciones RD 1226/2010, de 1 de octubre (BOE nº 240, de 4 de octubre)	Comisión Calificadora ⁷⁶

⁷² Orden CUL/3021/2006, de 25 de septiembre, por la que se crea la Comisión Calificadora de Documentos Administrativos del Ministerio de Cultura y de sus organismos públicos (BOE nº 237, de 4 de octubre)

⁷³ Orden EHA/242/2005, de 8 de febrero, por la que se constituye la Comisión Calificadora de Documentos Administrativos del Ministerio de Economía y Hacienda (BOE nº 37, del 12 de febrero).

⁷⁴ Orden EDU/3274/2009, de 30 de noviembre, por la que se crea la Comisión Calificadora de Documentos Administrativos del Ministerio de Educación, y se regula su organización y funcionamiento (BOE nº 292, de 4 de diciembre).

⁷⁵ Orden FOM/542/2005, de 2 de marzo, por la que se crea la Comisión Calificadora de Documentos Administrativos del Ministerio de Fomento y de sus organismos públicos (BOE nº 59 del 10 de marzo); modificada por Orden FOM/921/2009, de 27 de marzo (BOE nº 92, de 15 de abril).

⁷⁶ Orden ITC/3863/2004, de 17 de noviembre, por la que se crea la Comisión Calificadora de Documentos Administrativos del Ministerio de Industria, Turismo y Comercio (BOE nº 285, de 26 de noviembre).

Subsistema	Archivo cabecera y adscripción orgánica del mismo	Normas internas	
Interior	Ministerio del Interior	Secretaría General Técnica. Subdirección General de Recursos RD 1181/2008, de 11 de julio (BOE nº 171, de 16 de julio)	Comisión Calificadora y acceso ⁷⁷ Organización y funcionamiento del Sistema ⁷⁸ Régimen de transferencias ⁷⁹ Eliminación de documentos ⁸⁰
Justicia	Archivo General del Ministerio de Justicia	Secretaría General Técnica. Subdirección General de Documentación y Publicaciones RD 1203/2010, de 24 de septiembre (BOE nº 233, de 25 de septiembre)	Comisión Calificadora ⁸¹ Acceso ⁸² Archivo de la Comisión General de Codificación ⁸³

⁷⁷ Orden de 21 de diciembre de 2000 por la que se crea la Comisión calificadora de documentos administrativos del Ministerio del Interior y se regula el acceso a los archivos de él dependientes (BOE nº 4, de 4 de enero); se completa, en materia de acceso, con la Instrucción de 12 de julio de 2006, de la SGT (Orden General del CNP nº 1609, de 9 de octubre; BOCGC nº 29, de 20 de octubre)

⁷⁸ Orden de 7 de marzo de 2001 por la que se crean, dependientes del Archivo General del Ministerio del Interior, las Secciones de las Direcciones Generales de la Policía y de la Guardia Civil (BOE nº 65, de 16 de marzo); Orden INT/2528/2002, de 2 de octubre, por la que se regula el Sistema Archivístico del Ministerio del Interior (BOE nº 246, de 14 de octubre); Orden General nº 3, de 9 de marzo de 2005, sobre organización de la Sección de la Dirección General de la Guardia Civil del Archivo General del Ministerio del Interior (BOCGC nº 8, de 21 de marzo); Circular de 27 de diciembre de 2005, por la que se dictan normas sobre organización y funciones de la Sección de la Dirección General de la Policía del Archivo General del Ministerio del Interior, incardinada en el Archivo Central de la Comisaría General de Extranjería y Documentación y de los demás archivos de la Dirección General de la Policía, en orden a su adaptación al Sistema Archivístico del Departamento (Orden General nº 1569, de 9 de enero; sección 3).

⁷⁹ Instrucción de 1 de julio de 2003, de la Secretaría General Técnica, por la que se dictan normas sobre transferencias de documentos de los archivos de gestión de servicios centrales y periféricos del Departamento a los archivos correspondientes.

⁸⁰ Instrucción de la Secretaría General Técnica, de 10 de julio de 2007, sobre eliminación de documentos en el Ministerio del Interior

⁸¹ Orden JUS/2935/2009, de 26 de octubre, por la que se crea la Comisión Calificadora de Documentos Administrativos del Ministerio de Justicia y de sus organismos públicos (BOE nº 265, de 3 de noviembre).

⁸² Orden JUS/2546/2004, de 26 de julio, por la que se regula el acceso al Archivo General del Ministerio de Justicia (BOE nº 183, de 30 de julio).

⁸³ Con carácter autónomo, se encuentra regulado en el cap. IV (arts. 29 a 35) del Estatuto de este órgano colegiado. Real Decreto 160/1997, de 7 de febrero, por el que se aprueban los Estatutos de la Comisión General de Codificación (BOE nº 50, de 27 de febrero).

Subsistema	Archivo cabecera y adscripción orgánica del mismo	Normas internas	
Medio Ambiente (Min. Medio Ambiente y Medio Rural y Marino)	Archivo General del Área de Medio Ambiente	Secretaría Gral. Técnica. Subdir. Gral. de Información al Ciudadano, Documentación y Publicaciones RD 1443/2010, de 5 de noviembre (BOE nº 269, de 6 de noviembre)	-
Medio Rural y Marino (Min. Medio Ambiente y Medio Rural y Marino)	Archivo Central del Área de Medio Rural y Marino	Secretaría Gral. Técnica. Subdir. Gral. de Información al Ciudadano, Documentación y Publicaciones RD 1443/2010, de 5 de noviembre (BOE nº 269, de 6 de noviembre)	-
Política Territorial y Admin. Pública	Archivo Central del Ministerio de Política Territorial y Administración Pública	Secretaría Gral. Técnica. Subdir. Gral. de Relac. Internacionales, Publicaciones y Archivo RD 393/2011, de 18 de marzo (BOE nº 69, de 22 de marzo)	Comisión Calificadora ⁸⁴
Presidencia	Archivo Central del Ministerio de la Presidencia	Secretaría General Técnica. Subdirección General de Publicaciones, Documentación y Archivo RD 392/2011, de 18 de marzo (BOE nº 69, de 22 de marzo)	Comisión Calificadora y acceso ⁸⁵
Sanidad, Política Social e Igualdad	Archivo Central del Ministerio de Sanidad, Política Social e Igualdad	Secretaría General Técnica. Subdirección General de Recursos y Publicaciones RD 263/2011, de 28 de febrero (BOE nº 51, de 1 de marzo)	Comisión Calificadora ⁸⁶

⁸⁴ Orden TER/650/2010, de 4 de marzo, por la que se crea la Comisión Calificadora de Documentos Administrativos del Ministerio de Política Territorial (BOE nº 66, de 17 de marzo).

⁸⁵ Orden de 24 de abril de 1997 por la que se regula el acceso al Archivo Central del Ministerio de la Presidencia (BOE nº 103, de 30 de abril)

⁸⁶ Orden SAS/3592/2009, de 22 de diciembre, por la que se crea la Comisión calificadora de documentos administrativos del Ministerio de Sanidad y Política Social (BOE nº 4, de 5 de enero de 2010).

Subsistema	Archivo cabecera y adscripción orgánica del mismo		Normas internas
Trabajo e Inmigración	Ministerio de Trabajo e Inmigración	Secretaría General Técnica. Subdirección General de Informes Socioeconómicos y Documentación RD 777/2011, de 3 de junio (BOE nº 133, de 4 de junio)	Comisión Calificadora ⁸⁷

Mucho menos perfilado se encuentra el subsistema de la Administración central periférica⁸⁸, más allá de la consideración de los archivos históricos provinciales (AHP) -existentes en la mayor parte de las capitales de provincia⁸⁹- como archivos intermedios e históricos del mismo, de conformidad con el artículo 5 del citado Decreto 914/1969⁹⁰.

Desconocemos si existen verdaderamente archivos centrales –y no meros almacenes (Martínez 1999, p. 117)- en los órganos territoriales de la Administración General del Estado (Delegaciones del Gobierno en las

⁸⁷ Orden TIN/3130/2008, de 30 de octubre, por la que se crea la Comisión Calificadora de Documentos Administrativos del Ministerio de Trabajo e Inmigración (BOE nº 267, de 5 de noviembre).

⁸⁸ Cfr. López Alonso, R.M. 2003. Los Archivos de la Administración Delegada: las Delegaciones Provinciales y Autonómicas. En *Actas de las III Jornadas de Gestión del Patrimonio Documental. Archivos de la Administración Provincial: diputaciones, gobiernos civiles, delegaciones, audiencias, histórico-provinciales*. Córdoba: Diputación Provincial, pp. 259-295.

⁸⁹ De titularidad estatal pero gestionados por las respectivas Comunidades Autónomas, salvo en el caso de los AHP de Álava, Vizcaya y Guipúzcoa, gestionados aún por la Administración General del Estado a través del Ministerio de Cultura.

En las provincias de A Coruña, Islas Baleares, Navarra y Valencia, viene ejerciendo estas funciones los Archivos de los antiguos reinos, respectivamente: Archivo del Reino de Galicia (*Arquivo do Reino de Galicia*), Archivo del Reino de Mallorca (*Arxiu del Regne de Mallorca*) – en este caso con el Archivo Histórico Provincial de Mahón (*Arxiu Històric de Maó*) con respecto del ámbito territorial de la actual Dirección Insular de la AGE en Menorca-, Archivo General de Navarra y Archivo del Reino de Valencia (*Arxiu del Regne de València*), todos ellos de gestión autonómica (aunque su titularidad –salvo en el caso del Archivo General de Navarra- es estatal). En Madrid, cumple su papel el Archivo General de la Administración (de titularidad y gestión estatal). Por último, la ausencia de un Archivo Histórico Provincial de Barcelona ha ocasionado que haya documentos de la administración periférica repartidos en el Arxiu Nacional de Catalunya (de titularidad y gestión autonómica), el Archivo de la Corona de Aragón (de titularidad y gestión estatal) y el antiguo Depósito Regional de Cervera (*Dipòsit d'Arxius de Cervera*, de titularidad estatal y gestión autonómica), pero desconocemos qué centro efectúa en la actualidad las funciones de archivo intermedio de la administración periférica del Estado en la provincia de Barcelona.

⁹⁰ *A la documentación producida por los servicios provinciales de la Administración Central o Institucional será de aplicación lo dispuesto en los artículos anteriores [véase nota 65], a cuyos efectos los Archivos Provinciales cumplirán la finalidad asignada al General de la Administración Civil. En los casos en que especiales circunstancias lo aconsejen, el Ministerio de Educación y Ciencia podrá crear depósitos regionales que completen la estructura archivística de la Administración Civil.*

Comunidades Autónomas; Subdelegaciones del Gobierno en las Provincias; Direcciones Insulares de la Administración General del Estado) que gestionen (o, al menos, reúnan y custodien) los documentos producidos por los servicios integrados de la Administración periférica del Estado. Aunque sabemos que existe cierta coordinación desde el Ministerio de Política Territorial y Administración Pública. Así, en el *Informe de evaluación sobre el funcionamiento de los servicios de la Administración Periférica del Estado en 2010*⁹¹ se señala que:

Debido a la falta de espacio en los edificios de las Delegaciones y Subdelegaciones del Gobierno y la necesidad de agilizar el procedimiento de destrucción de documentos o de traslado a otros archivos, se ha establecido, en colaboración con la Subdirección General de Publicaciones, Documentación y Archivo del Ministerio, un sistema común de tratamiento de archivos para toda la Administración Periférica, con criterios comunes de actuación en todas las Delegaciones y Subdelegaciones del Gobierno. Este proyecto va a tener continuidad en el Ministerio de Política Territorial y Administración Pública.

El proyecto está enmarcado en dos líneas de actuación principales:

- Elaboración de un documento de nociones básicas para ordenación y limpieza de documentos para archivar por las Delegaciones y Subdelegaciones del Gobierno, así como destrucción o transferencia de documentación a archivos intermedios.
- Se ha creado un grupo de trabajo para el estudio de series documentales, tratándose de documentos comunes generados en las Delegaciones y Subdelegaciones del Gobierno, para su destrucción o transferencia a archivos intermedios.

Aún disponemos de menos información respecto de los documentos generados por los servicios no integrados de dicha Administración periférica y su relación con los subsistemas departamentales centrales. Podríamos destacar, no obstante, los dependientes del Ministerio de Economía y Hacienda⁹² y los del sistema archivístico del Ministerio del

⁹¹ Ministerio de Política Territorial y Administración Pública. 2010. *Informe de evaluación sobre el funcionamiento de los servicios de la Administración Periférica del Estado en 2010*. Madrid: MPTAP, p. 49. Disponible en: http://www.mpt.gob.es/ministerio/delegaciones_gobierno/informes/informe_ddgg_2010/document_es/documento.pdf [Consulta: 10 de junio de 2011].

⁹² Como señala Laso (2009, p. 90), “[q]uizá por su vinculación con el Cuerpo de Archiveros desde el año 1888, la documentación de los servicios provinciales del Ministerio de Hacienda estuvo presente en los AHP de forma temprana y generalizada, a lo que ayudó la orden de la Subsecretaría de Hacienda de 12 de enero de 1962 para la transferencia de los documentos de más de veinticinco años de antigüedad”. Destacan, por su espectacular volumen, los fondos documentales de las Delegaciones provinciales de Hacienda (actualmente,

Interior (Guardia Civil y Cuerpo Nacional de Policía; Jefaturas de Tráfico; establecimientos dependientes de Instituciones Penitenciarias)⁹³.

Por último se encontraría el subsistema de la administración instrumental o institucional, aún más heterogéneo si cabe en cuanto a su composición⁹⁴ y articulación con el resto del sistema archivístico de la AGE, debido al distinto grado de autonomía que confieren a las entidades que lo integran sus respectivos regímenes jurídicos. Aunque apenas disponemos de información sobre los archivos de las mismas, cabe destacar el caso de la Agencia Estatal de Administración Tributaria (AEAT)⁹⁵, institución pionera en la implantación de la Administración electrónica que ha desarrollado importantes avances en la tramitación electrónica de procedimientos y en la gestión de documentos electrónicos. La AEAT cuenta con su propia

Delegaciones de Economía y Hacienda), presentes en prácticamente todos los AHP (Laso 2009, p. 94).

Otro caso destacado y bien conocido –además de ser uno de los mejor integrados en el metasisistema estatal– es el de las Gerencias Territoriales del Catastro. Véase al respecto Garrigues Carnicer, C. 2003. Plan de Archivos Catastrales: 1999-2002, un balance. *CT/Catastro*, 49, pp. 97-132. Laso (2009, p. 99) ha destacado a este respecto “la incidencia que la consulta de estos fondos está teniendo en el servicio de los AHP”. Así –prosigue este autor– “[h]an llevado a sus salas de consulta personas con un interés estrictamente particular, que intentan localizar antecedentes para reclamar o defender sus derechos; por primera vez, en los AHP se ha sentido algo parecido a lo que es habitual en los archivos municipales urbanos: el archivo atiende las necesidades administrativas de numerosos ciudadanos como parte relevante de su tarea diaria”.

Otros servicios no integrados de la Administración periférica del Ministerio de Economía y Hacienda son las Intervenciones Delegadas Regionales y Territoriales y los Tribunales Económico-Administrativos Regionales y Locales, relacionados archivísticamente en mayor o menor medida con las Delegaciones del Ministerio.

⁹³ Véase el artículo de Casado de Otaola, L. 2007. El sistema archivístico del Ministerio del Interior y la Coordinación de los Archivos de los Servicios Periféricos. *Boletín de la ANABAD*, LVII (1), pp. 413-426. Respecto a la transferencia de documentos de las Comisarias de policía y las Jefaturas provinciales de Tráfico a los AHP, véase además Laso (2009, pp. 106-107).

⁹⁴ Pueden diferenciarse, entre las entidades de Derecho público, los organismos autónomos (art. 45 y ss. LOFAGE), las entidades públicas empresariales (art. 53 y ss. LOFAGE), las Agencias Estatales (Ley 28/2006), las entidades gestoras y servicios comunes de la Seguridad Social (Disp. Adic. sexta LOFAGE) y los organismos públicos que se rigen por su legislación específica o administraciones independientes (Disp. Adic. décima LOFAGE). Por otro lado se encuentran las sociedades mercantiles estatales, que se rigen por el ordenamiento jurídico privado, lo cual, “de ningún modo, debe suponer una desvinculación de la normativa del Estado en materia de archivos” (Martínez 1999, p. 119).

Hemos de tener en cuenta, además, que muchas de estas entidades cuentan con delegaciones periféricas, lo que hace más complejo describir un modelo genérico.

⁹⁵ Creada por el artículo 103 de la Ley 31/1990, de 27 de diciembre, de Presupuestos Generales del Estado para 1991, está configurada como una entidad de derecho público adscrita al Ministerio de Economía y Hacienda a través de la Secretaría de Estado de Hacienda y Presupuestos, aunque se rige por su legislación específica (Disp. Adic. novena de la LOFAGE).

Comisión Calificadora de Documentos Administrativos⁹⁶, bastante activa hasta la fecha. Además, alguna de sus delegaciones provinciales⁹⁷ transfiere –más o menos regularmente- documentos a los correspondientes archivos históricos provinciales⁹⁸. A pesar de ello, apenas contamos con información sobre su organización archivística y sus archiveros⁹⁹, así como si –más allá de la gestión de documentos- está llevando a cabo la función archivística que permita conservar a largo plazo los documentos de valor permanente, y garantizar su disponibilidad futura.

Además de la AEAT podríamos destacar al resto de instituciones que han constituido sus propias Comisiones Calificadoras de Documentos, lo que denotaría un aparente mayor grado de desarrollo y control archivístico¹⁰⁰. Algunas de ellas, además, han transferido documentos de sus delegaciones provinciales a los AHP.

- Agencia Española de Medicamentos y Productos Sanitarios (Ministerio de Sanidad, Política Social e Igualdad)¹⁰¹.
- Instituto de Mayores y Servicios Sociales (Ministerio de Sanidad, Política Social e Igualdad)¹⁰².
- Instituto Nacional de Gestión Sanitaria (Ministerio de Sanidad, Política Social e Igualdad)¹⁰³.

⁹⁶ Orden HAC/2991/2003, de 21 de octubre (BOE nº 259, de 29 de octubre).

⁹⁷ Por la publicación en el BOE de diferentes concursos, conocemos que los archivos de algunas Delegaciones (Madrid, Barcelona) son gestionados por empresas externas.

⁹⁸ Probablemente, fruto de un “convenio que la agencia firmó con el Ministerio de Cultura en 1998” (Laso 2009, p. 97).

⁹⁹ Sabemos que el Departamento de Informática Tributaria de la Agencia es el responsable de la organización y custodia de los archivos electrónicos corporativos de documentos electrónicos que formen parte de expedientes administrativos. Por su parte, el Departamento de Recursos Humanos se encarga del diseño y explotación de los sistemas de archivo de expedientes y procedimientos de personal y de los historiales administrativos de los empleados de la Agencia. Por otro lado, la disposición de creación de su Comisión Calificadora de Documentos Administrativos (véase nota 96) hace mención a los “diferentes tipos de archivo de la Agencia Estatal de Administración Tributaria”, aunque no hemos hallado ninguna referencia sobre los mismos.

¹⁰⁰ O, al menos, una mayor sensibilidad hacia la materia.

¹⁰¹ Orden SPI/341/2011, de 14 de febrero (BOE nº 45, de 22 de febrero).

¹⁰² Orden SAS/1775/2010, de 25 de junio (BOE nº 161, de 3 de julio). Sobre las Direcciones provinciales del antiguo Inersso (Instituto Nacional de Servicios Sociales) que han transferido documentos a AHP, véase Laso (2009, p. 121).

- Instituto Nacional de la Seguridad Social (Ministerio de Sanidad, Política Social e Igualdad)¹⁰⁴.
- Instituto Social de la Marina (Ministerio de Trabajo e Inmigración)¹⁰⁵.
- Servicio Público de Empleo (Ministerio de Trabajo e Inmigración)¹⁰⁶.
- Tesorería General de la Seguridad Social (Ministerio de Sanidad, Política Social e Igualdad)¹⁰⁷.

El sistema archivístico de la AGE se encuentra, como hemos tenido oportunidad de ver, débilmente articulado y coordinado. Se hace necesaria una ley de archivos que sirva verdaderamente de motor del sistema, defina su funcionamiento y establezca las responsabilidades de cada uno de los actores implicados. Sólo de esta manera, creemos, los archivos dejarán de ser servicios residuales de la Administración, casi con funciones museísticas, para convertirse en eje de las políticas de gestión de documentos¹⁰⁸ e información pública¹⁰⁹ de la AGE. Y podrá conservarse para las generaciones futuras –de una forma mucho más eficiente y

¹⁰³ Orden SAS/2554/2010, de 24 de septiembre (BOE nº 239, de 2 de octubre). Varios AHP conservan documentos de las Direcciones provinciales del antiguo Instituto Nacional de la Salud (Insalud). Véase Laso (2009, p. 118).

¹⁰⁴ Orden TAS/984/2007, de 11 de abril (BOE nº 91, de 16 de abril). Según Laso (2009, p. 119) –refiriéndose a las Direcciones provinciales de esta entidad gestora- “[a] pesar de las grandes masas de documentos que generan estas instituciones, solo en tres AHP podemos encontrarlos”.

¹⁰⁵ Orden TIN/349/2009, de 12 de febrero (BOE nº 44, de 20 de febrero).

¹⁰⁶ Orden TAS/3694/2006, de 23 de noviembre (BOE nº 290, de 5 de diciembre). En 9 AHP se conservan fondos de Direcciones provinciales de su antecesor, el Instituto Nacional de Empleo (INEM). Véase Laso (2009, pp. 126-127).

¹⁰⁷ Orden TAS/2862/2007, de 26 de septiembre (BOE nº 238, de 4 de octubre).

¹⁰⁸ Impulsadas gracias al avance de la Administración electrónica, aunque –en nuestra opinión- llevadas a cabo desde ópticas “cortoplacistas” y sesgadas. Las instituciones archivísticas deberían asumir un papel de coordinación en su implementación de forma integral, abarcando todo el ciclo de vida de los documentos y garantizando la conservación a largo plazo de los que tengan valor permanente.

¹⁰⁹ No nos parece coherente que, en muchos casos, ni siquiera dispongamos de los datos de contacto del archivo. Unos servicios destinados en buena medida a la información administrativa a los ciudadanos no deberían estar escondidos en las estructuras de los Ministerios, sino ser una ventana abierta a la necesaria transparencia de las administraciones públicas.

controlada que en la actualidad- esta parte de nuestro patrimonio cultural y, en definitiva, de nuestra memoria colectiva.

1. LA ARTICULACIÓN DE UN DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS

1.1. Ponerle vallas al campo. La amenaza informática y la necesidad de regular el tratamiento de datos de carácter personal

Es lugar común que el reconocimiento de este nuevo derecho, el de la protección de los datos de carácter personal, y la configuración de una normativa para dar cobertura al mismo, coincide con el nacimiento de la Sociedad de la Información. Hija de un contexto tecnológico determinado: el de la explosión de la informática¹¹⁰, en los años 60 del pasado siglo. Cuando la tecnología informática deja de ser monopolio de los Estados y las grandes corporaciones¹¹¹ -únicas instituciones capaces de adquirir y mantener las enormes y costosas computadoras de las primeras generaciones- y se pone al servicio del resto de empresas y de la sociedad en general.

Momento que coincide con la consolidación de las democracias en los países occidentales y la progresiva pérdida de legitimidad social de los regímenes autoritarios y el férreo control de la población que los

¹¹⁰ Sobre todo, con la tercera y cuarta generación de computadoras (circuitos integrados, microprocesadores).

¹¹¹ La primera computadora comercial fabricada para un uso no militar fue la UNIVAC I. Empleada inicialmente en agencias gubernamentales estadounidenses (oficina de censos, Fuerza Aérea, servicio de mapas del ejército), en enero de 1954 se instaló en la división de electrodomésticos de General Electric para gestionar los salarios de sus empleados, y posteriormente se extendió a otras empresas de gran envergadura. Los primeros ordenadores instalados en España, a finales de la década de 1950, fueron un IBM 650 de RENFE y un UNIVAC UCT de la Junta de Energía Nuclear. Ya en la década de los sesenta, el Instituto Nacional de Previsión contrató "un UNIVAC III, que fue el segundo ordenador administrativo del sector público español de entonces". En esa década, que supuso "el despertar de la informática en España", más de la mitad de los ordenadores fueron instalados por la Administración y el sector financiero (Barceló, M. 2008. *Una historia de la informática*. Barcelona: UOC, p. 134).

caracteriza¹¹². Control realizado no necesariamente a través de tecnologías informáticas, también mediante procedimientos “manuales”: voluminosas series de expedientes, dossiers y fichas personales que ofrecen testimonio del horror de esos regímenes en archivos como el de la antigua Stasi -*Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik* (BStU)- o en el propio Archivo General de la Administración – aunque no sea del todo comparable con el ejemplo anterior-, a través de los expedientes personales de actividades políticas y sindicales de la Dirección General de la Guardia Civil y los expedientes personales de información policial de la Dirección General de Seguridad del Franquismo.

No obstante, fue la generalización de las tecnologías de la información y las comunicaciones en nuestra Sociedad de la Información -concebida en este sentido en términos de amenaza¹¹³- el principal acicate para la configuración de un derecho a la protección de datos de carácter personal¹¹⁴. Asistimos, según Serrano Pérez, a una revolución incontrolada, casi a una “rebelión de las máquinas”, plagada de peligros ocultos (2003, p. 18)

Esta nueva técnica ha originado un giro radical en la forma de vida del hombre, que ahora se ve abocado no sólo a adaptarse a las nuevas tecnologías sino a aceptarlas como parte de su existencia cotidiana y en algunos casos ya como imprescindibles.

¹¹² Davara (2011, p. 59) señala que, de hecho, para algunos autores el derecho a la protección de datos de carácter personal “surgió como respuesta a los totalitarismos surgidos en la Europa de segunda mitad del siglo XX”.

¹¹³ Como ha señalado Serrano Pérez (2003, p. 89), “[l]a necesidad observada de reforzar la protección jurídica de los individuos frente a la amenaza proveniente de los tratamientos automatizados de datos personales es una consecuencia del impacto de las modernas tecnologías informáticas y su creciente utilización”.

¹¹⁴ Es el punto de arranque de las obras de Serrano Pérez (2003) y del Castillo Vázquez (2007a), que constituyen el objeto de sus respectivas tesis doctorales. Aunque Serrano no abunda mucho en la cuestión, es significativo señalar que ya en la primera oración de la introducción a su obra comienza afirmando que “[l]a informática en toda su extensión constituye una auténtica revolución” (p. 17), para terminar sentenciando –en la primera de las conclusiones finales de su libro- que “[l]a protección de la persona a través de sus datos personales informatizados es una consecuencia del desarrollo de los ordenadores y de su implantación en todos los ámbitos de la sociedad” (p. 483). Ciertamente, es una obviedad indicar que antes de la aparición de las computadoras no había datos informatizados, por lo que la anterior sentencia resulta de Perogrullo. No obstante, bastaría con prescindir de la expresión “informatizados” para descubrir el sentido que pretende dar la autora –y en el que coincide el resto de la doctrina-. Por su parte, Castillo es más explícita en alertar de la “amenaza informática”. Así, su primer capítulo (“Sobre la necesidad de proteger los datos de carácter personal”, pp. 51-74) se inicia tratando sobre “La sociedad de la información y las nuevas tecnologías” (I.1, pp. 51-59), para proseguir con la “Incidencia de las nuevas tecnologías sobre la protección de datos” (I.2.1, pp. 64-68).

El avance no tiene vuelta atrás. Frente a estas ventajas de las que disfruta a diario los inconvenientes de la informática son mucho más silenciosos, y en la mayoría de las ocasiones no resultan apreciables para el hombre. Esto significa que éste no es todavía consciente de la amenaza que supone el manejo de ordenadores, al menos en algunos campos como el que va a ser objeto de estudio por nuestra parte [el tratamiento de datos personales].

Una amenaza que se ha incrementado exponencialmente con el auge de Internet y “la facilidad de recopilación, ordenación y sistematización de datos personales que permite” (Fernández y Valero 2005, p. 328).

Ciertamente, buena parte de la doctrina jurídica viene a resaltar –de forma un tanto exagerada, a nuestro entender- esta facilidad que proporcionan las TIC. Así, Castillo (2007a, p. 64) considera que “las nuevas tecnologías convierten en sencillo lo que antes era una tarea laboriosa” y advierte (p. 65) que:

Si antiguamente los procesos de captación y compilación de datos se realizaban manualmente, la elaboración automática de estos procesos se traduce hoy en día, en una cómoda tarea que ocupará pocos minutos, a veces, segundos de dedicación. Es más, los datos obtenidos pueden montarse en sistemas integrados de información, refundiendo ficheros que ofrecerán a su elaborador un aspecto casi completo de la personalidad del afectado, quien podrá conocer sus hábitos y conductas, sin que el afectado sepa a ciencia cierta qué datos suyos se están utilizando ni para qué. De hecho, la utilización mediante procedimientos paralelos puede llegar a poner en alto riesgo las libertades civiles.

Fue el Tribunal Constitucional alemán¹¹⁵ el primero en afirmar que a través de la gestión integrada de inimaginables cantidades de datos de carácter personal, se coarta la libertad de decisión individual (Messía de la Cerda 2005, p. 268). Surgía así la denominada “teoría del mosaico”, según la cual, cualquier dato referido a una persona física, por inocuo o inofensivo que parezca, cobra especial relevancia en conexión con el resto de datos que sobre esa persona pueden circular en las redes de comunicación. Como indica Isabel-Cecilia del Castillo (2007a, pp. 41 y 63):

Ciertamente, son innumerables los datos propios de cada persona que se almacenan en todo tipo de ficheros –ya sean públicos o privados-, y cuya reunión (fortuita o

¹¹⁵ En Sentencia de 15 de diciembre de 1983, relativa a la constitucionalidad de la Ley del Censo electoral.

intencionada) podría verter con todo lujo de detalles una imagen casi perfecta de lo que somos, de cómo vivimos e, incluso, de lo que pensamos. El ser humano queda así, en el desamparo de una sociedad tecnológica, en donde el conocimiento abusivo de su esfera personal altera gravemente el desarrollo de la personalidad del individuo, por cuanto se sabe bajo la mirada atenta de un tercero que ejerce su poder desde el conocimiento de los más mínimos e insignificantes detalles de su vida.

[...]

Cobra, entonces, un primer plano «la teoría del mosaico», según la cual datos, en principio «neutros» pueden convertirse en datos «ultrasensibles» por la simple interconexión de ficheros, o el cambio de finalidad para la que fueron recogidos, dando la clave esencial que sirva para catalogar a una determinada persona.

Esta autora es bastante alarmista en este sentido, sobre todo cuando es el Estado el que tiene el control sobre los datos¹¹⁶. Así, afirma que “si no puede negarse que la presencia creciente de la Administración pública en el entorno Internet es positiva en su actividad, la utilización de las nuevas técnicas provoca un temor latente en la población” (p. 38). Temor “incontrolado” que, según la autora, “no es infundado” (p. 67 y n. 58, p. 38, respectivamente). Para más inri, recuerda (p. 68), como ejemplo temprano -y terrorífico- de la amenaza que puede suponer el tratamiento automatizado de datos personales, el uso por parte de la Alemania nazi de tabuladoras¹¹⁷ de IBM para identificar y controlar a judíos y enemigos del III Reich, confiscar sus propiedades y desplazarlos hacia los ghettos y campos de concentración, para finalmente exterminarlos¹¹⁸. Por supuesto, y en contra de lo que parece desprenderse de la lectura de algunos autores, creemos que el tratamiento informático no es una amenaza en sí mismo. Lo peligroso es la finalidad que pueda darse al mismo: como mencionamos anteriormente, la Stasi desplegó un vasto sistema de control

¹¹⁶ “El sector público no permanece ajeno a este almacenamiento de datos, ya sea como consecuencia de sus relaciones con sus funcionarios y empleados, ya sea en la prestación de sus servicios a los ciudadanos” (Castillo 2007a, p. 60)

¹¹⁷ Máquinas contables de tarjetas perforadas, aplicadas al tratamiento de datos administrativo, precedente más cercano de la primera generación de ordenadores.

¹¹⁸ Puesto de manifiesto por Edwin Black, no sin críticas por la excesiva importancia que concede al tratamiento automatizado de datos en el Holocausto. Black, E. 2001. *IBM y el holocausto: la alianza estratégica entre la Alemania nazi y la más poderosa corporación norteamericana*. Buenos Aires: Atlántida.

para la represión basado en fichas y expedientes en papel¹¹⁹; y gracias más a un importante equipo de archiveros que a las computadoras¹²⁰.

Por ello, creemos que más que una reacción ante el avance tecnológico, el nacimiento de este derecho debe entenderse más como fruto de la necesidad de regular el nuevo marco de relaciones que implica la Sociedad de la Información -que por supuesto emerge gracias a la expansión de estas tecnologías de la información y las comunicaciones- y en la que información y datos son el principal activo. Como dice Isabel Davara (2011, p. 36) "actualmente no existe actividad, pública o privada, comercial o no, que pueda sobrevivir sin tratamiento de datos de carácter personal (administrados, clientes, personal, etc.)". En este marco, las democracias occidentales han venido a reconocer el derecho de las personas a proteger los datos que de las mismas, pueden circular en manos de Administraciones Públicas y empresas privadas.

En resumen, el nacimiento de la Sociedad de la Información gracias a la rápida evolución de las tecnologías informáticas -contempladas entonces y ahora como una potencial y peligrosa amenaza, capaz de conectar y tratar con suma facilidad datos de las personas, permitiendo ofrecer una imagen perfecta de las mismas- fue el motor que propició el reconocimiento a nivel internacional de un nuevo derecho y su -también rápida y fuerte- entrada en los distintos ordenamientos jurídicos. De ello, con especial referencia a las instituciones europeas, trataremos en el siguiente apartado.

¹¹⁹ Una buena manera de acercarse a este caso la ofrece Timothy Garton Ash de la mano de su experiencia personal: Garton Ash, T. 1999. *El expediente. Una historia personal*. Barcelona: Tusquets.

¹²⁰ Nos parece excesiva la confianza en las posibilidades que otorgan algunos autores a las tecnologías informáticas para obtener en segundos, casi con un click o una búsqueda en Google, un retrato robot de las personas cuando, en otros contextos, se critica la falta de interoperabilidad de los sistemas.

1.2. Un derecho europeo para la protección de datos de carácter personal

Vista la necesidad de articular unas normas que permitieran defender las libertades de los individuos ante las injerencias en las mismas que las tecnologías podían facilitar en el marco de la nueva Sociedad de la Información, el problema fue encajar esta protección en los distintos ordenamientos jurídicos¹²¹. De acuerdo con Serrano (2001, pp. 19-20):

La protección de datos, como consecuencia de su relativa juventud, no ha encontrado desde siempre una previsión o constitucional o legal. Por ello, en el momento en que surge la necesidad de protegerse frente al avance de la recopilación de información surge también como prioritaria la necesidad de delimitar su naturaleza y su contenido, relacionándola por ello con otras categorías existentes en los ordenamientos y más consolidadas tanto a nivel internacional como a niveles nacionales.

Así, en Estados Unidos la protección de datos encontró cabida dentro del *right of privacy*, un "macroderecho protector de la esfera inmaterial y material de la persona" protegido constitucionalmente¹²², que ha ido definiendo y ampliando progresivamente su contenido por la vía jurisprudencial (Serrano 2001, pp. 29-38). En otros países, la recepción de este derecho como consecuencia de la irrupción de la informática en la

¹²¹ No entra en nuestros objetivos realizar un estudio de derecho comparado. No obstante, creemos necesario hacer un breve repaso por los antecedentes de nuestra normativa para comprender determinadas claves presentes en la misma. Para ello, seguimos fundamentalmente a E. Guichot (2005), tanto en lo que se refiere a la normativa europea, inspiradora e impulsora de nuestro ordenamiento en la materia (pp. 28-60); como a su inserción en nuestro orden constitucional (pp.61-168). Serán constantes, por ello, las referencias a esta obra, a la que remitimos para un análisis detallado y fundamentado de estas cuestiones. Para una síntesis global de la protección jurídica de los datos de carácter personal en el Derecho internacional, con especial referencia al ámbito europeo, véase Gutiérrez Castillo, V.L. (2005).

¹²² A pesar de no contar con un reconocimiento explícito en la Constitución de los Estados Unidos, se ampara en la IVª Enmienda, referida a la libertad de los bienes personales y de la propia persona.

sociedad y su encaje en los respectivos marcos constitucionales ha sido más problemático¹²³.

El caso español –como el del resto de Estados europeos– se enmarca dentro del proceso de construcción de un derecho común europeo de la protección de datos que ha sido estudiado por Emilio Guichot (2005, pp. 21-60), y cuyos principales hitos fueron el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal; y la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos¹²⁴, que han terminado configurando como derecho fundamental la protección de los datos de carácter personal de los ciudadanos europeos. Este derecho común (p. 43)

se ha ido formando [...] en un proceso de fecundación recíproca propio de la integración jurídica europea, en que se produce un efecto *boomerang*, en el que los Derechos nacionales inspiran al Derecho europeo, y éste, finalmente, se convierte en motor de reforma de los Derechos nacionales.

La norma pionera en este sentido, e inspiradora de todo el desarrollo legislativo posterior fue el ya mencionado Convenio 108 del Consejo de Europa (CoE), de 28 de enero de 1981. No en vano, desde el seno de esta institución venían desarrollándose iniciativas en este sentido desde finales de la década de 1960, a través de resoluciones y recomendaciones, tanto generales como sectoriales, aunque sin fuerza vinculante; o de la jurisprudencia del Tribunal Europeo de Derechos Humanos, que ha venido a dar acogida “constitucional” al derecho a la protección de datos de carácter personal a través del Convenio Europeo de Derechos Humanos (en adelante, CEDH) -concretamente, entendiéndolo comprendido en el derecho al respeto a la vida privada y familiar reconocido en su art. 8-. Pero fue, como ha quedado dicho, el Convenio 108 el primer instrumento que desplegó una eficacia jurídica efectiva en esta materia, convirtiéndose

¹²³ Véase, por ejemplo, el caso de Italia, estudiado por María Mercedes Serrano (2001, pp. 35-60).

¹²⁴ Diario Oficial nº L 281, de 23 de noviembre.

en "uno de los pilares jurídico-positivos de carácter internacional" sobre la protección de datos de carácter personal (Castillo 2007a, p. 87).

Guichot (2005, pp.36-39) ha destacado tres claves del derecho del Consejo de Europa en esta materia, que marcarán además su impronta en nuestra normativa nacional. En primer lugar, no se encuentra claramente delimitada la relación entre derecho a la protección de datos y derecho a la intimidad. Para Guichot -que entiende como sinónimos las expresiones "vida privada" (que es la empleada en el derecho del Consejo de Europa) e "intimidad"- se habría producido (o se está produciendo) una ampliación del ámbito de lo "íntimo" con respecto al reducto clásico, tanto desde un plano objetivo (lo que la Ley considera perteneciente al ámbito de la intimidad) como subjetivo (lo que cada individuo considera que forma parte de su intimidad). Por su parte, Del Castillo Vázquez plantea que se ha asistido a la definición jurídica de un nuevo ámbito de protección, el de la "privacidad". De este modo, refiriéndose al Convenio 108, señala (Castillo 2007a, p. 89) que

en ningún renglón del documento se habla de la "intimidad" de las personas. Sin embargo, la referencia a la "vida privada" de los ciudadanos es constante, por ser precisamente esto lo que se trata de proteger en su texto. A saber: un valor tutelable distinto y más amplio que el de intimidad, al que engloba, pero en el que no agota su contenido.

Una segunda clave es que la protección de datos se considera necesaria tanto frente a tratamientos automatizados -que permiten un almacenamiento y cruce de información ilimitados- como los no automatizados. A pesar de que "el Convenio reduce su ámbito de aplicación objetiva a los datos que sean sometidos a tratamiento automatizado" y por tanto, en sentido contrario, "niega su protección a los datos de carácter personal que no sean sometidos a un tratamiento automatizado" (Castillo 2007a p. 89), al tratarse de una norma de mínimos, daba la opción a los Estados de ampliar o no su aplicación a los tratamientos "manuales". En este sentido, Francia declaró al suscribir el Convenio que lo aplicaría a los tratamientos no automatizados. Así lo ha entendido también, por otro lado, el Tribunal Europeo de Derechos Humanos.

La última de las claves identificadas por Guichot es la dificultad para precisar el contenido del derecho a la protección de datos en el derecho del Consejo de Europa y el alcance de sus posibles límites (recogidos en el art. 9). El contenido mínimo de este derecho podría articularse en tres ejes –que serán también los pilares de la normativa posterior–:

- Calidad de los datos (art. 5), que implica los siguientes principios:
 - o Principio de veracidad: los datos serán exactos y se actualizarán si fuera necesario
 - o Principio de seguridad: se establecerán las medidas de seguridad pertinentes para permitir la integridad de los datos y evitar los accesos, modificaciones y difusiones no autorizadas
 - o Principio de finalidad: los datos únicamente serán recogidos para fines determinados y legítimos, y no se utilizarán para finalidades incompatibles con aquéllas; serán adecuados, pertinentes y no excesivos con los mismos; etc.

- Facultades destinadas a garantizar a los ciudadanos el respeto de los principios anteriormente señalados (art. 8); singularmente, los derechos de acceso, rectificación y cancelación.

- Garantías institucionales: autoridad independiente de control, sistema sancionador, etc.

En la elaboración del derecho del Consejo de Europa en materia de protección de datos y, en particular, del Convenio 108, desempeñó un importante papel la Comunidad Económica Europea¹²⁵. De hecho, la propia Comunidad instó a los Estados miembros (Recomendación 81/679/CEE) a armonizar sus legislaciones en esta materia, tomando como referencia el Convenio del CoE (Guichot 2005, pp. 44-45).

Teniendo en cuenta que el Convenio es una norma principal y de mínimos, que precisa además de desarrollo normativo conforme a lo dispuesto en su artículo 4, y que algunos Estados, como el nuestro, habían incumplido dicha obligación de

¹²⁵ Que “incorporó los principios del Convenio núm. 108 a su propia normativa, e impulsó la adopción, el 15 de junio de 1999, de una enmienda al Convenio que permite la adhesión de la Comunidad al mismo” (Guichot 2005, p. 29).

desarrollo normativo, la Comunidad decidió impulsar el proyecto de la que habría de ser la Directiva de 1995.

Tras superar un largo iter legislativo, la Directiva 95/46/CE se convertirá, por tanto, en la norma general de referencia para la protección de este derecho a través del cual se pretenden salvaguardar otros derechos y libertades fundamentales, en particular el derecho a la intimidad o a la vida privada (términos que parecen equivalentes en el texto de la Directiva). Un derecho –el de la protección de datos de carácter personal– cuyo contenido “viene a ser reproducción de lo dispuesto en el Convenio de 1981, si bien con mayores precisiones” (Guichot 2005, p. 41).

Podríamos destacar como notas características que la Directiva 95/46/CE regula, con carácter general, cualquier tipo de tratamiento de datos personales, sean o no automatizados¹²⁶. Y en ella cobra especial fuerza el principio de consentimiento del afectado –gracias a las reformas en este sentido introducidas por los dictámenes del Comité Económico y Social y del Parlamento Europeo en su tramitación (Castillo 2005, p. 98)–, necesario para determinar la legitimidad de un tratamiento (si bien se contemplan excepciones a este tratamiento).

Finalmente, el derecho a la protección de datos de carácter personal ha adquirido naturaleza constitucional con carácter *iusfundamental*, al ser reconocido como tal en la Carta de los derechos fundamentales de la Unión Europea de 2000 (cap. II, art. 8¹²⁷) que, desde la entrada en vigor del Tratado de Lisboa, ha pasado a tener el mismo valor jurídico que los Tratados; y los derechos, libertades y principios que establece, asumidos en el Tratado de la Unión Europea.

¹²⁶ No obstante, excluye explícitamente los tratamientos de datos efectuados en el ejercicio de actividades ajenas al ámbito de aplicación del derecho comunitario y, en cualquier caso, a aquellos que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en materia penal (art. 3.2).

¹²⁷ Artículo que se basa en el art. 286 TCE y en la Directiva 95/46/CE, así como en el art. 8 del CEDH y el Convenio 108 del CoE: *Artículo 8. Protección de datos de carácter personal. 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo. previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.*

De forma paralela a este recorrido normativo que tan someramente hemos resumido, “los Estados han ido aprobando sus respectivas Leyes de Protección de Datos, a partir de los principios de mínimos sentados en el Convenio de 1981, y de los más detallados establecidos en la Directiva de 1995, a cuya transposición estaban obligados en tanto que Derecho vinculante y con primacía respecto del nacional” (Guichot 2005, p. 45), dando lugar a un fenómeno de “normación en cascada”¹²⁸: de un Derecho de mínimos del Consejo de Europa (Convenio 108 y jurisprudencia del Tribunal Europeo de Derechos Humanos en torno al art. 8 de la CEDH), pasando por un derecho comunitario más detallado (Directiva 95/46/CE), hasta llegar a un derecho pormenorizado a través de las respectivas Leyes nacionales. Proceso a través del cual se ha asistido además al reconocimiento de la naturaleza *iusfundamental* del derecho a la protección de datos en todas las escalas: en el CEDH, integrado en el derecho a la vida privada del art. 8; en la Carta de los derechos fundamentales de la UE, como derecho autónomo del derecho a la intimidad; y, a través de distintas soluciones, en las Constituciones nacionales.

Así pues, el impulso de las instituciones europeas ha dado lugar a la construcción de un “modelo europeo” que concibe la protección de datos como un derecho fundamental recogido en las Constituciones nacionales y desarrollado por leyes y normativas específicas¹²⁹. Su articulación en España, en el marco de este proceso de “normación en cascada”, será el objeto de atención de nuestro siguiente apartado.

¹²⁸ Sobre el valor del derecho europeo de la protección de datos en nuestro derecho interno y, en particular, en nuestro sistema jurídico de derechos fundamentales, véanse Guichot 2005, pp.47-57; y Castillo 2005, pp. 117-131.

¹²⁹ Modelo que ha traspasado las fronteras europeas -ya que ha sido adoptado en multitud de países (Japón, Australia, Canadá, Argentina, México, Uruguay...)- y que suele contraponerse al estadounidense, propio de dicho país, en el que la protección de datos es “una libertad civil, protegida en gran medida por un mosaico de leyes federales y estatales que protegen ciertos sectores, además de la denominada «autorregulación industrial» desarrollada esencialmente por el sector privado” (Davara 2011, p. 90).

1.3. La configuración del derecho fundamental a la protección de datos en España

En nuestro ordenamiento jurídico, la prevención con respecto al uso de las tecnologías de la información se recogió ya en la Constitución de 1978, en lo que ha sido visto como una acertada previsión del Constituyente de la trascendencia que podría llegar a tener esta cuestión. Ciertamente, nuestra Norma Fundamental fue –junto con la portuguesa de 1976¹³⁰– “una de las primeras de nuestro entorno jurídico en dedicar un precepto a las relaciones entre informática y derechos fundamentales” (Guichot 2005, p. 61). Así, el artículo 18.4 estableció que “[l]a Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”. El legislador constitucional encuadraba, por tanto, la protección legal frente a la informática, en el marco del derecho a la intimidad.

A pesar de esta temprana previsión constitucional, su necesario desarrollo legislativo fue bastante tardío, y vino de la mano de los compromisos adquiridos por España en el contexto de la integración europea¹³¹. Resulta necesario mencionar, no obstante, como antecedente de este desarrollo, la Disposición transitoria primera de la Ley Orgánica 1/1982, de 5 de mayo,

¹³⁰ Llama la atención la “mejor elaboración técnica del texto portugués”, en palabras de Pérez Luño (cit. en Serrano 2003, p. 124, n. 204). La redacción original del art. 35 de la Constitución portuguesa destaca tanto por su detalle –“claridad y contundencia”, dice Guichot (2005, p. 33)– como por su similitud con los términos que finalmente estarán presentes en la normativa internacional, sobre todo en la europea: *1. Todos los ciudadanos tendrán derecho a tomar conocimiento de lo que consta en forma de registros mecanográficos acerca de ellos y de la finalidad a que se destinan las informaciones, y podrán exigir la rectificación de los datos, así como su actualización. 2. No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada salvo cuando se trate de elaboración de datos no identificables para fines estadísticos. [...]*. Cit. en Serrano Pérez 2003, p. 61, n. 63.

¹³¹ Así, por ejemplo, I.C. del Castillo (2007a, p.75) señala que “es fácil concluir el gran estímulo que ejerció el derecho comunitario sobre un legislador que, durante años, se dejó dormir en la inobservancia del mandato constitucional contenido en el artículo 18.4 CE”.

de protección civil del derecho al honor, a la intimidad personal y familiar, y a la propia imagen¹³², que establecía que

En tanto no se promulgue la normativa prevista en el art. 18, apartado 4, de la Constitución la protección civil del honor y la intimidad personal y familiar frente a las intromisiones ilegítimas derivadas del uso de la informática se regulará por la presente ley.

Esta disposición resulta significativa, por un lado, de la consideración por parte del Legislador de que la protección de datos formaba parte de la protección de los derechos del artículo 18.1; y, por otro, del "intento de encubrir la dejación del Legislativo a la hora de cumplir la obligación que le impuso el constituyente para limitar, por vía legal, el uso de la informática", en una práctica que demostró poca eficacia para llevar a cabo su objetivo (Castillo 2005, p. 144).

Hubo que esperar hasta la promulgación de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD) para que nuestro país contara con su primera norma de protección de datos. Como ha señalado Isabel del Castillo (2005, pp. 90-91), la LORTAD

fue consecuencia tardía de la obligación señalada por el constituyente español en el artículo 18.4 CE, del mandato del Convenio [108 del CoE], junto con los Acuerdos de Schengen¹³³; actuando en su nacimiento, como aliciente decisivo, la Propuesta de Directiva del Consejo de la Comunidad Europea, relativa a la protección de las personas en lo referente al tratamiento de datos personales.¹³⁴

Podemos considerar que la LORTAD constituye el acta de nacimiento de un nuevo derecho en nuestro ordenamiento jurídico, aún insuficientemente definido, y ligado al derecho fundamental a la intimidad. Así, la Ley

¹³² Derogada por la disposición derogatoria única de la Ley Orgánica 5/1992, de 29 octubre (LORTAD).

¹³³ Davara (2011, p. 64) considera que "la promulgación de la LORTAD en 1992, tres años antes que la Directiva que luego provocaría su modificación, parece que tuvo causa, al menos indirecta, en el veto de Alemania a nuestra entrada en el denominado Acuerdo de Schengen, porque, entre otras cosas, no teníamos una legislación sobre protección de datos de carácter personal".

¹³⁴ Junto a estas razones, Cruz y Alberch han destacado también "la eclosión sucesiva de diversos escándalos que evidenciaron el caos en que estábamos sumidos". Véase Cruz Mundet, J. R.; Alberch Fugueras, R. 1999. *iArchívese! Los documentos del poder. El poder de los documentos*. Madrid: Alianza, p. 39 y ss.

“presentaba a la vez su objeto como la protección de la intimidad ante los nuevos desafíos y como la garantía de un derecho distinto, el derecho a la privacidad” (Guichot 2005 p. 66)¹³⁵.

La aprobación de la Directiva 95/46/CE hizo necesaria la adecuación de la normativa española a sus términos, a pesar de que, como hemos señalado, la LORTAD había tenido en cuenta el proyecto inicial de la norma comunitaria. De forma que se procedió a su trasposición –aunque con retraso con respecto al plazo de tres años establecido a tal efecto– mediante la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD). Esta Ley, “respetando el grueso de la LORTAD, se limitó a adaptar el texto a las diferencias existentes con la Directiva y a introducir algunas otras modificaciones” (Guichot 2005, p. 64). En síntesis, las diferencias básicas que introduce con respecto a la LORTAD son (Guichot 2005, pp. 170-171, n.248):

- Aplicación de la normativa a los ficheros no automatizados (contemplada por la Directiva 95/46/CE).
- Reconocimiento de nuevos derechos a los afectados: el derecho a la información en la recogida de datos y el derecho de oposición.
- Permite el tratamiento de datos para usos no incompatibles con la finalidad para la que fueron recabados.
- Se flexibiliza la aplicación de los principios y garantías respecto a determinados tratamientos privados (censo promocional a disposición de las empresas de marketing directo y publicidad, ficheros comunes de aseguradoras sin consentimiento del afectado, etc.).

¹³⁵ Destaca el uso que hace la LORTAD del término “privacidad”, criticado tanto en términos jurídicos como en términos lingüísticos, a pesar de que permite hacer una estratificación de los distintos niveles de la vida social de los individuos, introduciendo una nueva categoría de protección entre el ámbito público y el más restringido de la intimidad. Así, Guichot (2005, p. 65) señala que la exposición de motivos de la LORTAD “Distinguía la intimidad, cuyo ámbito coincide con el protegido por los tres primeros párrafos del artículo 18 CE, y la privacidad, que tiene un ámbito más amplio. Mientras que la primera vendría a referirse a la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona –el domicilio, las comunicaciones– la privacidad cubriría todas aquellas facetas que, interrelacionadas gracias a las posibilidades informáticas, permiten obtener un perfil de la persona en cuestión, que después puede ser utilizado para diversos fines, limitando sus posibilidades de desenvolvimiento social”. Sobre la conveniencia lingüística de este término, véase Díaz 2002.

A lo largo de este proceso, el derecho a la protección de datos ha ido consolidando su consideración como derecho fundamental autónomo -a la par que instrumental para la efectividad de los demás derechos fundamentales-, sin dejar por ello de vincularse al art. 18.4 CE -aunque aquel se extienda a los ficheros y tratamientos no automatizados y éste se refiera únicamente a la protección de la intimidad frente a la informática-. Esta consideración -que venía forjándose a través de la jurisprudencia del Tribunal Constitucional desde su primera sentencia en torno a este precepto- ha tenido su punto culminante en la Sentencia STC 292/2000, de 30 de noviembre (recurso de inconstitucionalidad 1463/2000, ponente Julio Diego González Campos) -"verdadero pilar de la interpretación jurídica de la protección de datos" (Castillo 2005, p. 307)-, en la que se delimita, frente al derecho a la intimidad, el objetivo (que comparte con éste), función, objeto y contenido de este derecho¹³⁶.

Como ha indicado Guichot (2005, p. 153):

La cuestión es que, al haberlo configurado como un derecho fundamental, ha "caído" sobre él el peso de toda la dogmática de los derechos fundamentales, formulada en sus términos doctrinales más puros en la STC 292/2000, con la necesidad de que cualquier limitación haya de encontrar un fundamento constitucional y deba contar con una previsión legal precisa. [...] no siempre se cumplen ambas premisas (fundamento constitucional directo; previsión legal suficientemente precisa). Ni tan siquiera las excepciones generales contempladas en la propia LOPD satisfacen estos requisitos...¹³⁷

Por último, hemos de indicar que la normativa reguladora de este derecho se ha completado -necesariamente, ya que la LOPD remite en numerosas ocasiones a un desarrollo reglamentario de la misma- con la entrada en vigor del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (BOE nº 17, de

¹³⁶ Sentencia que, para Guichot, arroja luces y sombras y encierra serias indeterminaciones y contradicciones (2005, p. 91): "tal vez ha querido ir "demasiado lejos", y ha "pecado" de dogmática, a la par que de excesivamente "maniquea" en la diferenciación con un derecho, el derecho a la intimidad, con el que, en palabras del TC, comparte su "objetivo" y sus "límites", pero no su función, objeto y contenido".

¹³⁷ El malabarismo jurídico a través del cual la protección de datos se considera derecho fundamental contrasta con el rechazo que provoca en algunos autores la misma consideración respecto del derecho de acceso a archivos y registros administrativos.

19 de enero). Desarrollo “ansiado y esperado” (Palomino 2009, p. 360), ya que hasta su publicación continuaron vigentes –de conformidad con la disposición transitoria tercera de la LOPD- los reglamentos de desarrollo de la LORTAD¹³⁸; y fundamental para determinar el ámbito de aplicación y los límites de nuestro régimen de protección de datos (lo cual no ha dejado de ser criticado en cuanto a defecto de técnica legislativa)¹³⁹.

¹³⁸ Singularmente, los Reales Decretos 428/1993, de 26 de marzo; 1332/1994, de 20 de junio; y 994/1999, de 11 de junio. Derogados con la entrada en vigor del Real Decreto 1720/2007, con excepción del primero de los mencionados, referente al Estatuto de la AEPD.

¹³⁹ Puede verse una síntesis de las novedades que introduce este Reglamento en el artículo de Puente Escobar (2008).

2. EL RÉGIMEN DE LA PROTECCIÓN DE DATOS EN ESPAÑA

2.1. El objeto del derecho: los datos personales y su tratamiento en ficheros de datos. Datos especialmente protegidos

2.1.1. Los datos personales y su tratamiento

La Sentencia del Tribunal Constitucional 292/2000 vino a delimitar –como dijimos- el derecho a la protección de datos en contraposición al derecho a la intimidad. Así, aunque ambos derechos comparten el objetivo de garantizar la vida privada personal y familiar, difieren en lo que se refiere a su función, objeto y contenido. Frente a la función defensiva del derecho a la intimidad, el de la protección de datos viene a otorgar a las personas “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” (FJ 6). Su objeto es cualquier dato personal -forme parte o no de la intimidad- y su contenido, una serie de principios y derechos que dotan a las personas de un poder de disposición y control sobre los mismos.

Comenzamos, por tanto, nuestro análisis del régimen legal vigente centrándonos en el objeto de ese derecho y en el concepto fundamental sobre el que se funda: el concepto de dato personal.

Por dato personal, la Ley entiende cualquier información (numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo) concerniente a personas físicas identificadas o identificables (art. 3.a LOPD). A partir de esta definición, un tanto genérica en principio, las normas hacen una delimitación positiva de aquellos datos que forman parte de su ámbito de aplicación –de lo cual podemos deducir a priori que

existirán datos de carácter personal excluidos de dicho ámbito¹⁴⁰-. Así, en el art. 2.1 LOPD se indica que la Ley será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento. Tomando en consideración ambas referencias, podemos considerar que los datos personales afectados por esta normativa son aquellos:

- *Referidos a personas físicas.* Se excluyen por tanto, con carácter general, aquellos referidos a personas jurídicas. De hecho, el Reglamento (art. 2.2) señala explícitamente que no será aplicable a los tratamientos de datos referidos a personas jurídicas.

- *Identificadas o identificables.* En este sentido, el Reglamento (art. 5.1.o) define *persona identificable* como toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Es decir, un dato por sí solo que se refiera a una persona física no se considerará afectado por este derecho a no ser que permita identificar por sí mismo a una persona o esté vinculado a otro dato que sí lo haga. Así lo ha venido considerando la doctrina de la Agencia Española de Protección de Datos (AEPD), que considera como datos de carácter personal afectados por este derecho –no sin contradicciones, en algunos casos- cualquier dato relativo a una persona, siempre que esté asociado a otro u otros que permitan identificar a la misma (por ejemplo, el nombre y apellidos de la misma o su número de DNI): la dirección o datos de una vivienda, cuando van asociados al titular de la misma (Informe Jurídico AEPD 182/2008); los datos de los animales de compañía, cuando están asociados con los de los propietarios de los mismos (IJ 319/2008); el número de teléfono, siempre que esté asociado al concreto titular del mismo (IJ 575/2008), o bien a datos identificativos adicionales como pueden ser la dirección de la vivienda¹⁴¹ (IJ 285/2006); la huella dactilar de una persona, asociada a algún dato que permita identificar a la misma (IJ 82/2010).

¹⁴⁰ Aunque, como veremos, el concepto de "dato personal" ha ido adquiriendo en nuestro Derecho un extensión tal vez desmesurada, "que abarca en la práctica cualquier información que tenga un referente personal" (Guichot 2005, p. 152).

¹⁴¹ Adviértase cómo, en este caso, ambos datos no permiten por sí solos identificar a una persona concreta.

Ahora bien, de acuerdo con la normativa, para que un dato pueda considerarse identificable, debe permitir identificar a la persona afectada sin plazos o esfuerzos desproporcionados. En este sentido, la Agencia considera como dato identificable la matrícula de los vehículos, al considerar que la identificación del titular del vehículo no exige esfuerzos o plazos desproporcionados por existir un Registro de Vehículos establecido en el Reglamento General de Vehículos (aprobado mediante Real Decreto 2822/1998, de 23 de diciembre), cuya consulta es pública para los interesados y terceros que tengan interés legítimo y directo (IJ 425/2006). O las imágenes de personas físicas identificables¹⁴² tomadas con sistemas de vídeo (sistemas de videovigilancia, webcams); aunque su almacenamiento sea temporal, para su reproducción en tiempo real, sin ser conservadas posteriormente; y, aunque, en nuestra opinión, la identificación de dichas personas pueda suponer, en determinadas ocasiones, plazos ciertamente desproporcionados¹⁴³. O la dirección IP que identifica a un ordenador en Internet, ya que la Agencia “parte de la idea de que la posibilidad de identificar a un usuario de Internet existe en muchos casos” debido a la existencia de herramientas en la red que permiten encontrar el enlace entre el nombre de dominio y la empresa o el particular; que los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios a los que han asignado direcciones IP; o a la utilización de medios “tales como cookies con un identificador único o sistemas modernos de minería de datos unidos a bases de datos con información sobre usuarios de Internet” (IJ 213/2004). A pesar de ello, en determinados procedimientos la AEPD no ha podido sino reconocer, como ha señalado Samuel Parra con respecto a la Resolución R/00027/2006, de 8 de febrero de 2006 (procedimiento PS/00192/2005), que “la IP puede identificar a un ordenador conectado a Internet en un momento del tiempo determinado, pero en

¹⁴² Ya que si no puede reconocerse a ninguna persona en concreto, no podrá considerarse identificable. Véase al respecto el Informe Jurídico 0285/2010, sobre instalación de una webcam que permita tener una visión panorámica de una localidad.

¹⁴³ Se puede acceder a una selección de informes jurídicos de la AEPD sobre esta cuestión en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/videovigilancia/index-ides-idphp.php [Consulta: 15 junio 2011]

absoluto puede identificar al señor que está sentado y escribiendo desde él”.

Similar interpretación ha realizado la Audiencia Nacional respecto de la dirección de correo electrónico, a pesar de que la AEPD¹⁴⁴ se mostraba más prudente:

La dirección de correo electrónico se forma por un conjunto de signos o palabras libremente elegidos, generalmente por su titular, con la única limitación de que dicha dirección no coincida con la correspondiente a otra persona. Esta combinación podrá tener significado en sí misma o carecer del mismo, atendiendo al grado de identificación del titular de la cuenta de correo que proporcione la dirección de que se trate. Así, existirán supuestos en los que voluntaria o involuntariamente la dirección de correo electrónico contenga información acerca de su titular que lo identifique, en los cuales no existe duda de que dicha dirección ha de ser considerada como dato de carácter personal, o supuestos en los que la dirección de correo electrónico no parece mostrar datos relacionados con la persona titular de la cuenta, de modo que no nos encontramos ante un dato de carácter personal, a no ser que otros datos (dominio, domicilio, etc.), conjunta o separadamente, permitan, como en el presente supuesto, la identificación del sujeto sin un esfuerzo desproporcionado por parte de quien procede a la identificación, en cuyo caso, la dirección de correo electrónico quedará amparada por el régimen establecido en la LOPD.

A pesar de ello, la Sentencia de la Audiencia Nacional (Sala de lo Contencioso Administrativo, Sección Primera) de 15 enero 2011 (recurso nº 297/2010, ponente María Luz Lourdes Sanz Calvo) considera, remitiéndose a una sentencia anterior (SAN de 25 de mayo de 2006),

que la dirección de correo electrónico de que es titular una persona física constituye un dato personal porque “con independencia de que la denominación de la dirección corresponda o no con el nombre y apellido de su titular, país o empresa en la que trabaja, lo cierto es que se puede mediante una operación nada difícil, identificar perfectamente a una persona física, ya que esa dirección de correo electrónico aparecerá vinculada a un dominio concreto, por lo que sólo será necesario consultar al servidor en que se gestione dicho servicio. [...]”

Por tanto, la dirección de correo electrónico de una persona física, en la medida que permite identificar a su titular sin plazos ni actividades desproporcionadas, constituye un dato personal y su tratamiento en casos como el presente, y sin perjuicio de las previsiones específicas establecidas por la Ley de Servicios de

¹⁴⁴ Resolución R/00027/2006, de 8 de febrero de 2006 (procedimiento PS/00192/2005).

Sociedad de la Información para otros supuestos, está sometido a las previsiones de la LOPD.

La consideración de los plazos y esfuerzos como proporcionados o desproporcionados depende de los recursos de quien efectúa el tratamiento. En este sentido, la SAN (Sala de lo Contencioso Administrativo, Sección Primera) 1485/2002, de 8 de marzo (recurso nº 948/2000, ponente María Nieves Buisán García), señala que “para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona”.

- *Registrados en soporte físico.* A este respecto, y por abundar más en nuestro análisis, señalaremos que el Reglamento (art. 5.2.ñ) se ha ocupado también de ofrecer una definición amplia del término *soporte*, que se refiere a cualquier objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.
- *Susceptibles de tratamiento.* Esto es, que puedan someterse a operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias (art. 3.c LOPD).

Entra en juego, con este requisito, un segundo concepto fundamental para definir el objeto de este derecho: el de tratamiento de datos. Como ha señalado Troncoso (2008, p. 43):

no basta la presencia de un dato personal para que entre en juego el derecho fundamental a la protección de datos personales. Este derecho no tiene por objeto proteger en todos los supuestos los datos personales. En cualquier documentación administrativa hay datos personales, y esto no significa que se pueda ejercer en ese caso el derecho fundamental a la protección de datos personales. Este derecho protege las libertades y los derechos fundamentales frente a los *tratamientos* de datos personales (art. 1 LOPD). [...] Este derecho no protege los datos, ya que el riesgo no es que haya datos, sino que existan tratamientos de datos personales.

2.1.2. La importancia del concepto de fichero de datos

Para que estos datos –referidos a personas físicas identificadas o identificables y registrados en soportes físicos- puedan recuperarse sin que ello conlleve plazos ni actividades desproporcionadas y puedan ser sometidos, de esta manera, a algún tipo de tratamiento de datos – entrando, por tanto, dentro del ámbito de aplicación de esta normativa- creemos que debe cumplirse, además, otra condición: que dichos datos formen parte de ficheros. Un fichero de datos –el tercero de los conceptos básicos que definen, a nuestro parecer, el objeto de este derecho- es todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso (art. 3.b LOPD). Lo que define a un fichero de datos es, por tanto, la existencia de una estructura lógica que organice de alguna manera un conjunto limitado de datos, independientemente de los soportes en los que se encuentren registrados (electrónicos, analógicos o mixtos), dónde se almacenen (en un depósito central o de forma distribuida) y los sistemas empleados para su creación y gestión. El criterio de dicha organización deberá basarse, en los ficheros no automatizados (art. 5.1.n Reglamento), en criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, sea el fichero centralizado, descentralizado o repartido de forma funcional o geográfica. En el caso de los ficheros automatizados se presupone que la recuperación de los datos personales no implica dichos esfuerzos desproporcionados, aunque la norma no lo aclara.

La vaguedad de la definición de fichero que ofrece la Ley, unida a que no existe una clara unanimidad por parte de la doctrina en considerarlo como elemento definidor del objeto del derecho, está generando problemas y contradicciones en la aplicación de la normativa por parte de las autoridades de control y los tribunales, como tendremos oportunidad de tratar más adelante. Ciertamente, la cuestión es trascendental, ya que –de ser correcta nuestra interpretación-, podríamos excluir, por ejemplo, del ámbito de aplicación de la normativa de protección de datos la mención de datos personales en documentos en papel que obren en expedientes no

organizados de forma que puedan recuperarse a partir de criterios específicos relativos a personas físicas –por ejemplo, expedientes de inspección de un centro público (una escuela, un centro de trabajo, un hospital...) por parte de un órgano de control- y no una base de datos en la que aparezcan únicamente números de DNI (IJ 334/2008) –siempre que sus cifras no se hayan generado al azar sino que pertenezcan a personas y respondan a un criterio de recogida concreto¹⁴⁵-. La cuestión es compleja, y encierra en ocasiones alguna que otra contradicción, como ya hemos adelantado y tendremos ocasión de profundizar más adelante.

Un hecho que parece afianzar nuestra posición es que el concepto de fichero de datos resulta fundamental para la determinación negativa del objeto de la normativa de protección de datos de carácter personal. Así, se excluyen de su ámbito de aplicación (art. 2.2 LOPD):

- Los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
- Los ficheros sometidos a la normativa sobre protección de materias clasificadas.
- Los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada¹⁴⁶.
- Los ficheros de personas jurídicas que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.

¹⁴⁵ Un fichero formado por un listado de números de 8 cifras asociados a una letra (no establecida al azar, sino definida a través del algoritmo empleado en el DNI, ampliamente conocido) es muy sencillo de realizar: en poco tiempo podemos crearlo mediante una hoja de cálculo e incluso colgarlo en la Red, abierto a su indización por motores de búsqueda. Para que entre dentro del objeto de la LOPD –desde nuestro punto de vista- tendría que responder a algún criterio conocido más o menos explícito: por ejemplo, si la página web que hemos creado tiene como título (definido a través de la etiqueta <title> del documento, que hace que título aparezca en la barra superior del navegador empleado para visualizarlo) “Socios del Racing de Santander”, “Personas que han solicitado ayudas sociales” o “Inculpados en delitos contra la libertad sexual”.

¹⁴⁶ No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.

Esta delimitación negativa del objeto de la normativa de protección de datos, no obstante, incluye otras dos referencias –a través del Reglamento (artículos 2.3 y 2.4, respectivamente)- a ciertos tipos de datos sin hacer referencia al concepto de fichero: en primer lugar, los relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros; y, en segundo lugar, lo que nos parece más importante para el ámbito de los archivos públicos: se excluyen del ámbito de aplicación de la normativa los datos referidos a personas fallecidas. No obstante, se prevé que las personas vinculadas al fallecido, por razones familiares o análogas, puedan dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos.

Existen, por otra parte, determinados supuestos especiales que se rigen por sus disposiciones específicas y por lo especialmente previsto, en su caso, por la propia LOPD (art. 2.3), en los cuales también es esencial la referencia al concepto de fichero, ya que se refiere únicamente a determinados tipos –que habrán de ser tenidos en cuenta, dado que se refieren a “ficheros” que podrían obrar en archivos públicos-:

- Los ficheros regulados por la legislación de régimen electoral.
- Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.
- 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.
- Los derivados del Registro Civil y del Registro Central de penados y rebeldes.

- 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.

2.1.3. Datos sensibles o especialmente protegidos

Para finalizar este apartado hemos de hacer referencia a un tipo de datos de carácter personal a los que la normativa otorga una protección especial: se trata de los denominados "datos sensibles" o, de acuerdo con la terminología de la propia Ley, "datos especialmente protegidos" (art. 7 LOPD). Entre ellos se incluyen:

- Los llamados por algunos autores "datos ultrasensibles", categoría bajo la que se incluyen los datos que revelen la ideología, afiliación sindical, religión y creencias¹⁴⁷; así como los que hagan referencia al origen racial, a la salud y a la vida sexual¹⁴⁸. Su creación con la finalidad exclusiva de almacenar este tipo de datos (salvo los referidos a la salud¹⁴⁹) está prohibida, y su tratamiento, sometido a condiciones más estrictas¹⁵⁰ que el resto de datos. Además, requieren unas medidas de seguridad especiales (medidas de nivel alto).

¹⁴⁷ Datos que únicamente podrán ser objeto de tratamiento con el consentimiento expreso y por escrito del afectado (art. 7.2 LOPD).

¹⁴⁸ Datos que únicamente podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente (art. 7.3 LOPD).

¹⁴⁹ En este caso, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder a su tratamiento para atender a las personas que a ellos acudan o hayan de ser tratados en los mismos de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad (art. 8 LOPD). El Reglamento define "datos de carácter personal relacionados con la salud" como las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética (art. 5.1.g Reglamento).

¹⁵⁰ Véanse notas 147 y 148. No obstante, podrán ser objeto de tratamiento cuando resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. También podrán ser objeto de tratamiento los datos cuando sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento (art. 7.6 LOPD).

- El resto de datos sensibles está formado por los datos de carácter personal relativos a la comisión de infracciones penales o administrativas, que sólo podrán ser incluidos en ficheros de las administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras (art. 7.4 LOPD) y a los que también se deben aplicar unas determinadas medidas de seguridad (medidas de nivel medio).

2.2. El concepto de fichero y la delimitación del objeto de protección en los archivos públicos

Una vez que hemos delimitado el objeto general del derecho a la protección de datos y antes de adentrarnos en el contenido del mismo, creemos necesario definir cuál sería el objeto de protección, a tenor de esta normativa, en nuestro ámbito de análisis, aun a riesgo de adelantar algún concepto que será desarrollado en capítulos posteriores.

Como cualquier otro servicio o establecimiento público o privado, los archivos de la Administración General del Estado han de tratar, en mayor o menor medida, con datos de carácter personal. Tanto en las tareas más técnicas (gestión de documentos) -ya que buena parte de los documentos que forman parte de sus fondos albergan en su contenido este tipo de datos, al igual que muchos de los productos informativos que realizan para el control y la recuperación de dichos documento (sistemas de información archivística)- como en las propiamente administrativas, genéricas de buena parte de los establecimientos administrativos (gestión de usuarios, gestión de recursos humanos). Cosa distinta es, creemos, pensar que a todos estos datos les es de aplicación la normativa de protección de datos.

La cuestión puede ser hartamente compleja, vista la enrevesada articulación del objeto de este derecho que hemos desgranado en la primera parte de este Capítulo. En el mismo, defendíamos que el concepto de fichero de datos era un elemento fundamental para definir el objeto del derecho a la protección de datos. Para comprobar la validez de este criterio y poder delimitar el ámbito de los archivos que estaría sujeto al régimen de la normativa de protección de datos, buscaremos la opinión de la doctrina jurídica, las propias autoridades control y la jurisprudencia, especialmente respecto del caso que nos genera más dudas: los documentos y

expedientes administrativos que gestionan y son la razón de ser primera de los archivos de la AGE¹⁵¹.

2.2.1. La opinión de la doctrina jurídica. El criterio “totalizador”

La consideración o no de los expedientes administrativos (y los documentos que los componen) dentro del ámbito de aplicación de la normativa de protección de datos es algo que “no está ni mucho menos resuelto en nuestro ordenamiento”, como han llamado la atención Fernández y Valero (2005, p. 316). Así, señalan (pp. 335-336, n. 33) que algunos autores -entre los que citan expresamente a Mestre Delgado- consideraron en su momento

que la LORTAD se aplicaba exclusivamente a los conjuntos organizados de datos (esto es, a los ficheros), lo que no dejaba de ser verosímil con fundamento en su artículo 2.1, de modo que los expedientes administrativos, al no ser conjuntos organizados de datos personales, estaban excluidos *in toto* de la Ley. [...] Este criterio, que podríamos denominar *totalizador*, era desde luego gravemente perturbador antes de 1999, pues entre otras consecuencias implicaba que, por ejemplo, la cesión interadministrativa de los datos personales obrantes en los expedientes administrativos no se sujetase a la disciplina establecida al efecto en el artículo 19 LORTAD (hoy artículo 21 [LOPD]) y sí, en cambio, al mucho más generoso régimen de auxilio informativo entre Administraciones Públicas contenido en la [LPAC] (actualmente artículo 4), lo que no parecía del todo razonable. Desde luego, tras la [LOPD] la interpretación que sitúa como eje exclusivo de la disciplina de protección de datos al concepto de fichero parece sencillamente insostenible¹⁵².

No creemos que esta cuestión generase muchas perturbaciones antes de 1999 –en plena vigencia de la LORTAD–, cuando la normativa se aplicaba únicamente a los tratamientos automatizados, ya que la problemática no

¹⁵¹ Dejamos por tanto, de lado, lo referido a las tareas propiamente administrativas (gestión de clientes/usuarios, gestión de recursos humanos), genéricas a cualquier otro tipo de establecimiento público o privado, y comúnmente comprendidas en la esfera de actuación de la legislación de protección de datos de carácter personal.

¹⁵² El origen de la interpretación totalizadora pudo estar, para estos autores, en “algún punto la propia LORTAD de 1992 y que fue más tarde alimentada por el considerando 27º de la [Directiva 95/46/CE] (que establece que Las carpetas y conjuntos de carpetas, así como sus portadas, que no estén estructuradas conforme a criterios específicos no están comprendidas en ningún caso en el ámbito de aplicación de la presente Directiva)” (Fernández y Valero 2005, p. 335, n. 33).

existe tanto en los documentos electrónicos¹⁵³ como en los documentos en papel. Ni nos parece tampoco que, a partir de la LOPD, este criterio sea insostenible, ya que aún a día de hoy se plantean las mismas dudas ante una lectura detallada de la normativa -quizás debido a lo que ha supuesto en este sentido el desarrollo de los preceptos de la LOPD a través del Reglamento de 2007- como la que realizábamos en páginas anteriores; e incluso, avanzando algo que señalaremos más adelante, las propias agencias de protección de datos vienen defendiendo este criterio¹⁵⁴.

Por otro lado, la consideración del concepto de fichero como elemento fundamental para definir el objeto del derecho a la protección de datos, no implica la exclusión *per se* de todos los expedientes administrativos del régimen de la protección de datos. Como tendremos ocasión de analizar posteriormente, existen determinadas series de expedientes organizadas por criterios personales que, a nuestro entender, entrarían de lleno en el ámbito de aplicación de esta normativa.

El criterio "totalizador" es defendido actualmente por buena parte de la doctrina jurídica más cualificada. Así, Emilio Guichot ha señalado (2009, p. 186) que "puede sostenerse que ésta [la normativa sobre protección de datos] no es de aplicación si la información no se encuentra en un fichero, en el concepto del mismo que acuña la LOPD". Por ello, considera cuestionable -"y este parece ser el sentido de la Ley"- que la información obrante en archivos o expedientes administrativos que no responda a criterios subjetivos de clasificación -sino, "por ejemplo, a la localización, en el caso de los inmuebles; al número de matrícula, en el caso de los vehículos¹⁵⁵; etc."- tenga que someterse a la normativa de protección de datos.

De forma similar -aunque huyendo de mencionar expresamente el término "fichero"- se ha expresado también el director de la Agencia de Protección

¹⁵³ Que deberían permitir sin plazos o esfuerzos desproporcionados identificar a las personas, salvo error en el diseño de los mismos o del software empleado para su gestión.

¹⁵⁴ Si bien no podemos dejar de advertir que con múltiples contradicciones, debido sin duda a la confusa redacción de la normativa.

¹⁵⁵ El número de matrícula es considerado por la AEPD, como vimos anteriormente, un dato personal que permite identificar al titular del vehículo sin esfuerzos o plazos desproporcionados, dada la existencia de un Registro de Vehículos cuya consulta es pública para los interesados y terceros que tengan interés legítimo y directo.

de Datos de la Comunidad de Madrid, Antonio Troncoso (2008, p. 44, n. 56):

El hecho de que aparezca incidentalmente un nombre en un documento administrativo referido no a un sujeto sino a un objeto –por ejemplo, la tramitación de una ayuda de una Comunidad Autónoma para el viñedo- no quiere decir que éste sea un dato personal [amparado por la normativa de protección de datos]. El nombre de una persona identificada –Antonio Troncoso- en un documento administrativo es un dato personal. El problema estriba en saber si existe un tratamiento de datos personales. No lo habrá si se trata de documentación administrativa que no se encuentra alfabetizada –u ordenada en virtud de personas- ni parcialmente informatizada. Sin embargo, si esa documentación administrativa se encuentra estructurada conforme a criterios personales o si está automatizada, estaríamos hablando de un tratamiento de datos personales y del derecho fundamental a la protección de datos personales.

2.2.2. La defensa del criterio totalizador por las autoridades de control

También las autoridades de protección de datos se han atrevido en ocasiones a defender explícitamente esta teoría. Por ejemplo, la Agencia de Protección de Datos de la Comunidad de Madrid (APDCM) sigue el criterio antes expresado por su Director afirmando (2008, p. 23) que:

El ordenamiento jurídico de protección de datos personales [...] sólo rige para los datos de personas físicas identificadas o identificables que se encuentran incorporados a ficheros informatizados o a ficheros manuales estructurados de acuerdo con criterios personales. Así, cuando una persona solicita una información administrativa con datos personales y no existe un tratamiento informatizado o manual estructurado se aplica directamente el art. 37 de la Ley 30/1992 [...], en el que se establece el régimen para el ejercicio por los ciudadanos de su derecho de acceso a los archivos y registros de las Administraciones Públicas. Si, por el contrario, los datos solicitados se encontraran incorporados a un fichero automatizado o manual estructurado, se aplicaría la LOPD que regularía el ejercicio del derecho de acceso del titular de los datos o la cesión de la información a terceras personas con consentimiento del interesado o habilitación legal –habilitación que podría ser el acceso con interés legítimo previsto en la [LPAC]–.

La misma postura es sostenida por la propia Agencia Española de Protección de Datos (AEPD) en diversos informes jurídicos y, lo que es más importante, en resoluciones a procedimientos de tutela de derechos.

Un ejemplo reciente lo constituye la Resolución R/00431/2009 (procedimiento TD/01520/2008), con la que se ponía fin a un procedimiento iniciado por reclamación de un particular contra la Universidad de Burgos, a la que dicha persona estaba vinculada como empleado público, en calidad de personal docente e investigador. El reclamante había solicitado ejercer sus derechos de acceso y cancelación de datos respecto de sus datos personales contenidos en cierta "documentación obrante en poder de la Universidad de Burgos relativa a los asuntos aludidos en la Resolución Rectoral de 20 de febrero de 2003" (p. 1). Alegaba el interesado que dichos documentos formaban parte de expedientes "referentes a reclamaciones e incidencias, administrativas y judiciales, habidas en el pasado, siempre como resultado de denuncias [...] finalizadas con la total exoneración de responsabilidad", cuya naturaleza y alcance, así como su inexactitud –pues consideraba que no estaban actualizados– "permiten realizar una evaluación de la personalidad del denunciante" (p. 3). La Universidad expidió al interesado copia de dichos documentos (dentro del plazo previsto al respecto del ejercicio del derecho de acceso por la normativa de protección de datos). No obstante, le denegó el derecho de cancelación, ya que consideraba que dichos expedientes no entraban ámbito de aplicación de la normativa de protección de datos. La AEPD resuelve finalmente desestimando la reclamación del particular y dando la razón a la Universidad, afirmando en su fundamento de derecho 6º (p. 4):

Respecto a la cancelación referente a sus datos personales [...], le deniegan motivadamente el derecho solicitado dado que los datos a cancelar no corresponden a datos personales contenidos en ficheros, sino a documentos que forman parte de expedientes administrativos archivados en las dependencias de la universidad denunciada. Estos documentos que se encuentran en procedimientos administrativos se regulan por las normas de ámbito administrativo, en concreto la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

No procede eliminar los documentos obrantes en expedientes administrativos, dado que la Administración tiene la obligación de archivar la documentación que pertenece a los citados expedientes, habiéndose de cumplir con la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español y sus normas de desarrollo, que rigen la guardia y custodia de dichos documentos, su almacenamiento, la forma y el tiempo de destrucción.

Como consecuencia de lo expuesto anteriormente, procede desestimar el presente procedimiento de Tutela de Derechos.

A pesar de lo visto, la AEPD sigue interviniendo, tanto a instancia de parte como de oficio¹⁵⁶, en casos en los que no está clara la existencia o no de fichero de datos. Actuando –y aplicando la normativa de protección de datos- sin llegarse a plantear si entran o no en su dentro de su ámbito de actuación. O, mejor dicho, dando por sentada la primera opción.

2.2.3. Jurisprudencia en torno a un caso paradigmático: la polémica de los Libros de Bautismo

Más allá de la interpretación de la doctrina jurídica y de las autoridades de control, la teoría totalizadora que denostaban Fernández y Valero en 2005 y que venimos apoyando en este trabajo, ha venido a asentarse gracias a la jurisprudencia del Tribunal Supremo en un caso que -aunque no se refiere a documentos producidos por la Administración Pública- vale la pena reseñar por referirse directamente a esta cuestión, así como por la repercusión mediática que ha tenido.

Nos referimos al caso de los Libros de Bautismo, un litigio que tiene su origen en la intención de una serie de personas de ejercer sus derechos de cancelación ante diversos obispados y arzobispados españoles con respecto a los datos que de los mismos obraban en dichos libros sacramentales. Con ello, los interesados pretendían eliminar sus datos del libro registro de personas bautizadas en la fe católica y el reconocimiento de su acto de apostasía. A raíz de las trabas o negativas dadas por las instituciones eclesíásticas, estos particulares han presentado en los

¹⁵⁶ Por ejemplo en los casos en que interviene tras desvelar los medios de comunicación la aparición de documentos públicos que contienen informaciones personales en la basura o abandonados en la vía pública. El propio director de la AEPD, Artemi Rallo (2009), ha recogido algunos casos de este tipo referidos a documentación judicial: "Documentación judicial en contenedores de basura del Tribunal Superior de Justicia del País Vasco" (resolución R/00283/2004); "Documentación judicial del Juzgado de Algeciras en la vía pública" (resolución R/00306/2008); "Documentación de la Junta Electoral de Zona de Puertollano en la basura" (resolución R/00074/2008).

últimos años cientos de reclamaciones ante la Agencia Española de Protección de Datos¹⁵⁷.

Uno de estos casos –el que enfrentaba a Manel Blat González¹⁵⁸ con el Arzobispado de Valencia– motivó la primera sentencia del Tribunal Supremo sobre la materia (STS de 19 de septiembre de 2008, ponente Margarita Robles Fernández)¹⁵⁹, a través de la cual, la Sala Tercera del alto tribunal declaró que los libros de bautismo no son ficheros de datos y, por tanto, no les es de aplicación la normativa de protección de datos. Como recoge en su fundamento de derecho 4º:

no cabe aceptar que esos datos personales [...] estén recogidos en los Libros de Bautismo, como un conjunto organizado tal y como exige el art. 3.b) de la LO 15/99 , sino que resultan son una pura acumulación de estos que comporta una difícil búsqueda, acceso e identificación en cuanto no están ordenados ni alfabéticamente, ni por fecha de nacimiento, sino sólo por las fechas de bautismo, siendo absolutamente necesario el conocimiento previo de la Parroquia donde aquel tuvo lugar, no resultando además accesibles para terceros distintos del bautizado, que no podrían solicitar ajenas partidas de bautismo.

No cabe olvidar tampoco que [...] ni la propia Administración como recoge en su Resolución, ni siquiera el propio solicitante de la cancelación, que se aquieta con aquella, han considerado los Libros de Bautismo como ficheros, según la redacción dada por la LO 15/99 y a los efectos de la aplicación de esta Ley, según prescribe su art. 2.1

Con esta sentencia¹⁶⁰ y otras del mismo o parecido tenor que la sucedieron, el criterio “totalizador” adquiere carta de naturaleza en

¹⁵⁷ Sobre todo en los años 2007 y 2008, aunque aún siguen presentándose.

¹⁵⁸ Conocemos el nombre del afectado –denominado “Sr. Víctor” en el texto publicado de la Sentencia– (amén de otros datos personales del mismo) debido a la trascendencia mediática que, como decimos, está teniendo el caso. Trascendencia que tiene su origen en el rápido desarrollo de un movimiento apóstata en España, encauzado a través de distintos colectivos (y con bastante presencia en la Red), que ha protagonizado actos multitudinarios, como el realizado en junio de 2006, coincidiendo con la visita del Papa Benedicto XVI a Valencia, cuando más de mil personas solicitaron la “baja” del registro de la Iglesia católica.

¹⁵⁹ Esta Sentencia pone fin al recurso de casación interpuesto por el Arzobispado de Valencia contra la Sentencia de la Audiencia Nacional (Sala de lo Contencioso, Sección Primera), de 10 de octubre de 2007 (ponente Carlos Lesmes Serrano). La SAN, por su parte, venía a resolver el recurso nº 171/2006, interpuesto también por el Arzobispado de Valencia contra la Resolución de la Agencia Española de Protección de Datos R/00319/2006 (procedimiento TD/0046/2006), favorable a las pretensiones del reclamante.

¹⁶⁰ Este criterio no se cuestiona tampoco en el voto particular a del Magistrado Huelin Martínez de Velasco, cuya postura se centra en señalar que, dada la importancia (esencial) del concepto de fichero para la aplicación de la normativa de protección de datos, el Supremo debería haber consultado al Tribunal de Justicia de la Comunidades Europeas (TJCE) sobre la

nuestra jurisprudencia, confirmando así la doctrina sostenida anteriormente por la Audiencia Nacional¹⁶¹ -más explícita en este sentido que la del Supremo, aunque con distinta consecuencia¹⁶²-.

A pesar de ello, la Agencia Española de Protección de Datos quiso recurrir la mencionada Sentencia de 19 de septiembre de 2008 ante el Tribunal Constitucional¹⁶³. Recurso que, no obstante, fue rechazado¹⁶⁴, al entender el Constitucional que la autoridad de control carece de la legitimación activa para interponerlo, sin que en el auto ni en el voto particular que lo acompaña se realice pronunciamiento alguno sobre el fondo de la

interpretación de dicho concepto y el de tratamiento de datos. De esta manera –para el Magistrado– se consolidaría un criterio europeo común, ya que se trata de “conceptos autónomos de derecho comunitario, incluidos en una Directiva que persigue la armonización completa de las normativas nacionales sobre protección de datos personales”. Señala dicho Magistrado que *La sentencia mayoritaria concluye que los libros bautismales no son «ficheros» en el sentido de la regulación sobre protección de datos de carácter personal y que, en consecuencia, no cabía instar al Arzobispado de Valencia para que, en virtud de esta regulación (artículo 4, apartado 3, de la Ley Orgánica 15/1999), anotara el ejercicio por el Sr. Víctor del derecho a que sus datos fueran cancelados del correspondiente libro parroquial. [...] Pues bien, mi desacuerdo no se dirige contra esta conclusión y el razonamiento que la sustenta, irrelevantes a los efectos de este voto particular, sino que se detiene en un estadio preliminar. En mi opinión, la Sala, antes de pronunciarse, debió dirigirse al Tribunal de Justicia de las Comunidades Europeas y [...] interrogarle a título prejudicial sobre la interpretación de los conceptos de «fichero de datos personales» y «tratamiento de datos personales», para, una vez obtenida respuesta, resolver en consecuencia el conflicto que subyace en este recurso de casación.*

¹⁶¹ Así, en la SAN de 10 de octubre de 2007, ponente Carlos Lesmes Serrano) que dio lugar al recurso de casación que elevó el caso al Supremo, la Audiencia Nacional, apoyándose en la Directiva 95/46/CE, afirmó (fundamento de derecho 5º) que *Lo relevante, pues, para que estemos ante un "tratamiento de datos personales" es la realización de determinadas actuaciones en relación con los mismos, actuaciones que en su descripción son muy amplias y variadas. No basta, sin embargo, la realización de una de estas actuaciones para que la ley despliegue sus efectos protectores y las garantías y derechos del afectado. Es preciso algo más: que las actuaciones de recogida, grabación, conservación, etc... se realicen de forma automatizada o bien, si se realizan de forma manual, que los datos personales estén contenidos o destinados a un fichero. Surge así un segundo concepto, que constituye también un prius necesario para la aplicación de la ley: el fichero.*

¹⁶² Ya que para la Audiencia Nacional, los Libros de Bautismo sí eran ficheros de datos “en la medida en que recogen datos de carácter personal -al menos el nombre y apellidos del bautizado y el hecho mismo de su bautismo- con arreglo a criterios preestablecidos que permiten su tratamiento [...], y están sujetos, en cuanto tales, a la legislación en materia de protección de datos”. Es de señalar que la sentencia es anterior al Reglamento de desarrollo de la LOPD (aprobado por Real Decreto 1720/2007, de 21 de diciembre), que establece que esos “criterios preestablecidos” deben ser relativos a personas físicas (art. 5.1.n), cosa que no sucede en el caso de los libros de bautismo, que consisten en una sucesión cronológica de los actos que se inscriben (en este caso, los bautismos).

¹⁶³ El 23 de octubre de 2008, la AEPD presentó un escrito de nulidad de actuación con relación a la citada STS de 19 de septiembre de 2008, al amparo de lo establecido en los artículos 240 y 241 de la Ley Orgánica del Poder Judicial. Dicho escrito fue inadmitido por el Tribunal Supremo, lo que llevó a la Agencia a interponer un recurso de amparo ante el Tribunal Constitucional.

¹⁶⁴ Auto TC (Sala Primera) 20/2011, de 28 de febrero. Inadmite a trámite el recurso de amparo 9929-2008, promovido por la Agencia española de protección de datos, en contencioso sobre cancelación de datos obrantes en los libros bautismales.

cuestión¹⁶⁵. Habremos de atenernos, por tanto, a la interpretación del Supremo –compartida por parte de la doctrina jurídica e, incluso, por las autoridades de control-, que viene a reafirmar nuestra opinión respecto a la importancia fundamental del concepto de fichero para definir el objeto de protección a través del régimen jurídico que estamos estudiando.

De este modo, podemos concluir este apartado indicando que la normativa de protección de datos será de aplicación en los archivos de la AGE sólo cuando traten con ficheros de datos.

¹⁶⁵ Una muestra del interés que suscitaba el pronunciamiento final del Tribunal Constitucional sobre esta materia lo encontramos en la opinión del archivero Gómez-Llera quien, refiriéndose a las implicaciones que pudiera tener su interpretación en la consulta a los archivos históricos, escribió (2009, p. 27): *De la solución final que establezca el Tribunal Constitucional depende en gran parte cómo haya de encarar la consulta de abundantes fondos de los archivos históricos referentes a personas vivas, como los documentos judiciales, ordenados por secuencia cronológica de incoación de procedimientos y causas. Si se considera que los libros eclesiásticos de bautizados no constituyen ficheros personales por no responder a un orden establecido de acuerdo con criterios personales, tampoco lo serán los numerosos expedientes judiciales de todo orden (penal, civil, administrativo, mercantil, social, militar...) ordenados por número de incoación del procedimiento.*

2.3. El contenido del derecho: principios de la protección de datos y derechos de las personas

El contenido del derecho a la protección de datos recogido en nuestra normativa se inspira -como ha entendido de forma evidente y expresa la jurisprudencia del Tribunal Constitucional que ha definido el mismo- "en los textos internacionales y, muy especialmente, en el Convenio del Consejo de Europa de 1981 y en la normativa comunitaria" (Guichot 2005, pp. 147-148), y al mismo dedica la LOPD sus Títulos II y III, referidos respectivamente a los "principios de la protección de datos" (arts. 4 a 12) que obligan a los sujetos pasivos de este derecho; y a los "derechos de las personas" (arts. 13 a 19) y regulados con rango de ley orgánica, entendiéndose que constituyen el desarrollo directo de este derecho.

2.3.1. Principios de la protección de datos: calidad, consentimiento y finalidad

Los llamados principios de la protección de datos (Tít. II LOPD) –calidad, consentimiento y finalidad- tienen una importancia determinante, ya que "la efectividad del derecho de cada individuo al control sobre su información personal presupone la efectividad de [dichos] tres principios" (Guichot 2005, p. 226). Están destinados a ser cumplidos por los sujetos pasivos de esta normativa, en particular:

- El responsable del fichero o del tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente (art. 3.d LOPD).

- El encargado del tratamiento¹⁶⁶: la persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados (art. 5 Reglamento)¹⁶⁷.

El primero de los principios, el de calidad de los datos (art. 4 LOPD), engloba una serie de requisitos –en relación directa con los principios de consentimiento y finalidad que trataremos después- que podríamos denominar de proporcionalidad, veracidad, y ética en la recogida de datos.

- *Requisito de proporcionalidad*: manifestación también, como tendremos ocasión de ver más adelante, del principio de finalidad, implica que 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 (art. 4.1 LOPD)¹⁶⁸.
- *Requisito de veracidad¹⁶⁹ o exactitud*: los datos de carácter personal serán exactos y puestos al día de forma que respondan como veracidad a la situación actual del afectado (art. 4.3 LOPD); si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio

¹⁶⁶ A esta figura se dedica el Capítulo II del Título II del Reglamento, en lo que ha venido a denominarse su "estatuto regulador" (Puente 2008, p. 445).

¹⁶⁷ La normativa autonómica reconoce un tercer sujeto, el usuario del fichero (Guichot 2005, p. 191), figura que ha venido a integrarse en este derecho –junto con la del responsable de seguridad- a través del Reglamento de 2007.

¹⁶⁸ Como ha señalado Rallo (2009, p.111), "lo que la LOPD denomina "exceso de los datos" con respecto a la finalidad que ha justificado su tratamiento no es sino una reformulación del principio de proporcionalidad" que debe regir para conciliar el derecho a la protección de datos con otros derechos y principios constitucionales (acceso a la información, eficacia de las Administraciones, etc.).

¹⁶⁹ Utilizando la expresión de Guichot para referirse al requisito correspondiente del Convenio 108 CoE de 1981.

del derecho de los afectados a la rectificación y cancelación (art. 4.4 LOPD).

- *Requisito de ética en la recogida de datos*¹⁷⁰: se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos (art. 4.7 LOPD), “lo que puede conectarse con el principio de consentimiento” (Guichot 2005, p. 226) que veremos a continuación.

El principio de consentimiento es considerado generalmente como el eje principal del régimen de protección de datos de carácter personal, ya que, como ha señalado Messía de la Cerda (2005, p. 270),

constituye uno de los pilares básicos de la denominada autodeterminación informativa: el consentimiento es el principal mecanismo de exteriorización de la voluntad, como sostiene Vizcaíno Calderón [2001, p. 84], sin que sea suficiente el reconocimiento del derecho a ser informado para cubrir de forma satisfactoria la exigencia del control de la información.

Dicho principio consiste en que, por norma general, los datos de carácter personal –sobre todo los especialmente protegidos– únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento inequívoco para ello (art. 6.1 LOPD y art. 10.1 Reglamento), entendiendo por consentimiento toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen (art. 3.h LOPD). No obstante, “el alcance de esta exigencia se minimiza ante el excesivo elenco de excepciones al consentimiento” que la propia ley contiene (Messía de la Cerda 2005, p. 269) en su art. 6, bastante matizado posteriormente por el art. 10 del Reglamento. Así, el consentimiento no será preciso, entre otras razones¹⁷¹, cuando:

- Lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando el tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del

¹⁷⁰ Nos basamos en este caso en Aparicio Salom, quien califica este requisito como “deberes éticos en la recogida de datos”. Cit. en Guichot 2005, p. 226, n. 347.

¹⁷¹ Véanse los referidos artículos 6 LOPD y 10 Reglamento.

tratamiento o del cesionario¹⁷² amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre (art. 10.2.a Reglamento).

- Se recojan para el ejercicio de las funciones propias de las administraciones públicas en el ámbito de las competencias que les atribuya una norma con rango de ley o una norma de derecho comunitario (art. 6.2 LOPD, art. 10.3.a Reglamento).
- 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. 6.2 LOPD, art. 10.3.b Reglamento).

El último pilar de la normativa de protección de datos es el principio de finalidad -"una de las claves del sistema de protección de datos" (Guichot 2005, p. 230)-, que aparece recogido en los artículos 4 (apartados 1 y 2) y 11 (apartado 1) de la LOPD; "los dos preceptos exigen, con diversas redacciones, la conexión entre la naturaleza de los datos y los fines del tratamiento y la cesión, respectivamente" (Messía de la Cerda 2005, p. 275). Así, los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. Destaca, por otro lado, que no se considerará finalidad incompatible el tratamiento posterior de los datos con fines históricos, estadísticos o científicos (art. 4.2 LOPD). Para ello, el Reglamento ha precisado (art. 9.1) que para la determinación de estos fines se estará a la legislación que en cada caso resulte aplicable y, en particular, a lo dispuesto en la Ley 12/1989, de 9 de mayo, Reguladora de la Función Estadística Pública (BOE nº 112, de 11 de mayo), la Ley 16/1985, de 25 junio, del Patrimonio Histórico Español (BOE nº 155, de 29 de junio) y la Ley 13/1986, de 14 de abril de Fomento y Coordinación General de la Investigación Científica y Técnica (BOE nº 93, de 18 de

¹⁷² Destinatario o cesionario (art. 5.1.h Reglamento): la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos.

abril)¹⁷³, y sus respectivas disposiciones de desarrollo, así como a la normativa autonómica en estas materias¹⁷⁴. En este sentido, la LOPD se separa –como apuntamos sucintamente con anterioridad– de su predecesora (la LORTAD), que prohibía todo uso para una finalidad distinta de aquella para la que los datos hubieran sido recogidos (art. 4.2 LORTAD).

El principio de finalidad ha de cumplirse con independencia del consentimiento, como ha destacado Messía de la Cerda (2005, p. 276):

... no es admisible sostener que la concurrencia del consentimiento elimina la necesidad de cualquier otro requisito, al entender que el interesado es soberano de sus datos y puede, por tanto, con su voluntad superar el obstáculo legal. A tal efecto, el artículo 11 se manifiesta con claridad: se exige conjuntamente el consentimiento previo y los fines legítimos de ambas partes, sin que la concurrencia o falta de uno de ellos afecte al devenir del otro. Por su parte, los artículos 4 y 6 adoptan la misma solución respecto de los actos de tratamiento. Es más, si se lee con detenimiento el párrafo 2º de todos estos preceptos, se observa que los mismos establecen un elenco de excepciones al consentimiento, a la vez que guardan silencio respecto de la exigencia del requisito teleológico. Podemos concluir, por tanto, que en estos supuestos de excepción de la voluntad del interesado se sigue exigiendo, sin embargo, la concurrencia de los citados fines.

2.3.2. Derechos de las personas

Como indicamos en su momento, estos principios que acabamos de ver son garantes de los derechos de las personas con respecto a la protección de sus datos. Y, al mismo tiempo, requieren el desarrollo normativo de estos para llevar a cabo su cometido (Título III de la LOPD). Como ha señalado Guichot (2005, p. 225):

Para hacer efectivos estos principios se requiere que el ciudadano pueda conocer en todo momento quién posee qué información sobre su persona, a qué se destina, y retirarla del conocimiento ajeno en caso de que sea información inexacta o innecesaria (derechos de consulta al registro, y de información, acceso, rectificación y cancelación), impugnando, en su caso, las decisiones basadas exclusivamente en

¹⁷³ Actualmente derogada, por lo que creemos que deberá remitir a Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación (BOE nº 131, de 2 de junio).

¹⁷⁴ A pesar de ello, habrá que atenerse a lo que establece la normativa con respecto a la conservación y/o cancelación de los datos.

el tratamiento efectuado (derecho de impugnación de valoraciones), y exigiendo la compensación por los daños sufridos (derecho a ser indemnizado).

Los principales derechos que reconoce nuestro régimen de protección de datos son los de acceso, rectificación, cancelación y oposición (conocidos también -por el acrónimo formado con sus iniciales- como derechos "arco"), a los que el Reglamento de la Ley Orgánica dedica íntegramente su Título III (arts. 23 a 36)¹⁷⁵. Sus titulares son -más allá del concepto de ciudadanos empleado en el art. 18.4 CE- las personas físicas titulares de los datos que sean objeto del tratamiento, esto es, las personas "afectadas" o interesadas (art. 3.e LOPD). Gozan de un carácter personalísimo (art. 26 Reglamento), según el cual únicamente podrán ser ejercidos por el afectado (o su representante legal, en caso de incapacidad o minoría de edad) o a través de representante de la forma establecida en el propio Reglamento.

Con respecto al primero de los derechos señalados, el derecho de acceso a los datos de carácter personal -al que haremos especial referencia-, el art. 15.1 LOPD señala que consiste en la posibilidad, por parte del interesado, de solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos. De forma más detallada, el Reglamento define y regula el ejercicio de este derecho en el Capítulo II de su Título III (arts. 27 a 30).

- *Definición*: el derecho de acceso -que no debe confundirse, como dice el art. 27.3 con el que otorgan las leyes especiales y en particular la Ley 30/1992- es el derecho del afectado a obtener del responsable del fichero información sobre sus propios datos de carácter personal: si están siendo objeto de tratamiento, con qué finalidad, cuál es el origen de dichos datos y qué comunicaciones se han realizado o se prevén hacer (art. 27.1).
- *Solicitud*: puede referirse tanto a datos concretos, como a datos incluidos en un determinado fichero o a la totalidad de sus datos sometidos a tratamiento; no obstante, cuando razones de especial complejidad lo justifiquen, el responsable del fichero podrá solicitar del afectado la especificación de los ficheros respecto de los cuales quiera

¹⁷⁵ Capítulo I: Disposiciones generales (arts. 23 a 26); Capítulo II: Derecho de acceso (arts. 27 a 30); Capítulo III: Derechos de rectificación y cancelación (arts. 31 a 33); y Capítulo IV: Derecho de oposición (arts. 34 a 36).

ejercitar el derecho de acceso, a cuyo efecto deberá facilitarle una relación de todos ellos (art. 27.2).

- *Plazo de resolución* (art. 29.1): el responsable del fichero deberá resolver sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo. Si en dicho plazo el interesado no recibe respuesta expresa, podrá interponer ante la Agencia de Protección de Datos una reclamación de tutela de derechos.
- *Denegación de derecho de acceso*: el acceso podrá denegarse únicamente cuando el derecho ya haya sido ejercitado por el mismo interesado en los doce meses anteriores a la solicitud, salvo que se acredite un interés legítimo al efecto (art. 30.1); o cuando así lo prevea una Ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso (art. 30.2). En cualquier caso, la comunicación que recoja la resolución denegando el acceso informará del derecho del afectado a recabar la tutela de la Agencia de Protección de Datos (art. 30.3).
- *Ejercicio del acceso*:
 - o *Plazo* (art. 29.2): si no se ofrece en el momento de comunicarse la resolución, el acceso deberá hacerse efectivo durante los diez días siguientes a dicha comunicación.
 - o *Sistemas de consulta*: el acceso se ofrecerá de forma gratuita, pudiendo además optar el afectado –siempre que sea posible, en función de la configuración o implantación material del fichero o de la naturaleza del tratamiento¹⁷⁶– por recibir la información a través de uno o varios sistemas de consulta del fichero: visualización en pantalla; escrito, copia o fotocopia remitida por correo, certificado o no; telecopia; correo electrónico u otros sistemas de comunicaciones electrónicas; o cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable (art. 28.1 y 28.2). El responsable del fichero deberá cumplir al facilitar el acceso con las medidas de seguridad que correspondan según el Título VIII del Reglamento¹⁷⁷ (art. 28.3).
 - o *Formato de la información* (art. 29.3): la información que se proporcione, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos. Dicha información comprenderá todos los datos de base

¹⁷⁶ Aunque debe asegurarse la comunicación escrita si el afectado así lo exige (art. 28.2). Por otro lado, si el responsable ofreciera un sistema con las medidas de seguridad exigibles y el afectado exigiese otro, a través de un procedimiento que implique un coste desproporcionado, surtiendo el mismo efecto y garantizando la misma seguridad el procedimiento ofrecido por el responsable, serán de cuenta del afectado los gastos derivados de su elección (art. 28.3).

¹⁷⁷ No obstante, “Si tal responsable ofreciera un determinado sistema para hacer efectivo el derecho de acceso y el afectado lo rechazase, aquél no responderá por los posibles riesgos que para la seguridad de la información pudieran derivarse de la elección” (art. 28.3).

del afectado, los resultantes de cualquier elaboración o proceso informático, así como la información disponible sobre el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

El derecho de acceso permite a las personas, de esta manera, conocer los datos que sobre las mismas se encuentran en poder de una organización, así como los tratamientos que sobre los mismos se realizan y su finalidad. Se trata, por tanto, de un derecho básico para poder hacer efectivos los de rectificación, cancelación y oposición, configurando así todo un poder de disposición de una persona sobre sus propios datos (*habeas data*).

De esta forma, el derecho de rectificación otorga a la persona afectada la capacidad de exigir la modificación de aquellos datos que resulten ser inexactos o incompletos (art. 31.1 Reglamento); y el de cancelación, a que se supriman¹⁷⁸ los datos que resulten inadecuados o excesivos (art. 31.2 Reglamento) –conectando así ambos derechos con el principio de calidad de los datos-. Ambos derechos se regulan de forma conjunta en el Capítulo III del Título III del Reglamento (arts. 31 a 33):

- *Solicitud* (art. 32.1): la solicitud de rectificación deberá indicar a qué datos se refiere y la corrección que haya de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado. En la solicitud de cancelación, el interesado deberá indicar a qué datos se refiere, aportando al efecto la documentación que lo justifique, en su caso.
- *Plazo de resolución* (art. 32.2): máximo de diez días a contar desde la recepción de la solicitud.
- *Denegación*: la cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos (33.1). Podrán también denegarse los derechos de rectificación o cancelación en los supuestos en que así lo prevea una ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso (33.2). En todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de

¹⁷⁸ Sin perjuicio de que puedan estar disponibles durante un plazo determinado para la atención, por parte de las administraciones públicas y órganos judiciales, de las posibles responsabilidades que pudieran derivar del tratamiento (deber de bloqueo). De ello trataremos más adelante.

Protección de Datos o, en su caso, de las autoridades de control de las Comunidades (33.3).

Por último, el derecho de oposición (regulado en el Capítulo IV del mismo Título III del Reglamento, arts. 34 a 36) incluye los derechos de los afectados:

- a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en determinados supuestos¹⁷⁹;
- a no verse sometidos a una decisión con efectos jurídicos que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad (art. 13.1 LOPD); y
- a la impugnación de 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 LOPD).

Junto a los derechos "ARCO", hemos de recordar además otros tres a los que hemos hecho breve referencia arriba, con los que quedaría cerrado el régimen de derechos de la normativa de protección de datos:

- Derecho a la información en la recogida de datos (art. 5 LOPD)¹⁸⁰, según el cual los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco sobre el fichero o tratamiento de datos al que van destinados (finalidad, responsable, etc.) y sus derechos al respecto (acceso, rectificación, cancelación y oposición).

¹⁷⁹ Concretamente (art. 34 Reglamento): *a) Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario. b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, en los términos previstos en el artículo 51 de este Reglamento, cualquiera que sea la empresa responsable de su creación. c) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el artículo 36 de este Reglamento.*

¹⁸⁰ Conectado con el requisito de ética en la recogida de datos que forma parte, como vimos, del principio de calidad.

- *Acreditación del cumplimiento del deber de información* (art. 18 Reglamento): deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado. El responsable del fichero o tratamiento deberá conservar el soporte en el que conste el cumplimiento del deber de informar. Para el almacenamiento de los soportes, el responsable del fichero o tratamiento podrá utilizar medios informáticos o telemáticos. En particular podrá proceder al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales.
 - *Excepciones al deber de informar*: cuando los datos de carácter personal no hayan sido recabados del interesado, no será necesario informar si está expresamente previsto en una ley, si el tratamiento tiene unos fines históricos, estadísticos o científicos, o si la información al interesado resulta imposible o exige esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o de organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias (art. 5.5 LOPD). Tampoco, en el caso de los ficheros de titularidad pública, cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales (art. 24.1 LOPD)¹⁸¹.
- 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 LOPD).
- Derecho a indemnización por daño o lesión en sus bienes o derechos como consecuencia del incumplimiento de lo dispuesto en la Ley (art. 19 LOPD).

Toda vez que hemos repasado el juego de principios y derechos que contiene la normativa de protección de datos, proseguiremos este capítulo abordando las garantías institucionales que persiguen la efectividad de los mismos. Para ello, dedicaremos las siguientes páginas a la autoridad encargada de controlar y tutelar la aplicación de esta normativa (la Agencia Española de Protección de Datos) y, posteriormente, abordaremos

¹⁸¹ De acuerdo con la redacción dada a este artículo por la Sentencia del Tribunal Constitucional STC 292/2000, de 30 de noviembre.

con algo más de detalle las medidas de seguridad que exige la LOPD y, sobre todo, su Reglamento, para garantizar el cumplimiento de la misma.

2.4. La Agencia Española de Protección de Datos

Para controlar el cumplimiento de la normativa de protección de datos y ejercer la tutela de los ciudadanos cuando se atente contra sus derechos, la legislación de nuestro país previó la creación de una autoridad de control independiente –como ya obligaba el Convenio 108 del Consejo de Europa–: la Agencia Española de Protección de Datos (AEPD), creada por el artículo 34 de la derogada LORTAD. Es un ente de derecho público, con personalidad jurídica propia y plena capacidad que actúa con plena independencia de las administraciones públicas en el ejercicio de sus funciones. Se rige por lo dispuesto en la LOPD, que la dedica su Título VI (arts. 35 a 42); su Reglamento de desarrollo, en lo que se refiere a la regulación de sus procedimientos (Título IX, arts. 115 a 158); y su propio Estatuto¹⁸², principalmente en cuanto a su estructura orgánica (Capítulo III, arts. 11 a 31) y su régimen económico, patrimonial y de personal (Capítulo IV, arts. 32 a 39).

Existen además autoridades autonómicas de control, previstas en el art. 41 LOPD, que extienden sus competencias sobre los ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial¹⁸³. Dado que nuestro

¹⁸² Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos (BOE nº 106, de 4 de mayo).

¹⁸³ En la actualidad existen las siguientes autoridades autonómicas de control: la Agencia de Protección de Datos de la Comunidad de Madrid, creada por la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid; la Agencia de Protección de Datos de Cataluña, creada por la Ley 5/2002, de 19 de abril, de creación de la Agencia Catalana de Protección de Datos; y la Agencia de Protección de Datos del País Vasco, creada por la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos. Como señala la Agencia de Protección de Datos de la Comunidad de Madrid (2008, p. 745), en las últimas reformas llevadas a cabo en sus respectivos Estatutos de Autonomía, algunas Comunidades Autónomas como Baleares, Aragón y Castilla y León han asumido competencias en materia de protección de datos de carácter personal, previéndose en algún caso la posibilidad de crear una Agencia de Protección de Datos Personales.

ámbito de análisis se refiere a la Administración General del Estado, nos centraremos en analizar las funciones que le corresponde a la Agencia Española de Protección de Datos.

La primera que podemos destacar es la tutela directa de los ciudadanos en lo que se refiere a la protección de sus datos de carácter personal. Para ello, la Agencia atiende las reclamaciones formuladas por las personas afectadas (art. 37.1.d LOPD) a través de unos procedimientos establecidos al efecto (art. 18 LOPD¹⁸⁴ y de forma desarrollada en Tít. IX, Cap. II Reglamento, arts. 117 a 119)¹⁸⁵.

En segundo lugar, la AEPD se ocupa de la vigilancia y el control de los ficheros y tratamientos existentes, para velar por el cumplimiento de la legislación sobre protección de datos (art. 37.1.a LOPD). Para ello, puede recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria (art. 37.1.i LOPD), así como ejercer la potestad de inspección (art. 40 LOPD). Así mismo, le corresponde emitir, cuando procedan, las autorizaciones previstas en la normativa (art. 37.1.b) para determinados tratamientos¹⁸⁶.

En ambos casos, la Agencia podrá requerir a los responsables y los encargados de los tratamientos la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones (art. 37.1.f LOPD).

¹⁸⁴ El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación (art. 18.2 LOPD). El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses (art. 18.3 LOPD). Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo (art. 18.4 LOPD).

¹⁸⁵ Estas reclamaciones pueden conllevar un derecho de indemnización. Así, la LOPD reconoce este derecho a los interesados que, como consecuencia del incumplimiento de lo dispuesto en Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos (art. 19). Cuando se trata de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas. En el caso de los ficheros de titularidad privada, la acción se ejercerá ante los órganos de la jurisdicción ordinaria.

¹⁸⁶ Referidas a las transferencias internacionales de datos; a la exención del deber de información al interesado; y a la autorización de conservación de datos para fines históricos, estadísticos o científicos (arts. 137 a 144, 153 a 156 y 157 a 158 Reglamento, respectivamente).

Además, podrá ejercer, en su caso, la potestad sancionadora (art. 37.1.g LOPD) en los términos previstos por el Título VII de la LOPD -que establece el régimen de infracciones y sanciones (arts. 43 a 49)-, a través de los procedimientos regulados en el Capítulo III del Título IX del Reglamento (arts. 120 a 129).

Le corresponden además funciones reglamentarias, que ejerce principalmente a través de instrucciones¹⁸⁷, a través de las cuales suele tratar de adecuar determinados ficheros y tratamientos específicos a los principios de la Ley (art. 37.1.c LOPD).

También, el asesoramiento e información, tanto a los particulares (37.1.e LOPD) como a los poderes públicos, informando los proyectos de disposiciones generales que desarrollen esta normativa (art. 37.1.h LOPD). Elabora informes jurídicos a solicitud de los interesados (principalmente, responsables de ficheros), y le corresponde velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publica periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine (art. 37.1.j LOPD).

En relación con esta última cuestión, destaca el Registro General de Protección de Datos (art. 39 LOPD), órgano integrado en la AEPD en el que se inscriben obligatoriamente los ficheros públicos y privados, así como los datos relativos a los mismos que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición¹⁸⁸,

¹⁸⁷ Hasta el momento se han publicado las siguientes (señalamos con un asterisco aquellas que entendemos que continúan vigentes, al aparecer en el apartado "Legislación" del sitio web de la AEPD): Instrucción 1/1995, de 1 de marzo, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito (BOE nº 54, de 4 de marzo); Instrucción 2/1995*, de 4 de mayo, sobre garantía de los datos personales recabados en la contratación de seguro de vida de forma conjunta con un préstamo hipotecario o personal (BOE nº 110, de 9 de mayo); Instrucción 1/1996*, de 1 de marzo, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios (BOE nº 62, de 12 de marzo); Instrucción 2/1996*, de 1 de marzo, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo (BOE nº 62, de 12 de marzo); Instrucción 1/1998, de 19 de enero, relativa al ejercicio de los derechos de acceso, rectificación y cancelación (BOE nº 25, de 29 de enero); Instrucción 1/2000, de 1 de diciembre, relativa a las normas por las que se rigen los movimientos internacionales de datos (BOE nº 301, de 16 de diciembre); Instrucción 1/2004*, de 22 de diciembre, sobre publicación de sus Resoluciones (BOE nº 4, de 5 de enero de 2005); e Instrucción 1/2006*, de 12 de diciembre, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras (BOE nº 296, de 12 de diciembre).

¹⁸⁸ La notificación e inscripción de los ficheros de titularidad pública o privada en el Registro está regulada en el Capítulo II del Título V del Reglamento (arts. 55 a 64).

y cuya consulta es, como vimos, un derecho de los ciudadanos (art. 14 LOPD), instrumental para el ejercicio de los anteriores.

Por último, la LOPD encomienda otras funciones a la AEPD: redactar una memoria anual y remitirla al Ministerio de Justicia (art. 37.1.j LOPD); llevar a cabo la cooperación internacional en materia de protección de datos personales (37.1.l LOPD); y aquellas que le atribuye la Ley con respecto al tratamiento de datos estadísticos (art. 37.1.m LOPD).

2.5. Medidas de seguridad

El artículo 10 de la LOPD impone a los responsables de ficheros y a todos cuantos intervengan en cualquier fase del tratamiento un deber de secreto y custodia respecto de los datos de carácter personal. Para ello, impone una serie de medidas de seguridad (art. 9 LOPD), que han sido reguladas en el Título VII del Reglamento de la LOPD (arts. 79 a 114)¹⁸⁹.

2.5.1. Cuestiones generales y clasificación de las medidas

A través de las mismas se pretenden proteger los activos o recursos que componen los sistemas de información en que se integran los ficheros de datos, así como de definir los requisitos que afectan a los distintos agentes que participan en la gestión y uso de dichos sistemas de información. Entre estos agentes, aparte de los responsables y encargados del tratamiento, se introducen dos nuevas figuras: por un lado, la del responsable de seguridad (art. 5.2.l Reglamento), persona o personas designadas por el responsable del fichero para coordinar y controlar las medidas de seguridad aplicables en los sistemas de seguridad media y alta (ver más adelante)¹⁹⁰. Por otra, la de los usuarios, definidos (art. 85 Reglamento) como los sujetos o procesos autorizados para acceder a datos o recursos.

¹⁸⁹ Y antes de su promulgación, en el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado mediante Real Decreto 994/1999, de 11 de junio (BOE de 25 de junio), que fue derogado por éste de 2007.

¹⁹⁰ Su designación en ningún supondrá una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento. Dicha designación podrá ser única para todos los ficheros o tratamientos de datos, o diferenciada según los sistemas de tratamiento utilizados.

Es significativo el uso del concepto sistema de información como objeto de protección. El artículo 5.2.m del Reglamento define sistema de información como el conjunto de ficheros, tratamientos, programas, soportes¹⁹¹ y en su caso, equipos empleados para el tratamiento de datos de carácter personal. Y entre los activos o recursos¹⁹² que componen dichos sistemas destaca, desde nuestro punto de vista, la mención expresa al concepto de documento, que se define como todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada (art. 5.2.f Reglamento).

En este contexto, las medidas de seguridad establecidas en el Reglamento se clasifican de acuerdo a dos criterios:

- En función del sistema de tratamiento¹⁹³ empleado, se distingue entre medidas para sistemas de información automatizados; y medidas para sistemas de información no automatizados.
- En función de la mayor o menor "sensibilidad" de los datos incorporados en dichos sistemas, se diferencian unas medidas de seguridad de nivel alto (art. 81.3 Reglamento), que deben aplicarse a los sistemas que incluyan datos ultrasensibles¹⁹⁴, datos recabados para fines policiales sin consentimiento de las personas afectadas, y datos derivados de actos de violencia de género. Medidas de seguridad de nivel medio (art. 81.2 Reglamento), aplicables, en primer lugar, al resto de datos especialmente protegidos, esto es, a los relativos a la

¹⁹¹ Soporte: objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos (art. 5.2.ñ Reglamento).

¹⁹² Recurso: cualquier parte componente de un sistema de información (art. 5.2.k Reglamento).

¹⁹³ Sistema de tratamiento: modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados (art. 5.2.n Reglamento).

¹⁹⁴ Esto es, los datos que revelen la ideología, afiliación sindical, religión y creencias de los afectados; así como los que hagan referencia al origen racial, a la salud y a la vida sexual. No requieren este tipo de medidas los ficheros o tratamientos no automatizados en los que estos datos aparezcan de forma incidental o accesorio, sin guardar relación con su finalidad (art. 81.5.b Reglamento); o cuando se refieran exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos (art. 81.6 Reglamento).

comisión de infracciones administrativas o penales¹⁹⁵; en segundo lugar, a determinados tipos de datos de carácter económico y laboral enumerados en el Reglamento¹⁹⁶; y, por último, a los datos que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos. Y, finalmente, medidas de seguridad de nivel básico (art. 81.1 Reglamento), aplicables a cualquier sistema que contenga datos de carácter personal.

2.5.2. Medidas técnicas y organizativas

Podemos diferenciar dos tipos principales de medidas de seguridad: las destinadas a controlar el acceso a los sistemas de información y las referidas a la gestión de soportes y documentos. Con respecto a las primeras (control del acceso a los sistemas de información), el artículo 91 del Reglamento¹⁹⁷ establece los siguientes requisitos:

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.
2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

¹⁹⁵ Salvo, como ha quedado dicho, los referidos a actos de violencia de género, que requieren medidas de seguridad de nivel alto.

¹⁹⁶ Datos sobre solvencia patrimonial y crédito; aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias; aquellos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros; y los que sean responsabilidad de las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias, así como aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

¹⁹⁷ Referido tanto a los ficheros y tratamientos automatizados como -por remisión del art. 105.2- a los no automatizados. Respecto a estos últimos, el art. 113.1 incide en que el acceso a la documentación que forme parte de ficheros manuales con nivel de seguridad alto se limitará exclusivamente al personal autorizado.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Para cumplir con estos requisitos el Reglamento contempla distintos mecanismos:

- La identificación¹⁹⁸ y autenticación¹⁹⁹ de los usuarios (art. 93 Reglamento)²⁰⁰, en el caso de los sistemas de información automatizados.
- Medidas destinadas a controlar el acceso físico a los recursos o soportes en que se almacenan los datos de carácter personal, tanto en sistemas automatizados²⁰¹ como en sistemas no automatizados²⁰²
- Además, dispone la elaboración de determinados instrumentos para llevar a cabo este control en los sistemas con nivel de seguridad alto. En los sistemas automatizados estos instrumentos se centralizan en un registro de accesos que almacenará información sobre cada intento de acceder al sistema (art. 103 Reglamento)²⁰³. Su gestión estará bajo el

¹⁹⁸ Procedimiento de reconocimiento de la identidad de un usuario (art. 5.2.h Reglamento), de forma inequívoca y personalizada.

¹⁹⁹ Procedimiento de comprobación de la identidad de un usuario (art. 5.2.b Reglamento). Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.

²⁰⁰ En el caso de los ficheros con nivel de seguridad alto, el responsable establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información (art. 98 Reglamento).

²⁰¹ Para los ficheros de nivel de seguridad medio o alto, sólo el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información (art. 99 Reglamento).

²⁰² Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura (art. 107 Reglamento). Mientras la documentación con datos de carácter personal no se encuentre "archivada" en dichos dispositivos, por estar en proceso de revisión o tramitación, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada (art. 108 Reglamento). Los ficheros que requieran medidas de seguridad de nivel alto necesitan, además, que los armarios, archivadores u otros elementos en los que se almacenen se encuentren en áreas en las que el acceso esté protegido con puertas dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero (art. 111 Reglamento).

²⁰³ La identificación del usuario, la fecha y hora en que se realiza el intento; el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado; y, si ha sido autorizado, la

control directo del responsable de seguridad, sin que se pueda permitir su desactivación ni su manipulación. Éste se encargará además de revisar el registro al menos una vez al mes, y elaborará un informe de los problemas detectados²⁰⁴. En los sistemas no automatizados, se requieren también instrumentos similares para identificar los accesos a los documentos que puedan ser utilizados por múltiples usuarios; cuando accedan personas no autorizadas, deberá quedar registrarse esta circunstancia de acuerdo con el procedimiento establecido al efecto en el documento de seguridad (art. 113 Reglamento).

El segundo tipo de medidas podríamos encuadrarlo -como hace el Reglamento con algunas de las que englobamos bajo esta denominación-, bajo el epígrafe "gestión de soportes y documentos". Podríamos decir que estas medidas -al menos en determinados casos²⁰⁵- se refieren a procesos técnicos archivísticos, e incluirían:

- "Criterios de archivo", contemplados en este caso únicamente, con carácter general, para los sistemas no automatizados (art. 106) y que remiten a "los criterios previstos en su respectiva legislación". Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación. En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.
- Inventario y señalización de soportes y documentos. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen y ser

información que permita identificar el registro accedido. Esta información deberá poder conservarse al menos dos años.

²⁰⁴ El registro de accesos no será necesario cuando concurren las circunstancias señaladas en el art. 103 del Reglamento: a) que el responsable del fichero o del tratamiento sea una persona física; y b) que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales. La concurrencia de estas circunstancias deberá hacerse constar expresamente en el documento de seguridad.

²⁰⁵ Cuando el sistema de información sea un sistema de gestión de documentos y archivo o lo incluya; o cuando integre, en mayor o menor medida, documentos de archivo.

inventariados²⁰⁶ (art. 92.1 Reglamento). La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar –de forma obligatoria en sistemas automatizados de nivel alto (art. 101.1 Reglamento)- mediante sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas (art. 92.5 Reglamento).

- Movimiento de soportes y transmisión de documentos²⁰⁷. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad (art. 92.2 Reglamento). En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte (art. 92.3 Reglamento). Los sistemas automatizados con nivel de seguridad media y alta requerirán, además, la implantación de registros de entrada²⁰⁸ y salida²⁰⁹ de soportes (art. 97 Reglamento). El movimiento de soportes electrónicos que contengan datos de carácter personal y requieran medidas de seguridad de nivel alto, así como la transmisión de dichos datos a través de redes públicas o redes inalámbricas de comunicaciones electrónicas, implicará el cifrado de dichos datos o cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros (art. 101 y 104 Reglamento). Del

²⁰⁶ Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

²⁰⁷ Transmisión de documentos: cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo (art. 5.2.o Reglamento)

²⁰⁸ Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

²⁰⁹ Se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

mismo modo, cuando se proceda al traslado físico de la documentación contenida en sistemas no automatizados de nivel alto, deberán adoptarse medidas para impedir el acceso o manipulación de la información objeto de traslado (art. 114 Reglamento).

- Destrucción. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior (art. 92.4 Reglamento). Dicha prescripción afecta también, de acuerdo con los artículos 87 y 112 del Reglamento, a los ficheros temporales²¹⁰, copias de trabajo o reproducciones de documentos, una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

Fuera de estos dos grandes grupos de medidas, el Reglamento incluye otras referidas a la disponibilidad y el mantenimiento de los sistemas de información, como son la implantación de un registro de incidencias²¹¹ del mismo (art. 90 Reglamento)²¹²; y la realización de copias de respaldo y recuperación de los datos²¹³.

²¹⁰ Ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento (art. 5.2.g Reglamento).

²¹¹ El Reglamento entiende por incidencia cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos (art. 5.2.i Reglamento).

²¹² Así, señala la norma, deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas. En el caso de los ficheros automatizados con nivel de seguridad medio y alto, el registro de incidencias deberá recoger, además, las acciones relativas a la recuperación de datos y las personas involucradas en dicho proceso, cuando se haya producido una eliminación no prevista (art. 100 Reglamento).

²¹³ Los sistemas automatizados deberán contar con procedimientos de actuación para la realización -como mínimo semanal- de copias de respaldo que permitan recuperar los datos ante una eventual pérdida o destrucción (art. 94 Reglamento). Cuando se requiera un nivel de seguridad alto, la copia de respaldo de los datos y de los procedimientos de recuperación de los mismos se conservará en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan (art. 102 Reglamento).

2.5.3. Instrumentos administrativos: documento de seguridad, auditorías y formación

Para completar este sistema de medidas, el Reglamento dispone la existencia de diversos instrumentos administrativos que permiten llevar a cabo las mismas. El más importante de estos instrumentos es, sin duda, el documento de seguridad. Se trata de un documento interno de la organización, elaborado por el responsable del fichero o tratamiento, que recoge las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información (art. 88.1 Reglamento). El contenido básico que debe incluir este documento se recoge principalmente en el art. 88.3 del Reglamento:

- a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos²¹⁴.
- b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.
- c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros²¹⁵.
- d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

²¹⁴ Cuestión importante, ya que una organización puede contar con un documento único y comprensivo de todos los ficheros o tratamientos; documentos de seguridad individualizados para cada fichero o tratamiento; o varios documentos de seguridad, que agrupen cada uno de ellos varios ficheros o tratamientos.

²¹⁵ Personas habilitadas y/o delegadas para autorizar el acceso y tratamiento (art. 84 Reglamento); identificación del responsable o responsables de seguridad en el caso de sistema con medidas de seguridad de nivel medio o alto (art. 88.5 Reglamento); usuarios o perfiles de usuarios autorizados para trabajar con dispositivos portátiles o ubicados fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento (art. 86 Reglamento); funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información (art. 89 Reglamento); personal autorizado a acceder a soportes y documentos que contengan datos de carácter personal (art. 92.1 Reglamento); personal autorizado para controlar la realización de copias o reproducciones de documentos integrados en ficheros no automatizados con nivel de seguridad alto (art. 112.1 Reglamento). A todo ello habría que añadir el contenido referido al encargado del tratamiento, cuando lo hubiere: la autorización del acceso y cesión de datos al mismo (art. 82.1 Reglamento); identificación de los ficheros o tratamientos en que va a trabajar, con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo (art. 88.5 Reglamento); identificación de los datos personales o tratamientos que se incorporen y traten de modo exclusivo en los sistemas del encargado (art. 88.6 Reglamento). Cuando tal circunstancia afecte a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados. En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por el Reglamento.

- e) Procedimiento de notificación, gestión y respuesta ante las incidencias.
- f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.
- g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas (art. 88.7 Reglamento). Además, el contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal (art. 88.8. Reglamento).

Por otro lado, a partir del nivel medio de seguridad, los sistemas de información²¹⁶ y las instalaciones de tratamiento y almacenamiento de datos, se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento de las medidas establecidas en el Reglamento. En el caso de los automatizados se prevé la realización, además, de auditorías extraordinarias cada vez que se realicen modificaciones sustanciales en el mismo. Dicha auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias, para que el responsable del fichero o tratamiento, a través del responsable de seguridad, adopte las medidas adecuadas. Así mismo, los informes de auditoría quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las Comunidades Autónomas.

²¹⁶ Tanto automatizados como no automatizados (arts. 96 y 110 del Reglamento, respectivamente).

Por último, el Reglamento hace un hueco a la formación en materia de seguridad como requisito en las organizaciones que trabajan con datos de carácter personal. Así, establece que el responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento (art. 88.2 Reglamento).

2.6. Breve mención al régimen específico de los ficheros públicos

La Ley Orgánica de Protección de Datos recoge en su Título IV (arts. 20 a 32) una serie de disposiciones sectoriales que afectan de forma específica a los ficheros de titularidad pública, por un lado, y a los de titularidad privada, por otro. Son ficheros de titularidad pública (art. 5.1.m Reglamento) aquellos de los que son responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público. Sus disposiciones sectoriales se encuentran recogidas, principalmente, en los arts. 20 a 24 de la LOPD. Por su parte, los ficheros de titularidad privada (art. 5.1.l Reglamento) son aquellos de los que son responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que son responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica. Sus disposiciones sectoriales se encuentran principalmente en los arts. 25 a 32 de la LOPD y en el Título IV del Reglamento (arts. 37 a 51).

Centrándonos en los ficheros de titularidad pública –dado que los archivos hacia los que enfocamos nuestro trabajo se circunscriben al ámbito de lo público–, podemos señalar que sus disposiciones específicas tratan de regular, en primer lugar, la manera en que se produce su creación, modificación o supresión. Así, sólo podrá realizarse por medio de

disposición general²¹⁷ publicada con carácter previo en el Boletín Oficial del Estado o Diario Oficial correspondiente (art. 20.1 LOPD), conforme a lo establecido en los apartados 2 y 3 del art. 20 de la LOPD y en el art. 54 del Reglamento.

En segundo lugar, la LOPD reconoce una serie de excepciones a los principios de consentimiento y finalidad en la comunicación o cesión de datos entre administraciones públicas. De esta manera, aunque como norma general los datos de carácter personal recogidos o elaborados por alguna de éstas para el desempeño de sus atribuciones, no deban ser comunicados a otras para el ejercicio de competencias que versen sobre materias distintas, se establece una excepción: que la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos (art. 21.1 LOPD)²¹⁸. Podrán además, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración pública obtenga o elabore con destino a otra (art. 21.2 LOPD). En ambos supuestos no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la Ley (art. 21.4 LOPD).

Por último, se incluyen varias disposiciones (en los arts. 22 y 23 de la LOPD y en varias de sus Disposiciones Adicionales) que establecen una serie de regímenes especiales a determinados ramos y ficheros del sector público:

- Primero, a los ficheros de carácter policial creados por las Fuerzas y Cuerpos de Seguridad, a los que se permite, en determinados supuestos (arts. 22.2 y 22.3 LOPD), recoger y tratar datos personales –incluso datos ultrasensibles– sin el consentimiento de los afectados²¹⁹.

²¹⁷ Que, en el caso de los órganos de la Administración General del Estado o a las entidades u organismos vinculados o dependientes de la misma, deberá revestir la forma de Orden Ministerial o Resolución del titular de la entidad u organismo correspondiente (art. 53.1 Reglamento).

²¹⁸ La Sentencia del Tribunal Constitucional STC 292/2000, de 30 de noviembre, declaró inconstitucional y nulo un inciso de este apartado que permitía la comunicación de datos entre Administraciones cuando ésta hubiera sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regulara su uso.

²¹⁹ La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad (art. 22.2 LOPD). La recogida y tratamiento

Por otro lado, se hace especial hincapié en la cancelación de oficio de los datos cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento (art. 22.4 LOPD)²²⁰. Por último, se establecen una serie de excepciones a los derechos de acceso, rectificación y cancelación²²¹.

- En segundo lugar, a los ficheros de la Hacienda pública, reconociendo también excepciones al derecho de acceso, rectificación y cancelación²²².
- En tercer lugar, se exceptúa la aplicación del principio de consentimiento a la cesión de datos por parte del Instituto Nacional de Estadística a los ficheros y registros de población de la AGE y las administraciones autonómicas, acotando el contenido (requisito de proporcionalidad) y la finalidad de los mismos²²³.

por las Fuerzas y Cuerpos de Seguridad de datos "ultrasensibles" (los que revelen la ideología, afiliación sindical, religión y creencias; o hagan referencia al origen racial, a la salud y a la vida sexual) podrá realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales (art. 22.3 LOPD).

²²⁰ Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento. A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad (art. 22.4 LOPD).

²²¹ Los responsables de estos ficheros 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 LOPD). En el caso de ficheros mantenidos por Cuerpos de Policía autonómicos, el afectado al que se deniegue, total o parcialmente, el ejercicio de estos derechos podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de dicha Comunidad Autónoma, quienes deberán asegurarse de la procedencia o improcedencia de la denegación (art. 23.3 LOPD).

²²² Los responsables de los ficheros de la Hacienda Pública podrán denegar el ejercicio de estos derechos cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras (art. 23.2 LOPD). En el caso de ficheros mantenidos por las Administraciones tributarias autonómicas, el afectado al que se deniegue, total o parcialmente, el ejercicio de estos derechos podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de dicha Comunidad Autónoma, quienes deberán asegurarse de la procedencia o improcedencia de la denegación (art. 23.3 LOPD).

²²³ La Administración General del Estado y las Administraciones de las Comunidades Autónomas podrán solicitar al Instituto Nacional de Estadística, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes y en el censo electoral correspondientes a los territorios donde ejerzan sus competencias,

- Finalmente, la Disposición Adicional Tercera de la LOPD incorpora una serie de previsiones referidas a los expedientes instruidos al amparo de las Leyes de Vagos y Maleantes y de Peligrosidad y Rehabilitación Social²²⁴, estableciendo unas condiciones especiales para facilitar la comunicación de datos a terceros²²⁵ –en este caso, la investigación histórica- sin menoscabo de la protección de los datos personales de los afectados y de su derecho a la intimidad²²⁶.

Este régimen que acabamos de sintetizar hace, por tanto, del sector público, un ámbito privilegiado para el tratamiento de datos de carácter personal, dada la relajación de la exigencia de consentimiento del afectado y las excepciones establecidas al ejercicio de los derechos de acceso, rectificación y cancelación. O, si se prefiere, un ámbito ante el cual, los ciudadanos se encuentran más indefensos en beneficio de la eficacia de la Administración, la seguridad pública, la represión de infracciones penales o, como en el último de los supuestos señalados, la investigación y la memoria histórica.

para la creación de ficheros o registros de población (Disp. Adic. Segunda, 1 LOPD). Los ficheros o registros de población tendrán como finalidad la comunicación de los distintos órganos de cada Administración pública con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico-administrativas derivadas de las competencias respectivas de las Administraciones públicas (Disp. Adic. Segunda, 2 LOPD).

²²⁴ Esta disposición fue introducida en el texto del proyecto durante la tramitación del Dictamen de la Comisión. La portavoz del Grupo Vasco en la Comisión Constitucional, que fue quien presentó la enmienda, expuso ante dicha Comisión las razones de su inclusión: *se nos hizo receptores a todos los ponentes del proyecto de ley por parte de determinados colectivos sociales, fundamentalmente por los grupos que representan intereses de homosexuales [...] que estos expedientes, que debieran estar en sedes judiciales, están un poco por todas partes; algunos están en órganos policiales y, sobre todo, que con cierta frecuencia [...] se conocen y se usan con finalidades que debieran estar protegidas en la esfera de su intimidad personal. Se nos pedía que, aprovechando la regulación de la Lortad se incluyese una disposición adicional que permitiese, primero, que se recopilen todos estos expedientes de las viejas leyes de vagos y maleantes y de peligrosidad social y después que se les dé el tratamiento adecuado, primero, mediante la protección de los datos que contienen y también teniendo en cuenta que contienen datos de indudable interés histórico. Véase: Diario de Sesiones del Congreso de los Diputados. Comisiones, 15 de septiembre de 1999, 744, p. 744.*

²²⁵ Aunque, como tendremos ocasiones de ver, sean más restrictivas que las recogidas en la legislación reguladora del acceso a los archivos históricos.

²²⁶ Los expedientes específicamente instruidos al amparo de las derogadas Leyes de Vagos y Maleantes, y de Peligrosidad y Rehabilitación Social, que contengan datos de cualquier índole susceptibles de afectar a la seguridad, al honor, a la intimidad o a la imagen de las personas, no podrán ser consultados sin que medie consentimiento expreso de los afectados, o hayan transcurrido cincuenta años desde la fecha de aquéllos. En este último supuesto, la Administración General del Estado, salvo que haya constancia expresa del fallecimiento de los afectados, pondrá a disposición del solicitante la documentación, suprimiendo de la misma los datos aludidos en el párrafo anterior, mediante la utilización de los procedimientos técnicos pertinentes en cada caso (Disp. Adic. Tercera LOPD).

3. FICHEROS Y TRATAMIENTOS DE DATOS EN LOS ARCHIVOS PÚBLICOS

3.1. El objeto de protección en los archivos

3.1.1. Los ficheros del archivo: propuesta de sistematización

Como vimos en el capítulo anterior, la normativa de protección de datos afecta al ámbito de las tareas administrativas necesarias para el funcionamiento de los archivos que requieren el tratamiento de datos personales: la gestión de los recursos humanos y la relación con los clientes/usuarios²²⁷.

Pero, también, al tratamiento de los documentos²²⁸ que gestionan estos archivos, al menos respecto de las series²²⁹ que contienen datos de carácter personal (referidos a personas vivas, se entiende). Cabría diferenciar, no obstante, dos situaciones: la de los documentos electrónicos y la de los documentos en papel. Consideramos, así, que la totalidad de las series en soporte informático estaría afectada por la normativa de protección de datos, debido a las posibilidades de recuperación de los mismos mediante criterios personales. De hecho, si no pudiéramos recuperar documentos de este tipo de series mediante criterios personales, estaríamos ante un error en el diseño de los mismos o

²²⁷ Únicamente abordaremos en este trabajo el segundo de los casos, el de la gestión de usuarios, por ser más específico de los archivos que el primero, común al resto del personal de la AGE.

²²⁸ Incluimos también las copias que, por distintos motivos (preservación, difusión, complemento), pueden existir en los archivos.

²²⁹ La Comisión de Normas Españolas de Descripción Archivística ha definido las series como el conjunto de documentos, producidos por uno o varios agentes, que son testimonio continuado de una o varias actividades o procesos.

del software empleado para su gestión²³⁰. Por el contrario, únicamente entrarían en la órbita de esta normativa determinadas series en papel: aquellas ordenadas físicamente a partir de criterios personales, así como las que cuenten con instrumentos que permitan su recuperación a través de dichos criterios.

Lo cual nos lleva a otro ámbito, el de los sistemas de descripción archivística que incluyan entre sus puntos de acceso²³¹ elementos de carácter personal (nombre y apellidos, DNI), que se encontrarían también bajo la regulación de esta normativa.

De todos estos supuestos, probablemente el más complejo de delimitar sea el de series documentales en papel. Básicamente nos referimos, siguiendo a Terry Cook (1991), a dos grandes tipos de series:

- Series de expedientes de caso particular (*particular instance case files*) o expedientes procedimentales o resolutivos²³² referidos a personas. Integradas por expedientes encaminados a la resolución de un asunto o caso concreto y, por lo general, referidos a un único individuo, forman series con un elevado número de unidades, si bien cada una de ellas no suele ser muy voluminosa. Su contenido es generalmente homogéneo y abarca un lapso breve (semanas o meses, aunque en ocasiones varios años). A veces pueden integrarse físicamente dentro de expedientes evolutivos. Ejemplos de este tipo de series que podemos encontrar en los archivos públicos son:
 - o Expedientes disciplinarios
 - o Expedientes de selección de personal
 - o Expedientes sancionadores
 - o Expedientes de subvenciones y ayudas; expedientes de prestaciones

²³⁰ Un buen diseño identificaría (marcaría) dichos datos en la estructura lógica interna de los documentos o en sus metadatos, para su recuperación por el sistema empleado al efecto. O, de otra forma, permitiría la utilización de herramientas de indización de texto completo que permitieran dicha recuperación.

²³¹ La norma ISAD (G) define "punto de acceso" como el "nombre, término, palabra clave, frase o código que se puede utilizar para buscar, identificar y localizar una descripción archivística" (ICA 2000, p. 17).

²³² En el ámbito administrativo, los más comunes son los relacionados con el ejercicio de las potestades administrativas típicas: contractuales, expropiatorios, autorizatorios, sancionadores, disciplinarios (Rivero 2007, p. 95).

- Expedientes de concesión de títulos, premios, etc.
- Series de expedientes evolutivos (*continuing events case files*) o expedientes personales. Frente a las anteriores, estas series se componen de expedientes “abiertos” que reflejan una situación continuada en el tiempo. Contienen documentos relativos a más de un acontecimiento o transacción, si bien referidos todos a la misma persona. Ejemplos de este tipo de series pueden ser:
 - Expedientes personales de empleados públicos
 - Expedientes policiales
 - Expedientes de internos en prisiones
 - Historias clínicas de centros de salud públicos
 - Expedientes académicos de centros educativos públicos

La sujeción de este tipo de series que hemos recogido a modo de ejemplo (nada exhaustivo) –así como del resto de ficheros empleados en los supuestos referidos arriba- al régimen establecido por la LOPD y su Reglamento, implicaría, por tanto, una serie de requisitos:

- La necesidad de que se encuentren integrados en ficheros de datos, creados por una disposición general (Orden Ministerial en el caso de los órganos centrales de la AGE) publicada en el BOE²³³; e inscritos en el Registro General de Protección de Datos.
- Sobre los mismos podrán ejercer los ciudadanos sus derechos de acceso, rectificación, cancelación y oposición, con las excepciones y peculiaridades aplicables en cada caso²³⁴.
- En tercer lugar, los tratamientos que se sometan a los mismos deberán ajustarse a los principios de la protección de datos (calidad, consentimiento y finalidad), con las especiales condiciones establecidas para los ficheros públicos.

²³³ El mismo procedimiento se requiere para la modificación y supresión de estos ficheros.

²³⁴ La LOPD exige, además, la obligación de garantizar unas condiciones de conservación que permitan el ejercicio del derecho de acceso (art. 4.6) –y por extensión, creemos, del resto de derechos-. Por condiciones de conservación creemos que debemos entender no solamente las referidas a la integridad física de los soportes sino también, cuando se trate de documentos de archivo, la obligación de tratarlos archivísticamente para permitir su control y recuperación eficaz.

- Por último, deberán contar con unas medidas de seguridad concretas, adaptadas a la mayor o menor sensibilidad de los datos que contengan.

Las consecuencias que supone cumplir con estos requisitos serán abordadas en las siguientes páginas de este trabajo. En cualquier caso, consideramos que -desde el punto de vista proactivo que imprime la asunción de la gestión de documentos como función propia del archivo- los archiveros deberían ser los responsables de identificar los tratamientos de datos que se realizan en su organización referidos a documentos de archivo (aparte de los propios) para su consideración como ficheros y el cumplimiento de estas exigencias legales. El diseño de una metodología destinada a llevarlo a cabo escapa de los objetivos de este trabajo. No obstante, podemos adelantar que -vistas determinadas propuestas²³⁵-, debería incardinarse en el diseño e implementación de los sistemas propios de gestión de documentos de cada organización (ISO 15.489-1:2001, 8.4; ISO/TR 15.489-2:2001, 3).

3.1.2. Tratamientos de datos de los archivos públicos

Por lo que se refiere a los tratamientos de datos, recordemos que la LOPD entiende como tales (art. 3.c) las 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. En los mismos pueden participar directamente personas físicas o ser ejecutados íntegramente por sistemas informáticos o de otro tipo.

Partiendo de dicha definición, podemos diferenciar:

²³⁵ Por ejemplo, la propuesta por la Agencia de Protección de Datos de la Comunidad de Madrid (2008, pp. 174-189) para identificar e inventariar los ficheros de las Administraciones Locales.

- En primer lugar, las operaciones y procedimientos técnicos de recogida, grabación, elaboración y modificación de datos. La legislación no define explícitamente estos conceptos, que podríamos considerar de forma conjunta ya que todos se refieren a la entrada de datos (y su modificación) en un sistema de información –en un fichero de datos, en los términos de la Ley-, lo que en el lenguaje de las bases de datos se engloba bajo el término “actualización”; y la incorporación (registro) de dichos datos en un soporte físico, condición básica para que estos tratamientos entren dentro del ámbito de aplicación de la normativa (art. 2.1 LOPD)²³⁶. Los casos más representativos en los archivos son los relativos a la gestión de usuarios y a la elaboración de sistemas de descripción que contengan información personal.

- En segundo lugar se encuentra la conservación, sin duda el más obvio de los tratamientos de datos que se realizan en los archivos, si entendemos que en los mismos se custodian datos de carácter personal afectados por la LOPD.

- La cancelación y el bloqueo se definen de forma conjunta en el artículo 5.1.b) del Reglamento de 2007:

Cancelación: Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.

²³⁶ Serrano Pérez (2003, p. 437) equipara el término “grabación” con registro. Ciertamente, “grabación” puede entenderse como el proceso técnico de registro o incorporación de los datos a un soporte físico (por ejemplo, una grabación de audio o vídeo); pero puede generar dudas al hablarse en determinados contextos de “grabación de datos”, entendida como la entrada de datos en un sistema de información a partir de una fuente determinada (que puede ser producto de una recogida de datos al efecto; de otro sistema de información; o de cualquier otra fuente). De hecho, en muchos archivos existe la figura del “grabador de datos”, personal que incorpora a los sistemas de descripción archivística informáticos, por ejemplo, los datos de instrumentos de descripción tradicionales en papel.

Aunque no se corresponda exactamente, podemos entender el bloqueo como un plazo de reserva²³⁷ durante el cual esos datos no pueden ser consultados ni utilizados (con las excepciones referidas) por ningún usuario²³⁸. Una vez concluido este plazo de reserva o periodo de bloqueo, se debe proceder a la supresión de los datos. Así pues, podemos entender *cancelación* como la suma (o la sucesión) de los procesos de bloqueo y supresión. Recordemos además que la cancelación es una forma de tratamiento que responde a un derecho de los afectados (el derecho de cancelación).

- Por último, la cesión o comunicación de datos –dotada en nuestra legislación de un régimen específico- es toda revelación de datos realizada a una persona distinta del interesado (art. 3.i LOPD), lo que afectaría fundamentalmente al acceso a los documentos, pero también a la difusión de reproducciones de documentos en la Red (o en publicaciones impresas) o de las descripciones de los mismos.

Como vimos en el apartado anterior, los archivos deberán respetar los principios de la protección de datos (calidad, consentimiento y finalidad) en la ejecución de estos tratamientos. Tanto si son responsables del fichero o del tratamiento, como si –como sucede en el ámbito de la Administración General del Estado- dependen del órgano que ostenta dicha función. Así mismo, están obligados –cuando les corresponda- a permitir el ejercicio de los derechos de los afectados, debiendo cumplir en cualquier caso el deber de secreto estipulado por la Ley y las medidas de seguridad pertinentes en sus sistemas de información, aspectos estos que deberán cumplir también los empleados de las empresas contratadas para llevar a cabo algún trabajo o servicio en el archivo a través del cual tengan puedan tener contacto o, directamente, traten (encargados del tratamiento) con datos personales.

²³⁷ En Archivística, con esta denominación se hace referencia al período de tiempo durante el cual, según la normativa vigente, una documentación no puede ser consultada públicamente (DTA-SGAE).

²³⁸ Véase el concepto de usuario en el capítulo dedicado a las medidas de seguridad (2.5).

3.2. Cuando los archivos crean ficheros: algunas cuestiones referidas a la recogida de datos

Como hemos indicado previamente, los casos más representativos de recogida de datos personales en los archivos son los referidos a la gestión de usuarios y a la elaboración de sistemas de descripción que contengan información personal. Para analizar la incidencia de la normativa de protección de datos en la primera de estas cuestiones –la gestión de usuarios– vamos a estudiar el caso de los archivos y servicios archivísticos gestionados por el Ministerio de Cultura (los llamados Archivos Estatales), seguramente los que más usuarios atienden de todo el sistema archivístico de la AGE²³⁹. Tras ello, abordaremos la problemática relativa a los sistemas de descripción archivística y su importancia en el marco de la protección de datos.

3.2.1. Protección de datos en la gestión de usuarios de los Archivos Estatales

El registro y control de los usuarios de los archivos de la AGE se lleva a cabo, principalmente, a través de los expedientes de usuarios²⁴⁰. En ellos se reúnen los distintos documentos producidos como consecuencia del servicio del archivo a los mismos. Los principales datos personales que contienen son de carácter identificativo (nombre y apellidos, DNI) y de contacto (dirección postal a efectos de notificaciones, dirección de correo electrónico; número de teléfono). Junto a ellos se conservarán otros datos

²³⁹ En 2009 tuvieron cerca de 34.000 usuarios presenciales, más de 8.000 consultas por correo postal o fax y 21.000 telemáticas. Véase a este respecto el *Anuario de estadísticas culturales 2010* (Ministerio de Cultura 2010, p. 248).

²⁴⁰ Suelen estar divididos, por cuestiones prácticas, en varias subseries (por ejemplo, diferenciando los usuarios presenciales de los usuarios por correspondencia).

referidos a su relación con el archivo (documentos consultados, documentos reproducidos, convenios para el uso de reproducciones, datos económicos referidos al pago de precios públicos por determinados servicios). Pero estos datos no se encuentran únicamente centralizados en los expedientes de usuarios: suelen estar también presentes (de forma completa o incompleta) en distintos sistemas de información necesarios para llevar a cabo los servicios del centro. Por ejemplo, en el sistema que gestiona las de solicitudes de consulta y/o reproducción de documentos (actualmente, aplicaciones informáticas diseñadas al efecto²⁴¹) o en las aplicaciones destinadas a la facturación de reproducciones.

Los datos se conservan, por tanto, en distintos soportes, tanto "automatizados" como "no automatizados", y son empleados para llevar a cabo distintas tareas. No obstante, podemos contemplarlos como una unidad, ya que todos ellos son de un tipo similar, pues se refieren a un mismo sistema objeto (los usuarios de los archivos) y a las mismas cuestiones (identificación, datos de contacto...) –y, por tanto, tienen una "sensibilidad" homogénea que requerirá unas medidas de seguridad similares-. Del mismo modo, responden a una misma finalidad: llevar a cabo la función "gestión de usuarios de los archivos"²⁴². Por tanto, a efectos de la protección de datos, podríamos considerar todo este conjunto de datos (organizado, como vimos, a través de diversos sistemas) como un único fichero de datos²⁴³. Es más, podrían considerarse como un único fichero todos los conjuntos de datos de esta clase que se empleen en archivos dependientes de un mismo centro directivo u órgano que actúe como responsable del fichero o del tratamiento. Así lo entiende la Orden CUL/2211/2009, de 22 de junio, por la que se regulan los ficheros de datos de carácter personal del Ministerio de Cultura y sus organismos públicos (BOE nº 193, de 11 de agosto), que crea un único fichero –denominado "Gestión General de Archivos Estatales"– destinado a

²⁴¹ Bien en sistema con ese único propósito, bien como un módulo en sistemas integrales para la administración del archivo.

²⁴² De acuerdo con el *Diccionario de Archivística* de Cruz Mundet (2011, p. 192), "[á]mbito de la gestión archivística que se ocupa del análisis de las necesidades, de la prestación de servicios y del control de las actividades de los usuarios de los archivos".

²⁴³ Véase en este sentido, por ejemplo, el art. 56.2 Reglamento: *Cuando los datos de carácter personal objeto de un tratamiento estén almacenados en diferentes soportes, automatizados y no automatizados o exista una copia en soporte no automatizado de un fichero automatizado sólo será precisa una sola notificación, referida a dicho fichero.*

controlar la gestión de usuarios de todos los centros y servicios archivísticos gestionados por dicho Ministerio²⁴⁴, bajo la responsabilidad de la Dirección General del Libro, Archivos y Bibliotecas. Sus características, de acuerdo con el anexo incluido en dicha disposición, son las siguientes:

- A) *Finalidad del fichero y los usos previstos para el mismo*: Registro y control de las personas que acceden a los fondos de los Archivos Estatales [...], del Archivo Central del Ministerio de Cultura y del servicio de Reproducción de Documentos. Registro de usuarios del servicio Agenda del Portal de los Archivos (PARES)
- B) *Personas o colectivos sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos*: Personas físicas que acceden a los fondos documentales de los Archivos Estatales, Archivo Central del Ministerio de Cultura. Usuarios de los servicios de Reproducción de documentos [sic] y del servicio Agenda del Portal de Archivos (PARES).
- C) *Procedimiento de recogida de datos de carácter personal*: Declaración voluntaria del interesado o su representante a través de formularios.
- D) *Estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo*: Datos de carácter identificativo: nombre y apellidos, NIF/DNI, dirección (postal/electrónica), teléfono (móvil/fijo) y firma. Temas de investigación. Historial de fondos consultados.
- E) *Cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros*: No se prevén comunicaciones o cesiones de datos de carácter personal.
- F) *Órganos de las Administraciones responsables del fichero*: Dirección General del Libro, Archivos y Bibliotecas.
- G) *Servicios o Unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición*: Subdirección General de Archivos Estatales. Dirección General del Libro, Archivos y Bibliotecas. Ministerio de Cultura. Plaza del Rey n.º 1, 28004 Madrid.
- H) *Medidas de seguridad con indicación del nivel básico, medio o alto exigible*: Básico.
- I) *Sistema de tratamiento utilizado*: Automatizado/no automatizado.

Sobre esta descripción podemos detectar que son necesarias unas pequeñas correcciones al respecto de la finalidad y usos previstos del fichero (apartado A), las personas de las que se obtienen los datos (B) y el procedimiento de recogida de datos (C): así, falta una referencia expresa

²⁴⁴ Archivo de la Corona de Aragón (Barcelona), Archivo General de Simancas (Simancas, Valladolid), Archivo General de Indias (Sevilla), Archivo Histórico Nacional (Madrid), Archivo General de la Administración (Alcalá de Henares, Madrid), Archivo de la Real Chancillería de Valladolid (Valladolid), Archivo Histórico Provincial de Álava (Vitoria-Gasteiz), Archivo Histórico Provincial de Guipúzcoa (Oñati, Guipúzcoa), Archivo Histórico Provincial de Vizcaya (Bilbao), Archivo Central del Ministerio de Cultura (Madrid), Centro de Información Documental de Archivos (Alcalá de Henares, Madrid) y Servicio de Reproducción de Documentos (Madrid)

al registro y control de los usuarios de servicios de información documental (servicios de referencia) y reproducción de documentos (servicios de reprografía), tanto de forma presencial como, sobre todo, de forma no presencial²⁴⁵. En este sentido hemos de señalar que la recogida de datos no se realiza tan sólo a partir de formularios web: cuando se reciben solicitudes de información documental o de reproducción de documentos por correspondencia (correo postal, correo electrónico, fax), los datos son tomados de las propias comunicaciones de los usuarios²⁴⁶. Por último, no se indica el posible uso posterior de los datos con fines estadísticos.

A pesar de ello, creemos que la recogida de estos datos y los tratamientos posteriores que pudieran realizarse para los usos descritos se ajustan a los principios de la protección de datos:

- Principio de calidad: los datos, recogidos de forma ética, son adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades para las que se obtienen; son exactos –en la medida en que son manifestados directamente por los usuarios- y se van actualizando conforme se requiere, permitiéndose además el derecho de rectificación (art. 4 LOPD).
- Principio de consentimiento: los archivos de la AGE se pueden considerar eximidos del requerimiento del consentimiento del interesado, ya que los datos se recogen en el marco de una relación administrativa de la que es parte el afectado, y para la que son necesarios dichos datos (art. 10.3.b Reglamento).
- Principio de finalidad: los datos se recogen y tratan para unas finalidades determinadas, explícitas y legítimas, no siendo utilizados para otras finalidades incompatibles con aquellas para las que fueron

²⁴⁵ No nos referimos tanto a las consultas telefónicas (52.320 en 2009), en las que la respuesta suele ser inmediata y no se recogen datos de carácter personal, sino a las que se realizan por correo postal, fax, correo electrónico y formularios web (formularios de contacto presentes en los apartados respectivos a cada centro dentro del sitio web del Ministerio de Cultura <http://www.mcu.es>, que son gestionados a través de un software para la administración de la relación con los clientes o CRM).

²⁴⁶ Ya que requieren una contestación y, por tanto, disponer al menos de unos datos personales y de contacto mínimos.

recogidos (arts. 4.1 y 4.2 LOPD). No se considera incompatible el uso posterior de los datos con fines estadísticos (art. 9.1 Reglamento), ya que se encuentra amparado en la Ley 12/1989, de 9 de mayo, Reguladora de la Función Estadística Pública, al estar previstas las estadísticas estatales sobre archivos en los distintos Planes Estadísticos Anuales²⁴⁷.

El cumplimiento de estos principios no exime, por otro lado, del deber de informar al afectado²⁴⁸. Éste se realiza mediante unas cláusulas al respecto incorporadas en el formulario para apertura de expediente de usuario (presencial) y en los formularios web del servicio Agenda de PARES²⁴⁹ y en el sitio web de cada centro (dentro del sitio general del Ministerio)²⁵⁰, en

²⁴⁷ Concretamente, el Plan Estadístico para el año 2011 atribuye al Ministerio de Cultura, a través de la Subdirección General de los Archivos Estatales –con número de programa 5275 y código 50003 del Inventario de Operaciones Estadísticas–, la realización de esta serie de trabajos. Véase a este respecto el Real Decreto 1708/2010, de 17 de diciembre, por el que se aprueba el Programa anual 2011 del Plan Estadístico Nacional 2009-2012 (BOE nº 312, de 24 de diciembre).

²⁴⁸ De la existencia de un fichero o tratamiento de datos de carácter personal, la finalidad de la recogida de éstos y los destinatarios de la información; de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; y de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante (art. 5.1 LOPD).

²⁴⁹ El servicio Agenda del Portal de ARchivos ESpañoles (PARES) <<http://pares.mcu.es/>>, que permite almacenar y organizar resultados de búsquedas en este sistema de descripción, incluye la siguiente cláusula: *A los efectos previstos en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre (B.O.E. del 14-12-1999), de Protección de Datos de Carácter Personal, se le informa que los datos consignados en el presente modelo serán incorporados a un fichero del que es titular el Ministerio de Cultura. Sus datos serán empleados solamente para registrarse en la Agenda Pares y no serán cedidos ni usados para otro fin diferente. Respecto de los citados datos podrá ejercitar los derechos de acceso, rectificación y cancelación, en los términos previstos en la indicada Ley Orgánica 15/1999 ante la Subdirección General de Archivos Estatales, Dirección General del Libro, Archivos y Bibliotecas del Ministerio de Cultura (Plaza del Rey, 1, 28071 Madrid).* No se incluye, como vemos, la mención a un posible fin estadístico de los datos.

²⁵⁰ Las consultas recibidas por este medio son gestionadas, como se indicó en nota 245, mediante un software para la administración de la relación con los clientes o CRM. La cláusula, muy similar a la anterior –incluso en la no mención de la finalidad estadística–, es la siguiente: *A los efectos previstos en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre (B.O.E. del 14-12-1999), de Protección de Datos de Carácter Personal, se le informa que los datos consignados en el presente modelo serán incorporados a un fichero del que es titular el Ministerio de Cultura. Sus datos serán empleados solamente para atender su solicitud/queja/reclamación sobre/del Área a la que se dirige y no serán cedidos ni usados para otro fin diferente. Respecto de los citados datos podrá ejercitar los derechos de acceso, rectificación y cancelación, en los términos previstos en la indicada Ley Orgánica 15/1999 ante el Ministerio de Cultura, Secretaría General Técnica (Plaza del Rey, 1, 28071 Madrid).* En este caso, se indica que el órgano ante el que habrá que se pueden ejercitar los derechos de acceso, rectificación y cancelación será la Secretaría General Técnica, lo que parece indicar que los datos recabados de esta manera se conciben en el marco de un fichero distinto a este “Gestión General de Archivos Estatales” que estamos analizando. No obstante, consultados en la mencionada Orden CUL/2211/2009, de 22 de junio los distintos ficheros de datos que son responsabilidad de dicha Secretaría General Técnica, no queda muy claro a qué otro fichero podrían incorporarse estos datos (¿“Servicio de Información al Ciudadano”, “Quejas y Sugerencias?”). Sería necesaria, por tanto, una revisión del proceso de recogida de datos por este medio.

buena medida mejorables. No tenemos constancia de que se informe a los usuarios por correspondencia, por lo que vemos necesaria la inserción de unas cláusulas similares en los modelos de respuesta que se envíen al interesado.

Por último, y tras examinar el formulario de recogida de datos para la apertura del expediente de usuario presencial ("Datos para la apertura del expediente de usuario", véase el Anexo 1), creemos oportuno recomendar una serie de correcciones al mismo:

- La cláusula informativa de protección de datos²⁵¹ no expresa de forma clara y precisa cuál es la finalidad y usos previstos del fichero al que se incorporan los datos, ya que indica, primero, que los datos "son necesarios para garantizar el control y la seguridad de la documentación" pero que "se utilizan exclusivamente con fines estadísticos", para luego señalar que la finalidad del fichero es "facilitar la gestión administrativa del Archivo". Recomendamos, por tanto, modificar esta cláusula, advirtiendo expresamente que la finalidad y usos previstos del fichero serán los de controlar y garantizar la seguridad de los documentos; facilitar la gestión administrativa del Archivo; y proporcionar datos estadísticos sobre el servicio²⁵². Así mismo, habría de modificarse el apartado referente a la unidad ante la que pueden ejercitarse los derechos de acceso, rectificación, cancelación y oposición, sustituyendo la referencia "a la Dirección del Archivo o, en su caso, al Departamento de Referencias", por los datos de la Subdirección General de Archivos Estatales, tal y como aparece en la disposición de creación del fichero. De esta forma, se cumpliría con el principio de consentimiento, dándose cuenta de forma precisa e

²⁵¹ *Los datos de carácter personal consignados en la presente solicitud son necesarios para garantizar el control y la seguridad de la documentación y se utilizan exclusivamente con fines estadísticos.*

El firmante autoriza su inclusión en los ficheros automatizados cuya finalidad consiste en facilitar la gestión administrativa del Archivo. No obstante, el afectado podrá expresar su oposición por escrito en cualquier momento. El interesado tiene derecho a acceder a sus datos personales obrantes en los ficheros automatizados y a solicitar su rectificación o cancelación cuando los datos sean erróneos, según lo dispuesto en la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y demás disposiciones vigentes en la materia. A este efecto se dirigirán a la Dirección del Archivo o, en su caso, al Departamento de Referencias.

²⁵² Este mismo texto podría emplearse en la disposición creadora del fichero (apartado sobre finalidad y usos previstos).

inequívoca del derecho de las personas a ser informadas sobre el fichero y el tratamiento de datos al que van destinados (art. 5 LOPD).

- Por otro lado, creemos que sería conveniente incluir la variable "sexo" entre los datos personales a recoger en el formulario²⁵³. El artículo 20.a de la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres (BOE nº 71, de 23 de marzo), establece que al objeto de hacer efectivas las disposiciones contenidas en la Ley y garantizar la integración de la perspectiva de género en su actividad ordinaria, los poderes públicos deberán incluir sistemáticamente la variable de sexo en las estadísticas, encuestas y recogida de datos que lleven a cabo. De manera que, de conformidad con la LOPD, recoger dicho dato sería adecuado, pertinente y no excesivo, y facilitaría además el cumplimiento por parte de los archivos de dicha Ley Orgánica 3/2007.

3.2.2. Los sistemas descripción archivística como ficheros de datos

El segundo de los casos representativos sobre recogida, grabación, elaboración y modificación de datos personales en los archivos es, como ya hemos adelantado anteriormente, el referido a la elaboración de sistemas de descripción que contengan información personal. Para el caso que nos ocupa, entendemos el término "sistemas de descripción archivística" en sentido amplio, como cualquier sistema específico de información –elaborado tanto por archiveros como por gestores²⁵⁴- que recoja representaciones de documentos de archivo y, en su caso, de otras entidades archivísticas (agentes, funciones, etc). Nos referimos tanto a los tradicionales instrumentos de descripción en papel (singularmente inventarios, catálogos e índices) o automatizados (generalmente bases de datos, que pueden corresponderse con instrumentos de descripción tradicionales o contar con estructuras de datos más libres), como a sistemas web de descripción archivística como el ya mencionado PARES;

²⁵³ Señalamos esta cuestión ante las dudas de algunos archiveros sobre la "legalidad" de recoger este dato. Dato que, por otro lado, entendemos que no es "sensible", ya que no se pregunta sobre la tendencia o prácticas sexuales, sino únicamente si se es hombre o mujer.

²⁵⁴ Aunque nos centraremos en todo aquello que se refiere especialmente a los primeros.

así como a los módulos de descripción de los sistemas electrónicos de gestión de documentos y archivos.

No son muchos los sistemas de descripción de los archivos de la Administración General del Estado que han sido declarados como ficheros de datos ante la AEPD –y, por tanto, creados, como establece la normativa vigente, mediante disposición general publicada en el BOE-: destacan los del sistema archivístico del Ministerio del Interior²⁵⁵ -como INSTRUMENTA²⁵⁶, del Archivo General del Ministerio (su responsable es la Secretaría General Técnica) y ARCHIVO, del Cuerpo de Nacional de Policía-, aunque también ha sido declarado el fichero del Archivo Central del Ministerio de Política Territorial²⁵⁷ (cuyo responsable es también la Secretaria General Técnica de dicho Ministerio); y únicamente uno por parte del Ministerio de Cultura, denominado “Guerra Civil y Franquismo”, del que trataremos más adelante, cuando abordemos las cuestiones referidas a la cesión o comunicación de datos.

En el caso de los sistemas de descripción archivística resulta obviamente más complejo el cumplimiento del principio de consentimiento, ya que su puesta en práctica sería inviable. Habría que valorar, por tanto, la concurrencia de alguna de las excepciones al consentimiento que contempla la normativa (art. 6 LOPD y art. 10 Reglamento). En concreto, para el caso que nos ocupa, podría aducirse que los datos de carácter personal son recogidos para el ejercicio de funciones propias de las administraciones públicas en el ámbito de las competencias que les atribuye una norma con rango de ley (art. 10.3.a Reglamento)²⁵⁸. En este

²⁵⁵ Orden INT/1202/2011, de 4 de mayo, por la que se regulan los ficheros de datos de carácter personal del Ministerio del Interior (BOE nº 114, de 13 de mayo).

²⁵⁶ Al que se otorga un nivel de seguridad alto, con las implicaciones que ello conlleva (véase el capítulo 2.5).

²⁵⁷ Orden TER/2232/2010, de 29 de julio, por la que se regulan los ficheros de datos de carácter personal del Ministerio de Política Territorial (BOE nº 197, de 14 de agosto).

²⁵⁸ En ningún caso podría invocarse la excepción prevista en el art. 10.2.b Reglamento, de que *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, siempre que no se vulneren los derechos y libertades fundamentales del interesado*. El Reglamento (art. 7) ha venido a establecer una lista cerrada de lo que se considera a efectos de la normativa “fuentes accesibles al público”, y entre ellas no se encuentran los documentos obrantes en archivos públicos, sino el censo promocional; las guías de servicios de comunicaciones electrónicas; las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección

sentido podría invocarse –con fundamento en el artículo 44 CE- lo establecido el artículo 60.3 de la Ley 16/1985, de Patrimonio Histórico Español, que señala que los organismos competentes para la ejecución de esta Ley velarán por la elaboración y actualización de los catálogos, censos y ficheros de los fondos de los archivos estatales. Pero, también, lo dispuesto en el art. 37.9 de la Ley 30/1992, según el cual serán objeto de periódica publicación la relación de los documentos obrantes en poder de las Administraciones Públicas que puedan ser objeto de consulta por los particulares²⁵⁹.

A pesar de que estos preceptos legales puedan considerarse imprecisos, creemos que debe primar en este sentido el principio de proporcionalidad, ya que de otra manera no podrían incluirse en nuestros sistemas de descripción ningún tipo de datos referidos a personas vivas, por nimios e inofensivos que sean, impidiendo de esta manera la correcta identificación, gestión, localización y explicación de los documentos de archivo, así como de su contexto y del sistema que los ha producido. Ahora bien, habría que determinar si esta finalidad –diferente a aquella para la que fueron recogidos originalmente los datos- es compatible a efectos de la legislación de protección de datos²⁶⁰. En el caso de los archivos de la AGE, dado que la finalidad última del tratamiento que se pretende dar es facilitar la gestión y consulta de los documentos, regulada en el artículo 57 de la LPHE –norma citada expresamente en el art. 9.1 del Reglamento como habilitadora para determinar la compatibilidad de fines distintos a los originales- creemos que se cumpliría con el principio de finalidad.

Por último, habría que tener en cuenta el principio de calidad de los datos: al hilo de la proporcionalidad que invocábamos arriba, la Ley exige (art.

profesional e indicación de su pertenencia al grupo; los diarios y boletines oficiales; y los medios de comunicación social.

²⁵⁹ Se conecta así, de alguna manera, la legitimidad para tratar los datos con el derecho de acceso a los documentos. De ello trataremos más profundamente cuando analicemos la comunicación de datos.

²⁶⁰ Como ya hemos tenido oportunidad de indicar, la LOPD (art. 4.2) establece que no se considerará incompatible el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. El Reglamento (art. 9.1) establece que para la determinación de estos fines se estará a la legislación que en cada caso resulte aplicable y, en particular, a lo dispuesto en la Ley 12/1989, de 9 de mayo, Reguladora de la Función Estadística Pública, la Ley 16/1985, de 25 junio, del Patrimonio Histórico Español y la Ley 13/1986, de 14 de abril de Fomento y Coordinación General de la Investigación Científica y Técnica (en la actualidad, Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación), y sus respectivas disposiciones de desarrollo, así como a la normativa autonómica en estas materias.

4.1 LOPD) que los datos de carácter personal sólo se podrán recoger y someter a 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. Por ello, no cabrían descripciones demasiado prolijas en cuanto a informaciones de las personas afectadas, sobre todo en aquellos aspectos que pudieran afectar a su intimidad²⁶¹.

3.2.3. Algunas consideraciones sobre la importancia de los sistemas de descripción archivística desde la perspectiva de la protección de datos

Para concluir este apartado, hemos de llamar la atención sobre cómo -de acuerdo con lo visto hasta ahora- la conexión de los sistemas de descripción con el contexto archivístico del que proceden los datos puede suponer la entrada de determinadas series excluidas en principio -según el criterio totalizador que venimos defendiendo- del régimen de la protección de datos, en su ámbito de actuación. Por ejemplo: una serie de expedientes en papel referidas a la concesión de determinado tipo de licencias a personas, que están ordenadas por número de expediente y año, estaría excluida del ámbito de aplicación de la LOPD. La creación por parte de la unidad administrativa encargada de tramitar el procedimiento en cuestión -o por el archivo central, una vez ha ingresado esa documentación en el mismo- de un fichero o de una base de datos que permita recuperar los expedientes por criterios onomásticos; o la incorporación de información referencial de los expedientes a la aplicación informática empleada al efecto para gestionar la toma de decisiones (la concesión de las licencias, en este caso) -aunque la constancia documental del procedimiento se realice íntegramente en papel-, haría caer sobre la serie documental correspondiente el peso de la normativa de protección de datos.

²⁶¹ Lo cual, por otro lado, tampoco suele ser pertinente a efectos archivísticos. Por ejemplo, en una serie de ayudas a personas con discapacidad, incluir en la descripción de cada expediente detalles de la discapacidad de cada interesado.

Éste sería también el caso de los expedientes instruidos al amparo de las Leyes de Vagos y Maleantes y de Peligrosidad y Rehabilitación Social, únicas series específicas de documentos de archivo mencionadas expresamente en la normativa de protección de datos. Dichas series²⁶², conservadas en buena parte en centros del sistema archivístico de la Administración General del Estado²⁶³, están compuestas por expedientes en papel ordenados –como generalmente sucede con los expedientes judiciales– por criterios numéricos, no alfabéticos. Creemos –en consonancia con nuestro criterio– que son los instrumentos empleados para su gestión (en principio, los ficheros e inventarios que se crearon en los propios juzgados, pero también los sistemas de descripción creados por los archivos que finalmente custodian estos expedientes) los que permiten recuperarlos por criterios onomásticos y, por tanto, los introducen en la categoría de ficheros de datos y, en definitiva, en la órbita de la normativa de protección de datos de carácter personal.

Como vemos, las implicaciones que supone la relación entre documentos, sistemas de información para la gestión, sistemas de descripción archivística y sistemas electrónicos de gestión de documentos, con el concepto de fichero, pueden llegar a ser especialmente importantes, ya que supondrían la obligación de registrar nuevos ficheros de datos y adaptar su tratamiento a la legislación en esta materia.

²⁶² Como ha señalado Casado (2009, p. 68) al respecto de las custodiadas en el ámbito del Ministerio del Interior, “es necesario una completa identificación de las mismas en los fondos actualmente conservados” para poder atender el régimen específico que otorga a las mismas la LOPD.

²⁶³ Nos referimos, para el caso que nos ocupa, a los expedientes judiciales: son cinco los archivos históricos provinciales que cuentan entre sus fondos con este tipo de series (Laso 2009, pp. 58-59), además del AGA, para el ámbito territorial de Madrid. Otras series, de carácter administrativo, se conservan en los subsistemas departamentales de Interior (véase en este sentido Casado 2009) y Justicia, que han transferido ya algunas fracciones al AGA de las mismas.

3.3. ¿Conservación a largo plazo de los datos o cancelación?

La normativa de protección de datos de carácter personal establece la obligación de garantizar unas condiciones de conservación que permitan el ejercicio del derecho de acceso y unas medidas de seguridad adecuadas (arts. 4.6 y 9 LOPD). Pero, por lo general, esa conservación parece tener "fecha de caducidad", ya que tarde o temprano se exige su cancelación y, por tanto, su supresión. Hemos de preguntarnos, por tanto, si existe la posibilidad de conservar a largo plazo los datos (entendiendo como tal un plazo superior al de su uso para los fines que fueron recogidos), principalmente por lo que pudiera suponer con respecto de aquellos contenidos en documentos integrantes de ficheros de datos. Y, sobre todo, teniendo en cuenta que dichos documentos -en nuestro ámbito de análisis (el sistema archivístico de la AGE)- forman parte del patrimonio documental y, por tanto, están sujetos a un régimen específico en lo que se refiere a su eliminación.

3.3.1. Conservación a largo plazo: una excepción controlada por la AEPD

Como vimos anteriormente, la cancelación de los datos personales se puede producir a través de dos vías:

- A "instancia de parte", como resultado del ejercicio, por parte del afectado, de su derecho al respecto²⁶⁴, cuando su tratamiento no se

²⁶⁴ Véanse los artículos 4.5 y 16 de la LOPD; y 8.6, 31, 32 y 33 del Reglamento.

El ejercicio de este derecho podrá denegarse en los supuestos en que así lo prevea una ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al

ajuste a lo dispuesto en la normativa y, en particular, cuando los datos sean inexactos o incompletos. En este caso, la cancelación se realizaría una vez transcurridos los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

- En cualquier caso, "de oficio", una vez que los datos han dejado de ser necesarios o pertinentes para la finalidad para la que fueron recabados o registrados. En este caso también se prevé que puedan ser conservados durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado.

En ambos supuestos, la supresión definitiva de los datos no ha de realizarse hasta que prescriban las posibles responsabilidades administrativas y judiciales nacidas del tratamiento. Hasta ese momento, los datos se mantendrán bloqueados –esto es, reservados únicamente para atender dichas responsabilidades ante la Administración²⁶⁵ o los órganos judiciales-, sin que puedan someterse a ningún tipo de tratamiento. Cumplido este plazo de bloqueo -utilizando una terminología archivística, cuando prescriban los valores primarios de los documentos que los contienen- deberá procederse a la supresión de los datos, de forma que no se pueda acceder nunca más a los mismos²⁶⁶.

Únicamente se prevén dos vías a través de las cuales podrían conservarse datos a largo plazo:

- Previa disociación definitiva de los mismos (art. 8.6 Reglamento), esto es, de forma que no se pueda identificar al interesado. Esto implicaría

responsable del tratamiento revelar a los afectados el tratamiento de los datos sobre los que se quiere ejercer dicho derecho.

²⁶⁵ Por ejemplo, las infracciones previstas en la LOPD prescriben como máximo a los tres años (a contar desde el día en que la infracción se hubiera cometido). Entendemos, por tanto, que el período de bloqueo no puede ser inferior a dicho plazo.

²⁶⁶ El Reglamento establece, en este sentido, que la destrucción o borrado de cualquier documento o soporte que contenga datos de carácter personal deberá realizarse mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior (art. 92.4 Reglamento).

alterar la integridad de los documentos²⁶⁷ y, por tanto, entraría en conflicto con la obligación general de conservar los bienes del patrimonio documental que impone la Ley 16/1985, de 25 junio, del Patrimonio Histórico Español (LPHE) en su artículo 52.

- Con carácter excepcional, el art. 9.2 del Reglamento permite el mantenimiento íntegro de determinados datos con valor histórico, estadístico o científico (de acuerdo con la legislación específica²⁶⁸), mediante un procedimiento específico regulado en la Sección Segunda, Capítulo VII, Título IX del mismo (arts. 157 y 158). Dicho procedimiento otorga en último término a las agencias de protección de datos la potestad de autorizar, a solicitud del responsable del tratamiento, la conservación a largo plazo de los documentos afectados por esta normativa²⁶⁹.

SECCIÓN 2ª. Procedimiento para la autorización de conservación de datos para fines históricos, estadísticos o científicos

Artículo 157. Iniciación del procedimiento

1. El procedimiento para obtener de la Agencia Española de Protección de Datos la declaración de la concurrencia en un determinado tratamiento de datos de valores históricos, científicos o estadísticos, a los efectos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento, se iniciará siempre a petición del responsable que pretenda obtener la declaración.

2. En el escrito de solicitud, el responsable deberá:

- a) Identificar claramente el tratamiento de datos al que pretende aplicarse la excepción.
- b) Motivar expresamente las causas que justificarían la declaración.
- c) Exponer detalladamente las medidas que el responsable del fichero se propone implantar para garantizar el derecho de los ciudadanos.

²⁶⁷ Amén de lo costoso que podría resultar llevarlo a cabo, sobre todo, en series voluminosas (tanto en cantidad de expedientes, como en número de documentos por expediente) en soporte papel- para la unidad administrativa en cuestión, siendo preferible en estos casos la eliminación.

²⁶⁸ El Reglamento remite en particular a las Leyes 12/1989, de 9 de mayo, Reguladora de la Función Estadística Pública; 16/1985, de 25 junio, del Patrimonio Histórico Español; y 13/1986, de 14 de abril, de Fomento y Coordinación General de la Investigación Científica y Técnica; así como a sus respectivas disposiciones de desarrollo y a la normativa autonómica en estas materias.

²⁶⁹ Ya que la otra alternativa implicaría alterar de forma significativa la integridad de los documentos, lo que equivaldría prácticamente a una eliminación.

3. La solicitud deberá acompañarse de cuantos documentos o pruebas sean necesarios para justificar la existencia de los valores históricos, científicos o estadísticos que fundamentarían la declaración de la Agencia.

Artículo 158. Duración del procedimiento y efectos de la falta de resolución expresa

1. El plazo máximo para dictar y notificar resolución en el procedimiento será de tres meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud del responsable del fichero.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su solicitud.

Esta previsión, recogida únicamente –como vemos– en una norma de rango reglamentario, contrasta con el régimen previsto para el patrimonio documental por la Ley 16/1985, de 25 junio, del Patrimonio Histórico Español (LPHE).

De acuerdo con esta Ley, todos los poseedores de bienes del patrimonio documental están obligados, con carácter general, a conservarlos y protegerlos (art. 52.1 LPHE). No obstante, se prevé la posible eliminación de bienes del patrimonio documental de titularidad pública, que deberá ser autorizada por la Administración competente (art. 55 LPHE). El órgano concreto al que le corresponde conceder dicha autorización, así como el procedimiento destinado al efecto, han sido establecidos en el Real Decreto 1164/2002, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y la conservación de documentos administrativos en soporte distinto al original (BOE nº 274, de 15 de noviembre). De conformidad con el mismo, la competencia para resolver la autorización de eliminación corresponde al Subsecretario del Ministerio o al Presidente o Director del Organismo público en el que se encuentren custodiados los documentos, previo dictamen²⁷⁰, en cualquier caso, de la Comisión Superior Calificadora de Documentos Administrativos (CSCDA)²⁷¹

²⁷⁰ Que tendrá carácter vinculante en caso ser contrario a la eliminación (art. 5.2 del Real Decreto 1164/2002).

²⁷¹ Creada, como vimos anteriormente, por la LPHE (art. 58) para el estudio y dictamen de las cuestiones relativas a la calificación y utilización de los documentos de la Administración del Estado y del sector público estatal, así como su integración en los archivos y el régimen de acceso e inutilidad administrativa. Su composición, funcionamiento y competencias

-en la que casualmente hay un representante de la Agencia Española de Protección de Datos²⁷²-.

El Legislador no ha previsto, por tanto, la contradicción entre el mandato de la LPHE de conservar los documentos²⁷³ y la obligación de la LOPD de suprimir los datos personales contenidos en los mismos -lo que equivaldría, como ya dijimos, a eliminar dichos documentos-. Ni siquiera en el momento en que introdujo una posibilidad de excepción a esta última obligación²⁷⁴ a través del Reglamento de 2007²⁷⁵. A ello hemos de añadir que, incomprensiblemente, la disposición adicional sexta del mencionado Real Decreto 1164/2002 establece que la regulación contenida en el mismo "debe entenderse sin perjuicio de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal". Por el contrario, la normativa de protección de datos no incluye ninguna previsión sobre el régimen específico de los bienes integrantes del patrimonio documental. Y, lo que es más, erige a la Agencia Española de Protección de Datos, a través del procedimiento indicado anteriormente, en principal intérprete de los valores históricos, científicos y estadísticos de los datos.

A la vista de todo ello tenemos nuestras dudas sobre la posibilidad actual de conservar íntegramente y a largo plazo -incluso de que ingresen, mediante transferencia, en un centro de archivo- los documentos de series afectadas por la normativa de protección de datos. Por el contrario, tendrán que eliminarse (o modificarse sustancial y permanentemente, lo que equivaldría igualmente a su destrucción) con las garantías que establece la LOPD a favor de los afectados, eso sí, pero sin las previstas en

específicas fueron establecidas por vía reglamentaria a través del Real Decreto 139/2000, de 4 de febrero y, posteriormente, del Real Decreto 1401/2007, de 29 de octubre (BOE nº 267, de 7 de noviembre), que derogó al anterior.

²⁷² El citado Real Decreto 1401/2007 (véase la nota anterior) incluye entre los vocales de la CSCDA a un representante de la AEPD designado por su Director (art. 2.1).

²⁷³ En particular, los de cualquier época generados, conservados o reunidos en el ejercicio de su función por cualquier organismo o entidad de carácter público, por las personas jurídicas en cuyo capital participe mayoritariamente el Estado u otras entidades públicas y por las personas privadas, físicas o jurídicas, gestoras de servicios públicos en lo relacionado con la gestión de dichos servicios (art. 49.2 LPHE).

²⁷⁴ Lo cual ha sido visto como un defecto de técnica legislativa, al no estar prevista dicha posibilidad en la LOPD.

²⁷⁵ Sobre el proyecto de este Reglamento tuvo que informar -de conformidad con el art. 37.1.h LOPD- la AEPD, conocedora de esta contradicción al estar representada en la CSCDA.

el procedimiento de eliminación de bienes del patrimonio documental, a favor de nuestra memoria colectiva y, por tanto, del interés general.

3.3.2. Implicaciones de la cancelación de datos sobre el patrimonio documental: el caso de los ficheros de la Dirección General de Instituciones Penitenciarias

Un ejemplo significativo al respecto de lo que venimos tratando lo ofrece el caso de las series de "Expedientes personales de internos" producidas por los centros penitenciarios²⁷⁶. Existen diversas resoluciones de la AEPD a procedimientos de tutela de derechos²⁷⁷ iniciados a instancia de varios ciudadanos, con motivo de la denegación por parte de la Dirección General de Instituciones Penitenciarias (Ministerio del Interior) del ejercicio de su derecho de cancelación con respecto a los datos personales que de los mismos se contienen en varios ficheros de dicho órgano:

- Series de *Expedientes personales de internos*, en soporte papel (fichero no automatizado), obrantes en los archivos de gestión de los centros penitenciarios; fueron calificadas de conservación permanente por Acuerdo de 20/11/2002 de la Comisión Calificadora de Documentos Administrativos del Ministerio del Interior, que establece un plazo de retención de 52 años, tras el cual deberán transferirse al Archivo Histórico Provincial correspondiente²⁷⁸.
- Base de datos *Sistema de Información Penitenciaria (SIP-Internos)*, en soporte electrónico (fichero automatizado inscrito en el Registro General de Protección de Datos), que registra de forma centralizada en la Dirección General los datos esenciales de los expedientes de las series anteriores. Se trata de información anteriormente recogida en

²⁷⁶ Al menos en lo que se refiere a los expedientes de personas que únicamente estuvieron en prisión preventiva.

²⁷⁷ Por ejemplo, las Resoluciones R/00108/2005 (procedimiento TD/00389/2004), R/00357/2005 (procedimiento TD/00020/2005), R/00494/2005 (procedimiento TD/00151/2005), R/00666/2007 (procedimiento TD/00251/2007), R/00319/2008 (procedimiento TD/00785/2007).

²⁷⁸ Laso (2009, p. 108) ha señalado que son 16 los archivos históricos provinciales que conservan fondos documentales de prisiones provinciales.

diversos libros registro y ficheros manuales, muchos de los cuales se conservan aún en el Archivo General de la Administración²⁷⁹.

Los afectados alegaron que habían ingresado en prisión en su momento por orden de los respectivos juzgados de instrucción, con motivo de unas diligencias previas que finalmente derivaron en sentencias absolutorias. Uno de ellos, además, manifiesta que “instada por su parte la cancelación de antecedentes policiales relacionados con los mismos hechos objeto del presente procedimiento de tutela, los mismos fueron destruidos en su presencia según consta en Resolución del [...] del Archivo Central de la Policía”.

La AEPD resolvió en todos los casos, y en contra de lo alegado por la Dirección General, la cancelación de los datos de las personas afectadas, sin que dichas resoluciones fueran recurridas ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional.

En definitiva, la Dirección General de Instituciones Penitenciarias del Ministerio del Interior, ha justificado la negativa a cancelar los datos del reclamante en el Acuerdo de la Comisión de Clasificación de Documentos del Ministerio del Interior que, en virtud del valor histórico, estadístico, y las necesidades de gestión, calificó “de conservación permanente” tanto los expedientes personales de los internos en centros penitenciarios, como el fichero automatizado denominado “SIP-INTERNOS”. No puede admitirse tal habilitación legal por cuanto ambos ficheros recogen unos datos, que el caso del reclamante, son inexactos y no se encuentran actualizados, habida cuenta de que éste no se encuentra “interno” en ningún institución del sistema penitenciario. Tampoco puede admitirse como argumento para denegar la cancelación solicitada la referencia genérica a un “supuesto valor histórico o estadístico” que dichos datos pudieran llegar a alcanzar, y mucho menos las “necesidades de gestión” propias de la Administración Penitenciaria ya que el mantenimiento íntegro de datos con dichos fines tiene un carácter excepcional y reglamentariamente regulado por exigencia del artículo 4.5 de la LOPD.

En consecuencia no cabe admitir los motivos esgrimidos por la Dirección General de Instituciones Penitenciarias para denegar la cancelación de datos solicitada por el reclamante habida cuenta que no puede motivarse la falta de cancelación en su ausencia de regulación por parte del Reglamento Penitenciario, al tiempo que debe rechazarse que los datos del afectado continúen en un fichero en el que constan los datos personales de internos (o personas recluidas) en Instituciones Penitenciarias, ya que, en el caso del reclamante, son datos inexactos.

²⁷⁹ Principalmente la serie *Fichas de ingreso en prisión* (1938-1955), producida por la Sección de Tratamiento Penitenciario de la Dirección General de Prisiones.

Por último debe apuntarse que el vigente Código Penal establece en su artículo 136²⁸⁰ el derecho de los condenados a obtener del Ministerio de Justicia la cancelación de sus antecedentes penales una vez cumplidos determinados requisitos y plazos. En consecuencia y reconocido tal derecho respecto de los condenados, cabe atender el derecho a la cancelación de los datos del reclamante, tanto de su expediente personal como interno en el centro penitenciario del (...) en (...), como en el fichero denominado Sistema de Información Penitencia (SIP), habida cuenta de que en su caso, no se trata de un condenado por los Tribunales de Justicia, sino de un ciudadano que permaneció interno en un centro penitenciario, con carácter preventivo, siendo absuelto con todos los pronunciamientos favorables por parte del órgano judicial correspondiente.

En consecuencia procede la estimación de la tutela solicitada debiéndose llevar a cabo la cancelación y el consiguiente bloqueo de los datos personales del reclamante existentes en los ficheros a que se hace referencia en la presente resolución.

Creemos que en esta ocasión –al igual que en otras similares- se asiste a una confusión –tomando prestada la terminología diplomática- entre los efectos jurídicos de una determinada *actio* (los antecedentes), con el reflejo documental de dicha actio jurídica (su *conscriptio*). En nuestra opinión, el hecho de que un determinado documento refleje una circunstancia particular (por ejemplo, que una determinada persona ha estado en prisión en un determinado momento) no implica por sí mismo que tenga efectos sobre dicha persona u otras. Ni tampoco que la información de dicho documento tenga que ser automáticamente accesible a terceras personas o sistemas para la determinación o la aplicación de dichos efectos.

Por ejemplo, actualmente ninguna persona cuenta con antecedentes fundados en expedientes instruidos al amparo de las derogadas leyes de Vagos y Maleantes y de Peligrosidad y Rehabilitación Social, a pesar de que no han sido –afortunadamente- cancelados. Y eso que la LOPD no autoriza expresamente su conservación: el tratamiento especial que establece para ellos en su Disposición Adicional tercera garantiza la

²⁸⁰ Pensamos que la Agencia yerra al invocar el artículo 136 del Código Penal, referido a las inscripciones de antecedentes penales de personas que sí han sido condenadas –no como sucede en los casos de los reclamantes-, una vez satisfechas las responsabilidades civiles correspondientes y transcurridos determinados plazos sin que hubieran vuelto a delinquir. Quizás hubiera sido más conveniente que remitiera al artículo 137 de dicho Código, que establece que: *Las anotaciones de las medidas de seguridad impuestas conforme a lo dispuesto en este Código o en otras leyes penales serán canceladas una vez cumplida o prescrita la respectiva medida; mientras tanto, sólo figurarán en las certificaciones que el Registro expida con destino a Jueces o Tribunales o autoridades administrativas, en los casos establecidos por la Ley.*

protección de los datos personales de los afectados y su derecho a la intimidad hace innecesaria –por lo que podemos intuir- dicha cancelación²⁸¹.

Volviendo al caso que nos ocupa, la Agencia considera que no existe habilitación legal²⁸² para conservar los datos²⁸³ “por cuanto ambos ficheros recogen unos datos, que el caso del reclamante, son inexactos y no se encuentran actualizados, habida cuenta de que éste no se encuentra “interno” en ningún institución del sistema penitenciario”. Lo cual nos lleva a pensar que si el nombre y la función dadas al fichero *SIP-Internos* cuando se inscribió en el Registro, y a la serie documental en los instrumentos de control y descripción archivísticos se sustituye la referencia a los “internos” por “ciudadanos que en algún momento estuvieron internos” o cualquier otra alternativa que no sea inexacta o se encuentre desactualizada a juicio de la AEPD, existiría dicha habilitación legal y, por tanto, sí podría haberse denegado legítimamente el ejercicio del derecho de cancelación²⁸⁴. Aunque ello no haría sino “alargar la agonía” de unos documentos que, como hemos visto en el anterior apartado, tendrían irremediamente que ser destruidos tarde o temprano. ¿Quedaría en algún caso, a juicio de la Agencia, constancia documental de que, siquiera durante algunas horas, una persona determinada estuvo en prisión y, por tanto, bajo la responsabilidad del Estado?

²⁸¹ Circunstancia que, en el pasado, llevó a la destrucción –o casi- de algunos de estos expedientes (Ocaña 1999, p. 205), con indudable valor histórico y que, aún en la actualidad, sirven para reparar a las víctimas.

²⁸² Dado que el Reglamento de desarrollo de la LOPD establece que la cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables (art. 33.1); y que podrá además denegarse el derecho de cancelación en los supuestos en que así lo prevea una ley (art. 33.2).

²⁸³ No recuerda la Agencia –ni tampoco la Dirección General de Instituciones Penitenciarias en sus alegaciones- la obligación legal de conservar los bienes del patrimonio documental (art. 52 LPHE).

²⁸⁴ En ello nos reafirma la opinión mostrada por el Tribunal Supremo con respecto al caso de los Libros de Bautismo que fue analizado con anterioridad. Así, señala (STS de 19 de septiembre de 2008, fundamento de derecho 4º) que *en los Libros de Bautismo no cabe apreciar ninguna inexactitud de datos, en cuanto en los mismos se recoge un dato histórico cierto, salvo que se acredite la falsedad, cual es el referente al bautismo de una persona y cuando ésta solicita la cancelación de ese hecho, no está pretendiendo que se corrija una inexactitud en cuanto al mismo, sino que en definitiva está intentando y solicitando un sistema nuevo y diferente de registro de nuevos datos personales*. En el caso que nos ocupa, la estancia en prisión sería “un dato histórico cierto, salvo que se acredite la falsedad” y, por tanto, no inexacto.

He aquí la paradoja. Para la normativa sobre archivos y patrimonio documental, los documentos son de conservación permanente hasta que no se demuestre lo contrario. Por el contrario, para la normativa de protección de datos, todos los documentos, en tanto soporte de datos de carácter personal, son eliminables mientras no se demuestre –en casos excepcionales y ante la Agencia correspondiente- lo contrario²⁸⁵. Urge, por tanto, una conexión entre el régimen de la protección datos y el del patrimonio documental que evite este tipo de desencuentros y, lo que es más grave, la pérdida de buena parte de nuestra memoria colectiva.

3.3.3. La destrucción incontrolada de documentos: buena práctica para la AEPD

Esta desconexión entre ambos regímenes hace que la Agencia Española de Protección de Datos²⁸⁶ muestre en ocasiones una importante falta de sensibilidad con respecto al patrimonio documental. Así, queremos llamar la atención sobre un caso paradigmático. En diciembre de 2004, la Agencia Española de Protección de Datos publicó unas Recomendaciones al Instituto Nacional de Administración Pública²⁸⁷ como resultado de una inspección de oficio que incluyen un apartado (5.8) referido a su Archivo y al tratamiento archivístico de los documentos producidos por este organismo, que reproducimos íntegramente a continuación:

En los Servicios Centrales del I.N.A.P. se dispone de un Archivo Central en el que se custodia la documentación utilizada en la gestión de las actividades formativas incluida la correspondiente a los procesos y cursos selectivos. Dicho archivo ha sido creado hace unos doce años y contiene documentación desde el año 1944 procedente del desaparecido Instituto de Estudios de Administración Local.

²⁸⁵ Recordemos, no obstante, que estas disposiciones –al igual que el resto de la normativa de protección de datos- sólo afectarían (si aceptamos el criterio “totalizador” que en ocasiones ha aplicado la propia AEPD) a las series que se consideran ficheros de datos, y no a todas las series documentales, como hemos visto anteriormente con ocasión de la Resolución R/00431/2009 (procedimiento TD/01520/2008) referida a la denegación a un particular de su derecho de cancelación respecto de sus datos personales obrantes en determinados expedientes de la Universidad de Burgos; o en la polémica referida a los libros de bautismo.

²⁸⁶ Erigida por la LOPD, como vimos, en principal intérprete de los valores históricos, científicos y estadísticos de los datos, a través del procedimiento para la autorización de su conservación.

²⁸⁷ Recomendaciones de la AEPD al INAP, de 23 de diciembre de 2004.

La documentación que se custodia en el Archivo Central incluye entre otros aspectos, solicitudes, relaciones de participantes, nombramientos y evaluaciones de profesores, partes de firma, exámenes, trabajos, libros de registro de diplomas, fichas de opositores y actas de tribunales. Algunos Centros, con carácter previo a la remisión de la documentación al Archivo Central, realizan un expurgo de la misma y destruyen la que consideran que no es necesario conservar.

El I.N.A.P. no dispone de unas normas para determinar la documentación que se debe conservar ni del procedimiento a seguir para la destrucción de los documentos que contengan datos de carácter personal y que tengan que ser desechados.

Una empresa privada retira la documentación, que previamente ha sido depositada en cajas, de las instalaciones del Instituto para proceder a su destrucción emitiendo el correspondiente certificado. Entre el Instituto y la citada compañía no se ha formalizado un contrato que regule esta prestación de servicios.

Ante la destrucción incontrolada de documentos que forman parte de nuestro Patrimonio Documental, la AEPD no encuentra nada reprochable. No en vano, así se da cumplimiento al deber de cancelar los datos una vez han cumplido la finalidad para la que fueron recogidos. Las únicas recomendaciones al respecto son las de "delimitar [...] los procedimientos a seguir respecto a la documentación que deba ser desechada" –para que se realicen de conformidad con la normativa de protección de datos- y que el contrato con la empresa encargada de la eliminación -que sí debía existir, a pesar de lo que parece desprenderse de la última frase del texto citado- cumpla los requisitos exigidos por la LOPD.

Lo que estos hechos reflejan no es sino un desconocimiento y, como decíamos arriba, una falta de sensibilidad respecto de los archivos y documentos públicos que no es exclusiva de la Agencia Española de Protección de Datos²⁸⁸, sino, en general, de nuestras Administraciones Públicas y, por extensión, de la sociedad. De ahí que sea normal que frente a la normativa de protección de datos, los archivos se encuentren en situación de inferioridad.

²⁸⁸ En el caso tratado, el principal o único responsable es el INAP, cuya actuación –si el documento de la AEPD refleja verazmente los hechos- roza lo bochornoso si tenemos en cuenta que imparte formación sobre archivística y eliminación de documentos, si nos atenemos a lo que establece la Disposición adicional cuarta del Real Decreto 1164/2002: *El Instituto Nacional de Administración Pública, en el ámbito de sus funciones de formación y perfeccionamiento de funcionarios de los Cuerpos y Escalas de la Administración General del Estado y de los Organismos públicos vinculados o dependientes de la Administración General del Estado, incluirá en sus programas anuales la realización de cursos de formación sobre archivística, eliminación y conservación en soporte diferente del original de documentos administrativos.*

4. COMUNICACIONES DE DATOS EN LOS ARCHIVOS DE LA AGE

4.1. Las transferencias como cesión de datos

La normativa sobre protección de datos entiende como cesión o comunicación de datos toda revelación de datos realizada a una persona distinta del interesado (art. 3.i LOPD). De acuerdo con esta definición, el acceso por parte de los ciudadanos a los documentos y la difusión pública por distintos medios de descripciones o reproducciones de los mismos serían ejemplos de comunicaciones de datos que se realizan en los archivos de la AGE. Menos claros nos parecen dos casos que suponen el movimiento de documentos y que también abordamos en este capítulo: las transferencias y los préstamos.

Las transferencias son el procedimiento habitual de ingreso de fondos en un archivo mediante traslado de las fracciones de series documentales, una vez que éstas han cumplido el plazo de permanencia fijado por las normas establecidas en la valoración para cada una de las etapas del ciclo vital de los documentos. Como adelantamos en el Capítulo 3, el régimen de transferencias del sistema archivístico de la Administración General del Estado se reguló en el Decreto 914/1969, de 8 mayo, de creación del Archivo General de la Administración Civil (BOE nº 125, de 26 de mayo), que estableció el siguiente "circuito documental":

- Transferencias anuales²⁸⁹ desde las distintas unidades administrativas (archivos de gestión o de oficina) al archivo central de cada Ministerio, de los expedientes concluidos²⁹⁰ (art. 2).

²⁸⁹ Salvo resolución en contra del Subsecretario del Departamento correspondiente, cuando la índole de los documentos así lo aconseje o con aquellas series documentales que por razón de su frecuente consulta convenga conservar en la dependencia que las produce o tramita.

- Transferencias de los archivos centrales al Archivo General de la Administración, tras quince años de su ingreso en los mismos²⁹¹ (art. 3); y de los servicios provinciales a los archivos históricos provinciales²⁹² (art. 5).
- Transferencias del Archivo General de la Administración al Archivo Histórico Nacional de la documentación que con más de veinticinco años de antigüedad carezca, a juicio de la Dirección General del Libro, Archivos y Bibliotecas del Ministerio de Cultura²⁹³, de validez administrativa y tenga valor histórico (art. 3).

Este sistema –que lamentablemente nunca fue llevado correctamente a cabo- tendría que haber sido alterado a tenor de las normas de constitución y regulación de las distintas Comisiones Calificadoras de Documentos Administrativos –comenzando por la Superior (CSCDA)- creadas al amparo del artículo 58 de la Ley del Patrimonio Histórico Español. Así, se establece sobre el papel un nuevo sistema –aunque muy básicamente perfilado- en el citado Real Decreto 1164/2002²⁹⁴ y las distintas Órdenes ministeriales por las que se crean y regulan las distintas Comisiones Calificadoras de Documentos Administrativos departamentales.

²⁹⁰ Concretamente, el Decreto se refiere a los expedientes en que se hayan dictado actos administrativos de resolución que afecten de algún modo a derechos o intereses del Estado o de los administrados, cuando dichos actos hayan devenido firmes y se hayan practicado por la Administración las actuaciones conducentes a la total ejecución de sus pronunciamientos. Además, establece que cuando se trate de expedientes o documentos en que no proceda dictar actos administrativos de resolución del carácter expresado, así como informes, estudios, etc., pasarán al Archivo General cuando hayan producido en la dependencia que los ha elaborado o tramitado la totalidad de sus efectos.

²⁹¹ O con anterioridad si así lo acuerda el Subsecretario del Departamento, a propuesta del Archivo del Ministerio. Caso previsto para aquellas series documentales que tengan poco uso y se consulten raramente.

²⁹² Que cumplen, a nivel provincial, la finalidad asignada al AGA con respecto a los órganos centrales. Los AHP ejercen además, en dicho nivel -como su propio nombre indica-, la función del Archivo Histórico Nacional. El Decreto prevé, para los casos en que especiales circunstancias lo aconsejen, la creación por parte del Ministerio de Cultura de depósitos regionales que completen la estructura archivística de la Administración.

²⁹³ Mediante resolución y previa consulta a los Departamentos interesados.

²⁹⁴ Real Decreto 1164/2002, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y la conservación de documentos administrativos en soporte distinto al original

En dicho sistema no hay unos plazos generales de transferencia, sino plazos específicos para cada serie documental, que deberán ser establecidos, previo proceso técnico de valoración²⁹⁵ (art. 2.2 del Real Decreto 1164/2002) y a propuesta de la correspondiente Comisión Calificadora²⁹⁶ -que deberá ser elevada, por su parte, a la Superior para su dictamen²⁹⁷- mediante resolución de los propios Ministerios (Subsecretaría) u organismos públicos correspondientes.

A la vista de la definición de cesión de datos con la que iniciábamos este apartado (revelación de datos realizada a una persona distinta del interesado), no está claro que puedan entenderse como tales las transferencias que afecten a series documentales que contienen datos de carácter personal amparados por la normativa que estamos estudiando, ya que, por lo general, se trata de movimientos de documentos en el seno de una misma Administración, esto es, no se revelan a otra persona. Así, las disposiciones de creación de ficheros de los distintos órganos de la Administración General de Estado no contemplan como cesión de datos²⁹⁸ las transferencias a los archivos, singularmente al Archivo General de la Administración (adscrito, como ya se ha dicho, al Ministerio de Cultura, pero que recibe transferencias del resto de archivos centrales departamentales y de organismos públicos de la AGE).

²⁹⁵ Dicho proceso consiste en el estudio y análisis de las características históricas, administrativas, jurídicas, fiscales e informativas de la documentación; y es realizado, entendemos, por los distintos archivos centrales departamentales.

²⁹⁶ Las órdenes ministeriales por las que se crean las CCDA suelen establecer entre las funciones de dichos órganos colegiados la de proponer "los plazos de permanencia de los documentos o series documentales en los archivos de oficina del Ministerio y de sus Organismos públicos, proponer los criterios y plazos para su transferencia al Archivo Central del Ministerio, así como los plazos para su transferencia posterior al Archivo General de la Administración". Véanse, a este respecto, las normas por las que se crean las siguientes CCDA: Ministerio de Industria, Turismo y Comercio (Orden ITC/3863/2004, 2.b); Ministerio de Fomento (Orden FOM/542/2005, art. 3.a); Ministerio de Cultura (Orden CUL/3021/2006, art. 4.2); Ministerio de Trabajo e Inmigración (Orden TIN/3130/2008, art. 4.1.b); Ministerio de Educación (Orden EDU/3274/2009, art. 3.b); Ministerio de Justicia (Orden JUS/2935/2009, art. 5.1.b) -en este caso se prevé además la posible transferencia directa de documentos al Archivo Histórico Nacional-; Ministerio de Sanidad y Política Social (Orden SAS/3592/2009, art. 4.1.b) y Ministerio de Política Territorial (Orden TER/650/2010, art. 4.1.a).

²⁹⁷ El Real Decreto 1401/2007 establece que corresponde a la Comisión Superior Calificadora de Documentos Administrativos el estudio y dictamen sobre los plazos de permanencia de los documentos administrativos en cada uno de los diferentes tipos de archivos de oficina o gestión, central, intermedio e histórico; y sobre las transferencias, una vez cumplidos los plazos de permanencia, entre cada uno de los tipos de archivos (art. 1.1, apartados a y b).

²⁹⁸ De los documentos del archivo, nos referimos; sí se prevé, en algunos casos, la cesión de datos procedentes de los sistemas de descripción, que se realiza para acompañar a las transferencias.

Distinto sería el caso de las transferencias procedentes de entidades de la administración institucional, dotadas en este caso de personalidad jurídica propia. Así, la Resolución de 15 de abril de 2009, de la Mutualidad General de Funcionarios Civiles del Estado, por la que se crean ficheros de datos de carácter personal (BOE nº 123, de 21 de mayo), prevé la cesión de datos al AGA "cuando se transfiere la documentación al mismo"²⁹⁹. Más problemático sería el de las transferencias que se producen de los órganos de la Administración periférica del Estado a los archivos históricos provinciales (por ejemplo, de la Subdelegación del Gobierno al Archivo Histórico Provincial de Salamanca), que son gestionados por las Administraciones autonómicas.

En cualquier caso, las transferencias en el marco del sistema de archivos de la Administración General del Estado estarían plenamente permitidas por la normativa de protección de datos ya que se realizan para el cumplimiento de fines directamente relacionados con las funciones legítimas del "cedente" y del "cesionario"³⁰⁰ (art. 11.1 LOPD), teniendo por objeto el tratamiento posterior de los datos con fines históricos (arts. 4.2 y 21.1 LOPD) y no precisan además del consentimiento de los afectados (arts. 11.2.e y 21.4 LOPD)³⁰¹.

²⁹⁹ Este caso es significativo ya que declara como un único fichero –con la denominación "Archivo general"– lo que parece ser, precisamente, el propio Archivo central de la Mutualidad General de Funcionarios Civiles del Estado (MUFACE).

³⁰⁰ Que como ya se señaló, es el órgano administrativo al que se revelan los datos. En este caso, mediante transferencia de los documentos que los contienen.

³⁰¹ Podría considerarse, además, en este sentido, que están autorizadas por la Ley 16/1985, del Patrimonio Histórico Español (LPHE) a los efectos del art. 11.2.a LOPD, al menos en lo que se refiere a "los organismos dependientes de la Administración del Estado" y a las personas que por la función que desempeñen tengan a su cargo documentos de los englobados en el artículo 49.2 LPHE. Esta Ley ha dispuesto que cada Departamento ministerial tenga que asegurar la coordinación del funcionamiento de todos los archivos del Ministerio y de los organismos a él vinculados para el mejor cumplimiento de lo preceptuado en dicha Ley y en los reglamentos que se dicten para su aplicación (art. 65.1 LPHE). Así mismo, establece que la documentación de los organismos dependientes de la Administración del Estado será regularmente transferida, según el procedimiento que por vía reglamentaria se establezca, a los Archivos del Estado (art. 65.2 LPHE). También la de aquellas personas que por la función que desempeñen tengan a su cargo documentos a los que se refiere el artículo 49.2 de la Ley, que están obligados, al cesar en sus funciones, a entregarlos a quien les sustituya o remitirlos al archivo que corresponda (art. 54.1 LPHE).

4.2. Breve referencia a los préstamos

La Archivística española entiende por "préstamo" la salida temporal de documentos de un archivo con fines administrativos o judiciales (aunque generalmente se habla de préstamos administrativos en ambos casos) o de difusión cultural (préstamos para exposiciones). De estos últimos no trataremos, ya que su casuística es similar a la de la consulta de documentos, por lo que remitimos al apartado correspondiente para su análisis.

Por lo que se refiere a los primeros, no creemos que los préstamos "internos" (por ejemplo, del archivo central de un Ministerio o del AGA³⁰² al órgano productor de los documentos) puedan considerarse una cesión de datos. Ahora bien, el receptor del préstamo deberá estar autorizado para acceder al documento o documentos en cuestión, como establecen las medidas de seguridad del Reglamento de 2007. En cuanto a los "externos", esto es, a otras Administraciones, órganos judiciales, etc., entendemos que deben cumplirse las siguientes condiciones:

- Que se realicen para el cumplimiento de fines directamente relacionados con las funciones legítimas del "cedente" y del "cesionario"³⁰³ (art. 11.1 LOPD).

³⁰² El artículo 4 del citado Decreto 914/1969 establece que la documentación conservada en el Archivo General de la Administración se considerará en todo momento al servicio de los organismos que la hubieran remitido, debiendo aquél facilitar cualquier información, copia o certificación que le soliciten, e incluso remitirle la documentación original si así lo requieren.

³⁰³ Por "funciones legítimas del cesionario" creemos que deberían entenderse -dando la vuelta en sentido positivo a lo indicado en el art. 21.1 LOPD- aquellas realizadas en el ejercicio de competencias equivalentes o que versen sobre las mismas materias que para las

- Que cuenten con el consentimiento de las personas afectadas o, en otro caso, que la cesión está autorizada en una ley (art. 11.2.a LOPD); que el destinatario sea el Defensor del Pueblo, el Ministerio Fiscal, los Jueces o Tribunales, el Tribunal de Cuentas o las instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas, y se realice en el ámbito de las funciones que la ley les atribuya expresamente (arts. 11.2.d LOPD y 10.4.b Reglamento)³⁰⁴; o cuando tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos y científicos (art. 11.2.e LOPD).

que se recogieron los datos. Un ejemplo podría ser el préstamo de un expediente producido por un órgano de la AGE en el ejercicio de una competencia que ha sido posteriormente transferida a una Comunidad Autónoma, al órgano de dicha Comunidad encargado de la misma. También podemos considerar funciones legítimas aquellas que tengan por objeto fines históricos, estadísticos o científicos (arts. 4.2 y 21.1 LOPD), para cuya determinación habrá que atenerse a la legislación que en cada caso resulte aplicable y, en particular, a lo dispuesto en la Ley 12/1989, de 9 de mayo, Reguladora de la Función Estadística Pública, la Ley 16/1985, de 25 junio, del Patrimonio Histórico Español y la Ley 13/1986, de 14 de abril de Fomento y Coordinación General de la Investigación Científica y Técnica, y sus respectivas disposiciones de desarrollo, así como a la normativa autonómica en estas materias.

³⁰⁴ En estos casos, sus normativas específicas suelen habilitar, además, esta circunstancia, al amparo del artículo 11.2.a LOPD.

4.3. El acceso a los documentos como cesión de datos

4.3.1. Una necesaria habilitación legal

La función principal de los archivos es garantizar y proporcionar el servicio de los documentos que recoge y conserva a sus usuarios, que en el caso de los archivos públicos son tanto internos (vinculados a las actividades de los órganos y los servicios de la institución generadora de la documentación), como externos (investigadores profesionales y aficionados, estudiantes y ciudadanos en general). Este acceso por parte de usuarios externos³⁰⁵, cuando se refiere a documentos que contengan datos de carácter personal, sean electrónicos o en papel –siempre que estén organizados conforme a criterios personales-, supone una revelación de datos realizada a un tercero o, lo que es lo mismo, una cesión o comunicación de datos afectada por la normativa de protección de datos de carácter personal. Y, por tanto, la colisión entre dos derechos constitucionales: el derecho de acceso a archivos y registros administrativos (art. 105.c CE) -ampliado y redefinido en los últimos años como derecho de acceso a la información pública³⁰⁶- y el derecho a la protección de datos de carácter personal.

Lamentablemente, como ha señalado Guichot (2009, p. 198), “no hay estudios monográficos relevantes conocidos por nosotros que analicen el

³⁰⁵ Que afecta al archivo no solo en su acepción de servicio o institución, que definíamos en nuestro Capítulo 0. También, a los archivos de gestión de las oficinas y unidades administrativas.

³⁰⁶ En una nueva definición acorde con nuestro contexto europeo, que parece que acabará imponiéndose –al menos, esa es la intención- (Fernández Cuesta 2010).

encaje entre ambos derechos³⁰⁷; y cuando se ha realizado desde la óptica de la protección de datos se “ha llegado, en ocasiones, a opiniones maximalistas conforme a las cuales no cabe en ningún caso la comunicación a terceros de ningún dato personal en poder de la Administración³⁰⁸” (pp. 167-168). No es nuestra intención realizar un análisis exhaustivo de toda la casuística posible pero sí, como hemos hecho respecto a otros tratamientos, analizar en qué casos permite la normativa de protección de datos una comunicación a terceros, de conformidad con sus principios.

Por lo que se refiere al principio de finalidad, y como ya hemos señalado con anterioridad, la Ley establece que los datos de carácter personal sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario (art. 11.1 LOPD). En el caso que nos ocupa, entendemos que la legitimidad vendría conferida, principalmente, por la legislación reguladora del derecho de acceso a archivos y registros administrativos (art. 105.b CE)³⁰⁹, así como por la relativa al derecho de acceso a la cultura (art. 44.1 CE) y, en general, a los distintos fundamentos constitucionales del acceso a la información pública³¹⁰.

En segundo lugar, debe contarse con el consentimiento de la/s persona/s afectada/s (art. 6.1 LOPD y art. 10.1 Reglamento). Este requisito puede eludirse, como hemos visto en casos anteriores, si la cesión está autorizada en una ley (art. 6.2 LOPD) y, particularmente -de acuerdo con el art. 10.2.a del Reglamento-, cuando la cesión tenga por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dicha norma, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados, especialmente su honor y su intimidad personal y familiar; o cuando la

³⁰⁷ Quizás destaque la propia obra de Guichot, así como las de Castillo (2007a) y el extenso artículo de Troncoso (2008), al que nos remitiremos en buena parte de este apartado.

³⁰⁸ Lo que, para este autor (p. 168), “resulta absolutamente irreconciliable con el carácter no absoluto de los derechos fundamentales y su necesaria compatibilidad con el resto de derechos, bienes y principios constitucionales, afirmado por el Tribunal Constitucional”.

³⁰⁹ Derecho reconocido en el art. 35.h de la Ley 30/1992, de 26 de noviembre, de régimen jurídico de las Administraciones Públicas y del procedimiento administrativo común (LPAC) y regulado en el art. 37 de dicha ley.

³¹⁰ Véase en este sentido Troncoso (2008, p. 24 y ss.).

cesión sea necesaria para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas.

El acceso por parte de terceros a documentos que contienen datos de carácter personal amparados por la normativa que estamos tratando sin el consentimiento de las personas afectadas requiere, por tanto –en aras del cumplimiento de los principios de finalidad y consentimiento– una habilitación legal³¹¹, que vendrá dada –para el caso que nos ocupa– por la legislación reguladora del derecho de acceso a la información pública. Surge así un primer problema, ya que, como ha señalado Troncoso (2008, pp. 57-58):

No existe una habilitación legal clara que permita la cesión de datos personales sin un interés legítimo y sin consentimiento del interesado en beneficio del principio de transparencia administrativa. Es decir, la LOPD no contemplo como límite al derecho fundamental a la protección de datos personales un derecho de acceso a [la] información administrativa sin interés legítimo [...]. De esta forma, el mayor desarrollo legislativo de la protección de datos personales y la falta del mismo en el caso del acceso a la información pública sitúa la balanza más cercana a la protección de datos personales que a la transparencia administrativa.

4.3.2. Regulación legal del acceso a los documentos en los archivos de la AGE

En efecto, no contamos en nuestro país con una ley de acceso a la información pública, sino con una legislación deficiente, restrictiva y dispersa que, por lo que se refiere específicamente al acceso a los archivos de la AGE³¹², ha dado lugar a una situación de indeterminación en cuanto al régimen jurídico aplicable.

Esta indeterminación viene provocada, principalmente, por la dicotomía que la Ley 30/1992, de 26 de noviembre, de régimen jurídico de las Administraciones Públicas y del procedimiento administrativo común

³¹¹ Así lo entiende Guichot (2009, p. 190), que señala que “la posibilidad general de comunicar directamente datos personales a terceros sin consentimiento queda reducida al caso en que una ley así lo prevea (una ley que no es la propia LOPD, que se limita a establecer esta reserva legal)”.

³¹² Para un análisis de la normativa referida al derecho de acceso a archivos y registros administrativos, véanse especialmente las obras de Fernández Ramos (1997) y Rams (2008).

(LPAC) establece entre "archivos administrativos" y "archivos históricos". Esta diferenciación conlleva que cada tipo de archivo se inscriba en un distinto régimen jurídico: los "archivos administrativos", en el régimen general del derecho de acceso a los archivos y registros administrativos, reconocido en el artículo 105.b CE y regulado en la LPAC (art. 37)³¹³; y los "archivos históricos", al régimen específico de la consulta de los fondos documentales existentes en los archivos históricos -más relacionado con el derecho de acceso a la cultura reconocido en el artículo 44.1 CE³¹⁴- , regulado en la Ley 16/1985, de 25 de junio, de Patrimonio Histórico Español (LPHE, art. 57). A pesar de ello, nuestro ordenamiento jurídico no permite diferenciar claramente qué archivos se considerarían administrativos y cuáles históricos. Y más teniendo en cuenta el deficiente funcionamiento del régimen de transferencias entre los distintos tipos de archivo. Por último, a todo ello debemos unir que la LPHE extiende su régimen a los documentos "depositados y registrados en los Archivos centrales de las correspondientes entidades de Derecho Público", dificultando aún más si cabe este complicado solapamiento de regímenes jurídicos.

Así, aunque parece claro que buena parte de los llamados Archivos Estatales, gestionados por el Ministerio de Cultura, entran claramente en la categoría de archivos históricos (Archivo Histórico Nacional, Archivo de la Corona de Aragón, Archivo General de Simancas, Archivo General de Indias, Centro Documental de la Memoria Histórica, Sección Nobleza del Archivo Histórico Nacional), la situación se complica en los casos del Archivo General de la Administración (que no ha podido transferir documentos al AHN debido a la falta de espacio de éste, acumulando por tanto un importante volumen de documentación histórica), muchos archivos centrales departamentales (algunos de los cuales cuentan con documentos que se remontan al siglo XVI) y los archivos históricos provinciales (que son al mismo tiempo archivos intermedios y archivos históricos).

³¹³ Art. 37.1. LPAC: *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, siempre que tales expedientes correspondan a procedimientos terminados en la fecha de la solicitud.*

³¹⁴ Adviértase la distinta terminología aplicada en cada caso: acceso / consulta.

Por otro lado, el de los archivos históricos no es el único régimen especial que reconoce la LPAC. El artículo 37.6 señala, además, que se regirán por sus disposiciones específicas: los documentos sometidos a la normativa sobre materias clasificadas³¹⁵; los documentos y expedientes que contengan datos sanitarios personales de los pacientes³¹⁶; los archivos regulados por la legislación del régimen electoral³¹⁷; los archivos que sirvan a fines exclusivamente estadísticos dentro del ámbito de la función estadística pública³¹⁸; el Registro Civil³¹⁹, el Registro Central de Penados y Rebeldes³²⁰ y los registros de carácter público cuyo uso esté regulado por una ley³²¹; y el acceso a los documentos obrantes en los archivos de las Administraciones Públicas por parte de las personas que ostenten la condición de Diputado de las Cortes Generales³²², Senador³²³, miembro de una Asamblea legislativa de Comunidad Autónoma³²⁴ o de una Corporación Local³²⁵ (art. 37.6.f LPAC). A todo ello habría que sumar, además, multitud de disposiciones específicas dispersas en normas sectoriales³²⁶.

³¹⁵ Ley 9/1968, de 5 abril, de Secretos Oficiales (BOE nº 84, 6 de abril de 1968). Desarrollada por Decreto 241/1969, de 20 de febrero (BOE nº 47, 27 de febrero de 1969). Podrán ser consultados mediante autorización del órgano que efectuó la declaración de secreto o reservado (art. 57.1.b LPHE).

³¹⁶ Han sido regulados en la llamada Ley de Autonomía del Paciente: Ley 41/2002, de 14 noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (BOE nº 274, de 15 de noviembre).

³¹⁷ Ley Orgánica 5/1985, de 19 junio, del Régimen Electoral General (BOE nº 147, de 20 de junio).

³¹⁸ Ley 12/1989, de 9 de mayo, de la Función Estadística Pública (BOE nº 112, de 11 de mayo)

³¹⁹ Ley de 8 de junio de 1957, sobre el Registro Civil (BOE nº 151, de 10 de junio). Desarrollada por Decreto de 14 de noviembre de 1958 por el que se aprueba el Reglamento de la Ley del Registro Civil (BOE nº 296, de 11 de diciembre).

³²⁰ Real Decreto 95/2009, de 6 febrero, por el que se regula el Sistema de registros administrativos de apoyo a la Administración de Justicia (BOE nº 33, de 7 de febrero).

³²¹ Por ejemplo, el Registro de la Propiedad (Ley Hipotecaria, texto refundido aprobado por Decreto de 8 de febrero de 1946) o el Registro Central de Personal de la AGE (establecido por el artículo 13 de la Ley 30/1984, de 2 de agosto, y regulado por Real Decreto 1405/1986, de 6 de junio, por el que se aprueban el Reglamento del Registro Central de Personal y las normas de coordinación con los de las restantes administraciones públicas).

³²² Reglamento del Congreso de los Diputados de 10 de febrero de 1982 (BOE nº 55, de 5 de marzo).

³²³ Reglamento del Senado, texto refundido de 3 de mayo de 1994 (BOE nº 114, de 13 de mayo).

³²⁴ Por ejemplo, Reglamento de las Cortes de Castilla y León, de 24 febrero 1990 (BOCYL nº 45, de 5 de marzo).

³²⁵ Ley 7/1985, de 2 de abril, de bases del Régimen Local (BOE nº 80, de 3 de abril). Real Decreto 2568/1986, de 28 noviembre, por el que se aprueba el Reglamento de organización,

Si el acceso a documentos que contengan datos de carácter personal afectados por la regulación de la LOPD se realiza de conformidad con la norma aplicable en cada caso, entendemos que la cesión se realiza de conformidad con los principios de finalidad y consentimiento exigidos. Dejando a un lado las disposiciones específicas y sectoriales y ciñéndonos al marco establecido por la LPAC y la LPHE³²⁷, podemos encontrar esa necesaria habilitación legal para la consulta por parte de terceros de documentos que contengan datos personales en los siguientes supuestos:

- En general, cuando exista consentimiento expreso de las personas afectadas (art. 57.1.c LPHE)
- En el caso de los documentos que contengan datos de carácter íntimo, cuando haya transcurrido un plazo de cincuenta años a partir de la fecha de los documentos (art. 57.1.c LPHE)³²⁸.
- Respecto al resto de documentos con datos personales, cuando se realice para el ejercicio de los derechos de los ciudadanos, previa acreditación de un interés legítimo y directo (art. 37.3 LPAC)³²⁹; cuando los documentos obren en archivos históricos (art. 57.1.a LPHE) o cuando haya transcurrido el referido plazo de cincuenta años, a partir de la fecha de los documentos.

funcionamiento y régimen jurídico de las Entidades Locales (BOE nº 305, de 22 de diciembre).

³²⁶ Por ejemplo, la Ley 27/2006, de 18 julio, por la que se regulan los derechos de acceso a la información, de participación pública y de acceso a la justicia en materia de medio ambiente (BOE nº 171, de 19 de julio). O las disposiciones relativas al acceso a la documentación catastral contenidas en el Real Decreto Legislativo 1/2004, de 5 de marzo por el que se aprueba el Texto Refundido de la Ley del Catastro Inmobiliario (BOE nº 58, de 8 de marzo) y en el Real Decreto 417/2006, de 7 de abril, por el que se desarrolla el texto refundido de la Ley del Catastro Inmobiliario (BOE nº 97, de 24 de abril).

³²⁷ Siguiendo el modelo propuesto por Fernández Ramos (1997) para articular los regímenes de ambas y que se basa en que "el art. 57.1.c LPHE debe aplicarse no sólo a los Archivos General de la Administración e Histórico Nacional, sino también a los archivos precedentes cuando se cumplan los plazos fijados en la Ley" (p. 98).

³²⁸ Este artículo contempla también un plazo de veinticinco años desde la muerte de la persona afectada, si su fecha es conocida, que no contemplamos a efectos de nuestro estudio, dado que la normativa de protección de datos únicamente se refiere a las personas vivas.

³²⁹ La denegación de esta autorización podrá realizarse únicamente cuando prevalezcan razones de interés público, intereses de terceros más dignos de protección o cuando así lo disponga una ley, debiendo para ello el órgano competente dictar resolución motivada (art. 37.4 LPAC).

4.3.3. Acceso a los documentos y principio de calidad

Por tanto, si el acceso a los documentos obrantes en los archivos de la AGE se realiza de conformidad con la legislación vigente en esta materia, estaríamos ante un tratamiento de datos ajustado a los principios de finalidad y consentimiento que exige la LOPD. El siguiente paso nos lleva a analizar la conformidad de este tipo de cesión de datos con el tercer principio de la protección de datos, el de calidad, en su vertiente de proporcionalidad.

De esta manera, el acceso a los documentos cumpliría con las tres premisas exigibles que legitiman los límites y las intromisiones en los derechos fundamentales: el límite debe estar previsto en una ley (en nuestro caso, la LPAC y la LPHE), debe ser un bien o valor constitucional (el derecho de acceso a la información pública³³⁰) y debe respetarse el principio de proporcionalidad (Troncoso 2008, pp. 61-62). Así, se exige, además de la referida habilitación legal, una conexión entre la naturaleza de los datos y los fines de la cesión, ya que los datos de carácter personal no pueden usarse, con carácter general, para finalidades incompatibles con aquellas para las que fueron recogidos (art. 8.3 Reglamento)³³¹.

En este sentido, y como hemos indicado con anterioridad, no se considera incompatible la comunicación de datos de carácter personal a terceros con fines históricos (art. 9.1 Reglamento), legitimándose dicha circunstancia a través de la citada Ley 16/1985, de 25 junio, del Patrimonio Histórico Español y sus normas de desarrollo. Por ello, creemos que las consultas de documentos que se realicen de conformidad con el art. 57 de la LPHE son proporcionales y están perfectamente legitimadas frente a la normativa de protección de datos. Con una única excepción: la de los ya mencionados expedientes instruidos al amparo de las Leyes de Vagos y Maleantes, y de Peligrosidad y Rehabilitación Social. En este caso, la LOPD (Disp. Adic. tercera) ha previsto unas condiciones más estrictas para su consulta.

³³⁰ Que "aunque no ha sido expresamente reconocido como derecho, como ocurre en otros países", tiene en el nuestro "un sólido fundamento constitucional" (Troncoso 2008, p. 40).

³³¹ Como ha indicado Troncoso (2008, p. 62), "la habilitación legal para el acceso a información [...] elude la necesidad del consentimiento del interesado, pero no la vigencia del principio de calidad".

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

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

El principal problema para conciliar el acceso a los documentos³³² con el principio de calidad lo encontramos cuando aquel se realiza fuera de los archivos históricos y requiere la acreditación de un interés legítimo (art. 37.3 LPAC). Según Troncoso (2008, p. 63 y ss.):

El juicio de proporcionalidad en sentido estricto nos obliga a ponderar en cada caso si el fin a alcanzar –el bien constitucional que requiere acceso a información administrativa– es proporcional con el medio –la intromisión en el derecho fundamental a la protección de datos personales–, un análisis que no siempre deja cerrado el legislador y que no es fácil despegar del supuesto concreto.

Para ello propone un modelo que podría inspirar a la futura –y tan reclamada– ley de acceso a la información pública³³³ pero que serviría, sobre todo, para realizar “la necesaria valoración de cada caso concreto” que, en nuestra opinión, habría de hacer, en primer lugar, el órgano encargado de resolver la solicitud de acceso. Y que se enriquecería con la doctrina de las Comisiones de Acceso a la Información (p. 166) que, como ocurre en otros países, sería conveniente que se configuraran “en cada una de las en cada una de las Administraciones Públicas”. Como señala Guichot (2009, p.272),

[p]ara el correcto funcionamiento del sistema y la creación de directrices que guíen su aplicación, resulta fundamental la institución de un organismo de control del funcionamiento del sistema de acceso a la información (bien burocrático en cada

³³² Nos referimos, claro está, al acceso a los documentos producidos por la AGE que contengan datos de carácter personal, que no afecten al ámbito estricto de la intimidad y sin el consentimiento de los afectados.

³³³ “[Y]a que los límites a los derechos fundamentales están sometidos a reserva de ley” (Troncoso 2008, p. 99).

Administración, bien con la naturaleza de una Administración independiente), que pudiera pronunciarse sobre las decisiones administrativas, dando una respuesta rápida y gratuita [...] y sentando gradualmente los criterios generales de ponderación, siendo en todo caso recurribles ante los tribunales contencioso-administrativo las decisiones sobre acceso.

Este modelo, válido también para evaluar la publicidad de oficio de las actuaciones administrativas y, en definitiva, de la información pública (incluidos los sistemas de descripción archivística) consiste en analizar:

- Los distintos niveles de publicidad³³⁴, ya que (Troncoso 2008, p. 64)

no es lo mismo el acceso en un registros público a una información administrativa en la que se contengan datos personales a que te faciliten copia del expediente, a la publicación de esa información en un tablón de anuncios, a la publicación en una Intranet, a la publicación en un espacio privado en Internet, a la publicación abierta en Internet y a la publicación en un boletín oficial.

- Cuáles son los plazos de cancelación y si los datos son excesivos, aspecto referido más propiamente a los supuestos de publicidad de oficio de las actuaciones administrativas (pp. 67-75) –por ejemplo, en las ediciones electrónicas de los diarios oficiales³³⁵–, que supone valorar la idoneidad de los datos a difundir de forma que no sean excesivos, así como su exactitud y actualización y el cese de dicha publicación cuando se haya cumplido la finalidad para la que fue realizada³³⁶.
- La tipología de los datos personales (pp. 75-86), en función de su “sensibilidad” y de las medidas de seguridad y acceso que requieran.

³³⁴ Por ejemplo, si la posibilidad de acceder a un documento conlleva además la de obtener copia del mismo.

³³⁵ Véase a este respecto el artículo de Troncoso que venimos siguiendo en este apartado (2008, 101-112).

³³⁶ Este criterio viene a hacer efectivo el llamado “derecho al olvido” que está reclamando la doctrina de las agencias de protección de datos, con respecto a la indexación por los motores de búsqueda de datos personales, procedentes en ocasiones de publicaciones oficiales. Cuestión de bastante actualidad, ya que ha llevado recientemente a que el BOE tome medidas para limitar dicha indexación. Véase “Lo que Google sabe de ti a través del BOE... y tú no quieres que sepa” en *ABC.es*, 22 de junio de 2011. Disponible en: <http://www.abc.es/20110622/espana/abci--201106212026.html> [Consulta: 22 jun. 2011].

- La existencia del interés público que está detrás de la solicitud de acceso (pp. 87-101), cuestión que depende esencialmente del contenido de la información, pero también de quién lleva a cabo la solicitud (medios de comunicación³³⁷, particulares o entidades privadas que desarrollan investigaciones históricas o científicas³³⁸...)

Ciertamente, el modelo nos parece adecuado, siempre que se sustente en una ley de acceso a la información pública y se apoye en una autoridad de control (Comisión de Acceso a la Información) que –como decía Guichot– pueda pronunciarse sobre las decisiones administrativas y vaya sentando gradualmente los criterios generales de ponderación. Autoridad que, en nuestra opinión, debería ser independiente y no incardinarse en las Agencias de Protección de Datos como propone Troncoso (2008) y parecía decantarse el anteproyecto de ley de transparencia y acceso a la información pública filtrado en 2010 (Fernández Cuesta 2010)³³⁹.

La situación actual no ofrece tantas garantías y, ante la ausencia de esa necesaria ley de acceso a la información pública que aborde estas cuestiones y ponga fin al caos normativo existente, prima el derecho a la protección de datos³⁴⁰, al menos hasta el ingreso de los documentos en un archivo histórico³⁴¹.

³³⁷ Aunque “[u]na información no tiene interés público por el único hecho de que la solicite un medio de comunicación, sino que hay que tener en cuenta también el contenido de la misma” (Troncoso 2008, p. 95).

³³⁸ Así, “el interés público en la actividad investigadora permite el acceso a documentos administrativos que tengan datos nominativos, salvo que afecte a la intimidad de la persona o transcurran 25 años desde su muerte si la fecha es conocida o, en otro caso, de 50 años a partir de la fecha de los documentos” (Troncoso 2008, pp. 95-96), de acuerdo con el art. 57.1.c de la LPHE.

³³⁹ Ya que, por un lado, el derecho de acceso a la información pública no está limitado únicamente por el derecho a la protección de datos: otros bienes y valores constitucionales pueden entrar en juego, desde la seguridad y la defensa del Estado, a la propiedad industrial. Y, por otro, el historial de la AEPD hasta el momento no nos augura un equilibrio perfecto entre ambos derechos, sino que la balanza se inclina más del lado de la LOPD.

³⁴⁰ De hecho, llama la atención que “un cotejo de las disposiciones generales de creación de ficheros públicos permite comprobar que éstos no prevén la cesión de sus datos a sujetos privados, salvo que el fichero tenga precisamente por finalidad, exclusiva o concurrente, la información a los directamente implicados” (Guichot 2009, p. 192).

³⁴¹ Lo cual, dado el régimen actual de transferencias, parece difícil. Urge por tanto que la ley de acceso venga acompañada de una ley de archivos que permita una gestión eficaz de los documentos que produce la AGE, su ingreso en archivos y el servicio desde los mismos a los ciudadanos.

4.4. Los problemas de la difusión de información archivística.

La problemática que acabamos de señalar con respecto al acceso y consulta de los documentos obrantes en los archivos públicos se reproduce de forma similar en lo que se refiere a los sistemas de descripción archivística, especialmente en aquellos que permiten la difusión universal de los datos en la Red, dado que la LOPD tampoco previó como límite al derecho fundamental a la protección de datos personales “una publicación generalizada de información administrativa con datos personales a instancias de la Administración” (Troncoso 2008, p. 57).

Para comprender dicha problemática vamos a analizar el único fichero de este tipo declarado por el Ministerio de Cultura -“Guerra Civil y Franquismo”- y su difusión a través del Portal de Víctimas de la Guerra Civil y Represaliados del Franquismo³⁴².

4.4.1. El fichero “Guerra Civil y Franquismo”

Este fichero, creado por la Orden CUL/2211/2009, de 22 de junio, por la que se regulan los ficheros de datos de carácter personal del Ministerio de Cultura y sus organismos públicos (BOE nº 193, de 11 de agosto), se encuentra declarado de la siguiente manera:

- A) Finalidad del fichero y los usos previstos para el mismo:
Finalidad: El Real Decreto 1891/2004, de 10 de septiembre, crea una Comisión Interministerial para el estudio de la situación de las víctimas de la guerra civil y del franquismo con el fin de proponer las medidas legales, o de otro tipo, que resulten necesarias para ofrecer un adecuado reconocimiento y satisfacción

³⁴² Véase: <http://pares.mcu.es/victimasGCFPortal> [Consulta: 10 ene. 2011]

moral a los que padecieron actuaciones represivas durante la guerra civil y el franquismo, y hasta la restauración de las libertades democráticas. Esta comisión tiene, entre otras, la función de extraer de la documentación disponible los datos personales de los afectados, con los que se elaborara una base de datos o fichero. Recoger los nombres de las personas que estuvieron al servicio de la República en las Fuerzas del Orden Público o Cuerpo de Carabineros durante la Guerra Civil, y cuyos nombramientos aparecieron durante los años del conflicto en diferentes publicaciones oficiales. Recoger datos de los desaparecidos, muertos e inútiles como consecuencia de la Guerra Civil Española. El acceso a la información contenida en este fichero se adecuará a lo establecido en la Ley 16/1985 de Patrimonio Histórico Español (artículo 57).

Usos: Registros personalizados para consultas.

- B) Personas o colectivos sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos: Inculpados que aparezcan en los fondos seleccionados para el estudio. Personas afectadas.
- C) Procedimiento de recogida de datos de carácter personal: Recogida de datos específicos sobre los inculpados que aparezcan en los fondos seleccionados para el estudio, realizada por profesionales de los archivos. Ficheros automatizados antiguos.
- D) Estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo:
Para víctimas: Nombre y apellidos. Alias. Profesión que ejercía. Lugar de los hechos. Fondo donde consta su implicación y su causa.
Para Republicanos, desaparecidos, muertos e inútiles como consecuencia de la Guerra Civil: Nombre y apellidos.
- E) Cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros: A descendientes directos de las víctimas que así lo soliciten para la indagación, localización e identificación de las personas desaparecidas violentamente durante la Guerra Civil o la represión política posterior y cuyo paradero se ignore, según lo dispuesto en los artículos del 11 a 13 de la Ley 52/2007, de 26 de diciembre.
- F) Órganos de las Administraciones responsables del fichero: Dirección General del Libro, Archivos y Bibliotecas.
- G) Servicios o Unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Subdirección General de Archivos Estatales. Dirección General del Libro, Archivos y Bibliotecas. Ministerio de Cultura. Plaza del Rey n.º 1, 28004 Madrid.
- H) Medidas de seguridad con indicación del nivel básico, medio o alto exigible: Básico.
- I) Sistema de tratamiento utilizado: Automatizado/no automatizado.

En primer lugar, debemos señalar que en esta declaración no se expresa de forma clara la finalidad del fichero³⁴³, sino que, a través de un largo y

³⁴³ Para empezar, se da a entender que dicho fichero es fruto de la función de la Comisión Interministerial para el estudio de la situación de las víctimas de la guerra civil y del

confuso texto, se viene a decir que la finalidad del fichero es elaborar un fichero que recogerá datos de determinadas personas (lo cual es una obviedad que no viene a decir nada), a los que se accederá de conformidad con una ley que regula la consulta de documentos integrantes del patrimonio documental español. Tampoco viene a decir nada la declaración sobre los usos previstos para el fichero: "registros personalizados para consultas".

Por lo que se refiere a las personas o colectivos sobre los que se pretende obtener datos de carácter personal, se distinguen dos supuestos: primero, el de los "inculpados"³⁴⁴ que aparezcan en los fondos seleccionados para el estudio", lo cual requiere que dichas personas aparezcan en unidades documentales referidas a procedimientos penales o sancionadores. Y, segundo, el de las "personas afectadas". Sobra decir, creemos, esta obviedad: que entre las personas susceptibles de ser afectadas se encuentran las "personas afectadas". En otros elementos de la declaración se indica, sin embargo, de otra forma, quiénes son las personas de las que se obtendrán los datos: así, en el apartado A se habla de las personas que estuvieron al servicio de la República en las Fuerzas del Orden Público o Cuerpo de Carabineros durante la Guerra Civil; y de los desaparecidos, muertos e inútiles como consecuencia de la Guerra Civil Española. A estos "republicanos, desaparecidos, muertos e inútiles como consecuencia de la Guerra Civil" se añaden, en el apartado D, las "víctimas", entendemos que de la Guerra Civil y del Franquismo. De acuerdo con ello, todas estas

franquismo, creada por Real Decreto 1891/2004, de 10 de septiembre, de "extraer de la documentación disponible los datos personales de los afectados" para elaborar "una base de datos o fichero". Aunque en dicha norma no se atribuye esta función a la Comisión, podemos entender que fuera necesario para "proponer las medidas legales, o de otro tipo, que resulten necesarias para ofrecer un adecuado reconocimiento y satisfacción moral" a las víctimas de la Guerra Civil y el Franquismo. Si posteriormente se ha querido emplear esta base de datos con otra finalidad, debería haberse indicado claramente en la declaración, prescindiendo de los motivos que motivaron originariamente su creación. Dejando esto a un lado, la declaración continua indicando una serie de personas o colectivos sobre los que se van a extraer los datos de carácter personal (personas que estuvieron al servicio de la República en las Fuerzas del Orden Público o Cuerpo de Carabineros durante la Guerra Civil, y cuyos nombramientos aparecieron durante los años del conflicto en diferentes publicaciones oficiales – recordemos que el hecho de que dichos nombramientos se publicaran en diarios oficiales no significa que los datos se recojan de fuentes accesibles al público-; y desaparecidos, muertos –a los que, como ha quedado dicho, no afecta la normativa de protección de datos- e inútiles como consecuencia de la Guerra Civil Española), pero en ningún caso se declara con qué finalidad se recogen los datos. Y, por último, se indica que "[e]l acceso a la información contenida en este fichero se adecuará a lo establecido en la Ley 16/1985 de Patrimonio Histórico Español (artículo 57)", vinculando de esta manera la cesión de datos al derecho de consulta de los documentos: un usuario externo de este fichero podrá acceder únicamente a los datos referidos a las unidades documentales de libre consulta.

³⁴⁴ Aquellos que fueron objeto de acusación en un procedimiento penal o sancionador.

personas tendrían que aparecer mencionadas en unidades documentales referidas a procedimientos penales o sancionadores o en sistemas de descripción referidos a los mismos ("ficheros automatizados antiguos"), a partir de las cuales se realiza el procedimiento de recogida de datos de carácter personal (apartado C de la declaración).

La única cesión prevista de los datos es a "descendientes directos de las víctimas que así lo soliciten para la indagación, localización e identificación de las personas desaparecidas violentamente durante la Guerra Civil o la represión política posterior y cuyo paradero se ignore, según lo dispuesto en los artículos del 11 a 13 de la Ley 52/2007, de 26 de diciembre"³⁴⁵.

Por último, se indica que al fichero le serán de aplicación medidas de seguridad de nivel básico. Sin embargo, si sus datos se refieren ciertamente a inculpados en procedimientos penales o sancionadores, el fichero requeriría –como vimos en capítulos anteriores–, unas medidas de seguridad de nivel medio. Sería necesario, por tanto, hacer mención expresa al artículo 3 de la Ley 52/2007, por el que

1. Se declara la ilegitimidad de los tribunales, jurados y cualesquiera otros órganos penales o administrativos que, durante la Guerra Civil, se hubieran constituido para imponer, por motivos políticos, ideológicos o de creencia religiosa, condenas o sanciones de carácter personal, así como la de sus resoluciones.
2. Por ser contrarios a Derecho y vulnerar las más elementales exigencias del derecho a un juicio justo, se declara en todo caso la ilegitimidad del Tribunal de Represión de la Masonería y el Comunismo, el Tribunal de Orden Público, así como los Tribunales de Responsabilidades Políticas y Consejos de Guerra constituidos por motivos políticos, ideológicos o de creencia religiosa de acuerdo con lo dispuesto en el artículo 2 de la presente Ley.
3. Igualmente, se declaran ilegítimas, por vicios de forma y fondo, las condenas y sanciones dictadas por motivos políticos, ideológicos o de creencia por cualesquiera tribunales u órganos penales o administrativos durante la Dictadura contra quienes defendieron la legalidad institucional anterior, pretendieron el restablecimiento de un régimen democrático en España o intentaron vivir conforme a opciones amparadas por derechos y libertades hoy reconocidos por la Constitución.

³⁴⁵ Desconocemos por qué no se incluyó, por tanto, entre las finalidades y usos previstos para el fichero, la de facilitar a descendientes directos de las víctimas la indagación, localización e identificación de las personas desaparecidas violentamente durante la Guerra Civil o la represión política posterior y cuyo paradero se ignore, según lo dispuesto en los artículos del 11 a 13 de la Ley 52/2007, de 26 de diciembre.

Como vemos, la forma en que fue declarado el fichero es altamente mejorable, especialmente en lo que se refiere a su finalidad y los usos previstos para el mismo, así como a las personas o colectivos sobre los que se pretende obtener datos de carácter personal³⁴⁶. Circunstancia tampoco muy importante dado el reducido –y amparado legalmente– ámbito de cesión que se contempla. El problema vino cuando se pretendió difundir el fichero a través de una base de datos accesible en línea a cualquier persona a través de la Red, en el citado Portal de Víctimas de la Guerra Civil y Represaliados del Franquismo.

4.4.2. El Portal de Víctimas de la Guerra Civil y Represaliados del Franquismo

Mediante oficio de 22 de abril de 2010 –véase nuestro Anexo 2–, el Subdirector General de los Archivos Estatales solicitó a la Agencia Española de Protección de Datos informe jurídico sobre la posibilidad de publicar en la Red una base de datos con las víctimas de la Guerra Civil y la represión de la Dictadura franquista que aparecen en los documentos de los Archivos Estatales (esto es, un fichero de autoridades³⁴⁷ sobre este tipo de personas), incluidos “los datos personales que referencien expedientes posteriores a 1960”³⁴⁸.

El informe de la AEPD emitido al respecto (Informe de 25 de mayo de 2010, del Gabinete Jurídico de la Agencia Española de Protección de Datos, ref. de entrada 142746/2010) –véase Anexo 3– es lo bastante significativo para ayudarnos a comprender la problemática de la aplicación de la normativa de protección de datos a los sistemas de descripción archivística, especialmente aquellos accesibles por Internet.

³⁴⁶ Por ejemplo –conectando la finalidad del fichero con la Ley de Memoria Histórica– indicando en este apartado a las “personas que aparecen en los documentos y que pueden ser causantes o titulares de derechos a los efectos de la Ley 52/2007, o de interés para la recuperación de su memoria personal y, por extensión, de la memoria histórica”.

³⁴⁷ La norma ISAAR-CPF define “registro de autoridad” como la “[f]orma autorizada del nombre, combinada con otros elementos informativos que permiten identificar y describir la entidad mencionada y que pueden también remitir a otros registros de autoridad relacionados” (ICA 2004, p. 12). Un fichero de autoridades sería “el conjunto organizado de todos los registros de autoridad” (véase, por ejemplo, Ortego de Lorenzo-Cáceres, P.; Bonal Zano, J.L. 1999. El control de autoridades y la normalización de los puntos de acceso en los archivos. *Tábula*, 4, pp. 41-68).

³⁴⁸ Y, por tanto, de consulta restringida de acuerdo con el art. 57.1.c de la LPHE.

Llama la atención que casi la mitad del informe esté dedicado a delimitar el ámbito sobre el que le corresponde informar a la Agencia, a raíz de la consulta planteada. Que no es otro que la legalidad -conforme a la normativa de protección de datos- de la cesión de datos de carácter personal expresada en la consulta, cuando dichos datos procedan de personas físicas vivas.

Tras esta larga introducción, la AEPD comienza su análisis jurídico comprobando, en primer lugar, si la difusión de estos datos sin el consentimiento de los afectados está amparada por la LOPD. Al no tratarse de datos recogidos de fuentes accesibles al público -con independencia de que algunos de los datos hayan aparecido en determinadas publicaciones³⁴⁹-, el informe procede a "analizar si existe una norma con rango de Ley que habilita la cesión derivada de la publicación a la que se refiere la consulta" (p. 6), como permite el art. 11.2.a LOPD.

Para ello, parte de la premisa de que la publicación de los datos en el Portal "no ha de entenderse en términos similares al acceso a la documentación contenida en los archivos públicos" (p. 6). Esta idea ya la había avanzado en la primera parte del Informe, donde observaba (p. 2) que "es preciso diferenciar entre el derecho de acceso a la documentación vinculada con los mencionados expedientes del tratamiento de datos que supondrá la inserción de los datos personales en el portal al que se refiere la consulta". Una de las implicaciones de esta diferencia es, a juicio de la Agencia, que la accesibilidad legal de los documentos no es relevante "para determinar la legitimación para el tratamiento de los datos efectuado mediante la inserción de los mismos en el portal".

Dicho esto, las dos normas que a juicio de la AEPD podrían invocarse para la habilitación serían la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español, concretamente su artículo 57³⁵⁰; y la Ley 52/2007, de

³⁴⁹ Concretamente los de los inculcados por el Tribunal de Orden Público (TOP) en: Águila Torres, J.J. del. 2001. *El Top: La represión de la libertad (1963-1977)*. Barcelona: Planeta; y en Gómez Alén, J. y Vega, R. 2007. *Las sentencias del Tribunal de Orden Público. TOPDAT: una base de datos para explotar*. Oviedo: Universidad, Consejería de Justicia del Gobierno del Principado de Asturias.

³⁵⁰ Artículo 57.

26 diciembre, por la que se reconocen y amplían derechos y se establecen medidas en favor de quienes padecieron persecución o violencia durante la guerra civil y la dictadura³⁵¹ (en adelante, LMH), en concreto su artículo 22³⁵². En ambos casos, la Agencia considera que no se pueden considerar normas legitimadoras del tratamiento de datos que se pretende, ya que estas normas “regula[n] el derecho a acceder a los documentos, pero no autoriza[n] ni legitima[n] la difusión universal de los datos asociados a su contenido a cualquier persona, tenga o no interés en conocer dicho contenido” (p. 9).

En segundo lugar, el Informe señala que la publicación de los datos en el Portal “deberá respetar el principio de proporcionalidad consagrado por el artículo 4.1 de la Ley Orgánica 15/1999” (p. 7), según el cual, como hemos señalado reiteradamente, los datos de carácter personal sólo se podrán someter a tratamiento cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas,

1. La consulta de los documentos constitutivos del Patrimonio Documental Español a que se refiere el artículo 49.2 se atenderá a las siguientes reglas:

a) Con carácter general, tales documentos, concluida su tramitación y depositados y registrados en los Archivos centrales de las correspondientes entidades de Derecho Público, conforme a las normas que se establezcan por vía reglamentaria, serán de libre consulta a no ser que afecten a materias clasificadas de acuerdo con la Ley de Secretos Oficiales o no deban ser públicamente conocidos por disposición expresa de la Ley, o que la difusión de su contenido pueda entrañar riesgos para la seguridad y la defensa del Estado o la averiguación de los delitos.

b) No obstante lo dispuesto en el párrafo anterior, cabrá solicitar autorización administrativa para tener acceso a los documentos excluidos de consulta pública. Dicha autorización podrá ser concedida, en los casos de documentos secretos o reservados, por la Autoridad que hizo la respectiva declaración, y en los demás casos por el Jefe del Departamento encargado de su custodia.

c) Los documentos que contengan datos personales de carácter policial, procesal, clínico o de cualquier otra índole que puedan afectar a la seguridad de las personas, a su honor, a la intimidad de su vida privada y familiar y a su propia imagen, no podrán ser públicamente consultados sin que medie consentimiento expreso de los afectados o hasta que haya transcurrido un plazo de veinticinco años desde su muerte, si su fecha es conocida o, en otro caso, de cincuenta años, a partir de la fecha de los documentos.

2. Reglamentariamente se establecerán las condiciones para la realización de la consulta de los documentos a que se refiere este artículo, así como para la obtención de reproducciones de los mismos.

³⁵¹ Conocida como Ley de la Memoria Histórica (BOE de 27 de diciembre).

³⁵² Artículo 22. Derecho de acceso a los fondos de los archivos públicos y privados.

1. A los efectos de lo previsto en esta Ley, se garantiza el derecho de acceso a los fondos documentales depositados en los archivos públicos y la obtención de las copias que se soliciten.

2. Lo previsto en el apartado anterior será de aplicación, en sus propios términos, a los archivos privados sostenidos, total o parcialmente, con fondos públicos.

3. Los poderes públicos adoptarán las medidas necesarias para la protección, la integridad y catalogación de estos documentos, en particular en los casos de mayor deterioro o riesgo de degradación.

explícitas y legítimas para las que se hubieron obtenido. El propio Ministerio señaló en su solicitud de informe las finalidades del fichero: "por un lado, la educación y la cultura; por otro, la comunicación de datos a los descendientes directos y afectados por la Ley de Memoria Histórica con vista a los distintos derechos establecido en su articulado" (p.7).

Así pues, las normas que se invoquen para habilitar la publicación de los datos en el Portal deberían recoger o permitir las finalidades señaladas (subordinación de la habilitación legal al principio de proporcionalidad). Por ello, y a pesar de que -como se vio en el punto anterior-, el art. 22 de la LMH no habilita para la cesión de los datos, la Agencia, en un intento por crear doctrina en la materia, se ocupa de analizar (pp. 9-10) "si en caso de venir esa norma [la Ley 52/2007 en su artículo 22] referida no a los documentos obrantes en los archivos, sino a los datos personales de los propios interesados, la misma otorgaría cobertura a la cesión" (p.9).

La finalidad en este caso vendría definida en el art. 1 de la Ley 52/2007:

Artículo 1. Objeto de la Ley

1. La presente Ley tiene por objeto reconocer y ampliar derechos a favor de quienes padecieron persecución o violencia, por razones políticas, ideológicas, o de creencia religiosa, durante la Guerra Civil y la Dictadura, promover su reparación moral y la recuperación de su memoria personal y familiar, y adoptar medidas complementarias destinadas a suprimir elementos de división entre los ciudadanos, todo ello con el fin de fomentar la cohesión y solidaridad entre las diversas generaciones de españoles en torno a los principios, valores y libertades constitucionales.

2. Mediante la presente Ley, como política pública, se pretende el fomento de los valores y principios democráticos, facilitando el conocimiento de los hechos y circunstancias acaecidos durante la Guerra civil y la Dictadura, y asegurando la preservación de los documentos relacionados con ese período histórico y depositados en archivos públicos.

Con respecto a la finalidad establecida en el art. 1.1, el informe se centra únicamente en la declaración de reparación y reconocimiento personal, concluyendo que "cuando se trate de personas no fallecidas será únicamente el interesado quien podrá solicitar la declaración a la que el precepto se refiere, por lo que el acceso a los datos por parte de los

restantes sujetos [...] no será relevante para obtener el reconocimiento y reparación establecidos en la Ley” (p. 10). En segundo lugar, trata sobre el posible amparo legal a partir de la finalidad establecida en el art. 1.2 (fomentar los valores y principios democráticos y facilitar el conocimiento de los hechos y circunstancias acaecidos durante la Guerra civil y la Dictadura), descrita en la consulta del Ministerio como “la educación y la cultura”. En este caso, la Agencia va mucho más allá del propósito inicial de analizar la cuestión únicamente “desde el punto de vista de las normas de protección de datos” (p. 1), para decidir qué es relevante para la educación y la cultura, afirmando que “lo relevante a tal efecto no son los datos personales concretos de la totalidad de las personas relacionadas con los expedientes, sino las causas que pretendieron justificar su tramitación o incluso las circunstancias en que el procedimiento se desarrollo [sic]”. Por ello, concluye finalmente que “la inclusión de los datos personales de un interesado sin recabar su consentimiento [...] resultaría excesiva para el cumplimiento de la finalidad de “educación y cultura” pretendida por la Ley 52/2007” (p. 10). Por tanto,

la inclusión de sus datos [refiriéndose a los datos de personas no fallecidas] en el portal únicamente debería llevarse a cabo con su consentimiento, no siendo posible, sin más, dicha inclusión en los términos previstos en la consulta, dado que, sin perjuicio de la existencia o inexistencia de una merma del derecho a la intimidad de los interesados, se estaría produciendo una vulneración de su derecho fundamental a la protección de datos de carácter personal”

Por último, y en relación con lo dicho en el punto anterior, debemos destacar que la Agencia, a pesar de que podría considerarse que es una cuestión en buena parte ajena al estricto ámbito de actuación que delimitó al inicio, se pronuncia con respecto al derecho de acceso establecido en el artículo 22 de la Ley 52/2007. Considera el Informe que la inclusión en dicho artículo de la expresión “a los efectos de lo previsto en esta Ley” implica que “este derecho a conocer los documentos [...] se encuentra [...] limitado en cuanto a la finalidad que lo justifica, que deberá derivar directamente de los dispuesto en la propia Ley 52/2007” y, por tanto, “el acceso a los documentos [a tenor de dicho artículo] no será ilimitado sino que debe tener por objeto la obtención de las medidas de reconocimiento y compensación establecidas en la propia Ley o la divulgación de los hechos acaecidos en los períodos a los que la misma se refiere” (p. 8).

A partir de esta argumentación jurídica, la Agencia establece sus conclusiones, señalando que

desde la perspectiva de la aplicación de las normas de protección de datos de carácter personal, sólo será posible la publicación en el portal al que se refiere la consulta de los datos relativos a las personas que tengan la condición de víctimas de la Guerra Civil o represaliados del Franquismo, y en particular, los vinculados con los sumarios tramitados por los Juzgados y Tribunales de Orden Público si se cumplen las siguientes condiciones:

- 1) Que se trate de personas fallecidas, debiendo contrastarse los datos que obren en poder de la consultante con los resultantes de otros registros que permitan acreditar esta circunstancia cuando sea necesario.
- 2) Tratándose de personas no fallecidas, que se haya obtenido el consentimiento de los interesados para que sus datos sean incluidos en el portal, debiendo informarse al interesado de todos los extremos relacionados con ese tratamiento en los términos previstos por el artículo 5 de la Ley Orgánica 15/1999.
- 3) En caso de no contarse con el consentimiento, la información que conste en el portal en relación con las personas que no lo hubieran prestado deberá constar de forma dissociada, de forma que no resulte posible identificar directa o indirectamente al interesado.

Dejando a un lado el resto del informe, no podemos estar de acuerdo con estas conclusiones. Creemos que la Agencia olvidó invocar como norma que podría habilitar esta cesión a la Ley 30/1992 (LPAC). El artículo 37.9 de la misma establece que será objeto de periódica publicación la relación de los documentos obrantes en poder de las Administraciones Públicas sujetos a un régimen de especial publicidad por afectar a la colectividad en su conjunto y cuantos otros puedan ser objeto de consulta por los particulares. De esta forma, podría ligarse la difusión de los datos con la accesibilidad de los documentos de los que proceden³⁵³, algo que la Agencia rechaza de inicio: si un documento puede ser objeto de consulta por los particulares, también puede publicarse su referencia archivística. Y no de forma dissociada, ya que el principal punto de acceso a las

³⁵³ La AEPD daba por sentado que la cesión no podía entenderse en los mismo términos que el acceso a la documentación contenida en los archivos públicos. En nuestra opinión, esta circunstancia es fundamental para que la cesión sea proporcionada y no excesiva.

descripciones de este tipo de documentos ha de ser, necesariamente, onomástico.

Además, puede argumentarse que la proporcionalidad de la cesión viene dada por el interés público que está detrás de la difusión de los datos, que no es sino fomentar los valores y principios democráticos y facilitar el conocimiento de los hechos y circunstancias acaecidos durante la Guerra Civil y la Dictadura (art. 1.2 LMH), empleando para ello un sistema de descripción archivística que permite localizar e identificar, a partir de los nombres de las víctimas, los documentos necesarios para alcanzar dicho conocimiento.

Por otro lado, el nivel de publicidad que supone el Portal en relación con otros supuestos de "difusión universal de los datos en Internet" no es tan alto, ya que los datos incluidos en este sistema de descripción archivística pertenecen a la llamada "Web profunda" y no son indizados por buscadores como Google.

En definitiva, creemos que la difusión de descripciones³⁵⁴ referidas a unidades documentales de libre consulta (por haber transcurrido los plazos establecidos en el art. 57.1.c LPHE) no tiene por qué contradecir a priori la normativa de protección de datos, aunque se refiera a personas vivas, ya que existe habilitación legal para hacerlo. Sería necesario, no obstante, someter a un juicio de proporcionalidad los proyectos que se quieran sacar a la luz para comprobar la idoneidad de los mismos. Una idoneidad que, en el caso que hemos expuesto, estaría más que justificada.

³⁵⁴ Bien de documentos de archivo, agentes (como en este caso) o cualquier otro tipo de entidad archivística

5. LAS MEDIDAS DE SEGURIDAD COMO FUNCIÓN ARCHIVÍSTICA

5.1. Modelo básico de responsabilidades del archivo en materia de seguridad

El artículo 9 de la LOPD exige, como tuvimos ocasión de estudiar anteriormente, la adopción de las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos de carácter personal y evite su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana del medio físico o natural. Dichas medidas, reguladas en el Título VII del Reglamento de 2007 (arts. 79 a 114) tratan de proteger los activos o recursos que componen los sistemas de información en que se integran los ficheros de datos, así como de definir los requisitos que afectan a los distintos agentes que participan en la gestión y uso de dichos sistemas de información. Entre estas medidas, destacan –como vimos– las referidas al control de acceso a dichos sistemas de información y la gestión de documentos y soportes.

A partir del análisis que realizamos anteriormente, podemos proponer un modelo básico de las responsabilidades del archivo con respecto a las mismas:

- Identificar los requisitos generales de seguridad del sistema o los sistemas de gestión de documentos de la organización, así como de los sistemas de información exclusivos del archivo que contengan datos de carácter personal afectados por esta normativa. Y colaborar, en este sentido, con otros servicios o unidades de la organización, en lo

referido a sus sistemas de información que se nutran de datos procedentes de documentos de archivo.

- Definir y controlar la implantación de las medidas de seguridad exigibles en dichos sistemas. Especialmente en lo referido a las medidas necesarias para el control del acceso a los mismos y a los recursos que los integran; y a la política de "gestión de soportes y documentos" de la organización. Del mismo modo, podría considerarse la posibilidad -en el caso de que dichos sistemas requieran medidas de seguridad media o alta-, de que el archivo o, más bien, el archivero o la archivera designado/a al efecto, ejerza de responsable de seguridad de los mismos.
- Llevar a cabo las auditorías internas de dichos sistemas y colaborar en la ejecución de las externas.
- Integrar las cuestiones de seguridad y acceso requeridas en la normativa de protección de datos en los programas de formación en materia de gestión de documentos que sean responsabilidad del archivo.

Esto supone ir más allá de concepciones finalistas del archivo, en sintonía con lo promulgado por la Archivística española actual, que contempla como propia -aunque no exclusiva de los archiveros- la gestión de los documentos desde su creación. Las normas ISO 15.489 ofrecen criterios de seguridad y acceso para implantar en los sistemas de información que se ocupan de los documentos de archivo (sistemas de gestión de documentos de archivo o SGDA) que son coincidentes, en cierta manera, con los que requiere la normativa de protección de datos de carácter personal, y que permiten desarrollar ese modelo básico de intervención que esbozábamos arriba.

5.2. Seguridad y acceso en las normas ISO 15.489

De acuerdo con las normas ISO 15.489, entre las funcionalidades que debe contemplar un SGDA se encuentra la implantación de medidas de seguridad y el control de acceso para garantizar que no peligre la integridad del propio sistema³⁵⁵ ni la de los documentos³⁵⁶ y para cumplir con los derechos y restricciones establecidos³⁵⁷. Conseguir, en definitiva, un control de acceso y un nivel de seguridad apropiados³⁵⁸.

Los controles de acceso apropiados se garantizan mediante la asignación de un nivel de acceso tanto a los documentos como a los individuos (ISO 15489-1:2001, 9.7). El instrumento básico para llevar a cabo este control es el cuadro o tabla de acceso y seguridad -según la norma es uno de los principales instrumentos usados en las operaciones de gestión de documentos, junto con el cuadro de clasificación y el calendario de conservación-. Para su elaboración y aplicación se requieren, además, otras herramientas no específicas de la gestión de documentos cuyo

³⁵⁵ ISO 15489-1:2001, 8.2.3. *Deberían aplicarse medidas para controlar el acceso, la identificación del usuario, la destrucción autorizada y la seguridad, con la finalidad de evitar el acceso, la destrucción, la modificación o la eliminación de documentos sin autorización. Estas medidas de control pueden formar parte del sistema de gestión de documentos o ser externas al mismo.*

³⁵⁶ ISO 15489-1:2001, 8.3.6. *Los sistemas [de gestión de documentos] deberían incluir y aplicar controles de acceso para garantizar que no peligre la integridad de los documentos. Además, deberían proporcionar y mantener pistas de auditoría u otros métodos de seguimiento que demuestren que los documentos están protegidos frente a la utilización, la modificación y la destrucción no autorizadas.*

³⁵⁷ ISO/TR 15489-2:2001, 4.2.5.2. *El acceso a los documentos puede estar restringido para proteger: la información personal y la intimidad; los derechos de propiedad intelectual y el secreto comercial; la seguridad de los bienes(físicos o financieros); la seguridad pública; y los privilegios legales y profesionales.*

Igual importancia revisten los derechos de acceso legalmente reconocidos en virtud de las normas de buen gobierno, la libertad de información, la protección de la intimidad, el ordenamiento jurídico y la legislación archivística.

³⁵⁸ Seguridad apropiada (ISO/TR 15489-2:2001, 4.2.5.2): nivel de seguridad que, según el sentido común, se necesitaría para proteger la información de cualquier acceso, recopilación, uso, divulgación, borrado, modificación o destrucción sin autorización.

desarrollo “está fuera del alcance de esta parte de la Norma ISO 15489” (ISO/TR 15489-2:2001, 4.2.1): un análisis del marco normativo, en este caso, centrado en las normas que afectan al acceso a los documentos y la seguridad de la información; un análisis de riesgos; una relación de asignación de responsabilidades en la organización; y un registro de los empleados y de los permisos de usuario del sistema.

Por lo que se refiere al análisis del marco normativo de la organización en materia de acceso a los documentos y seguridad de la información, la norma señala que ha de tenerse en cuenta (ISO 15489-1:2001, 9.7):

- El marco reglamentario en el que la organización realiza sus actividades, que puede establecer una serie de principios generales sobre los derechos, condiciones y restricciones de acceso que deberían aplicarse en el funcionamiento de los sistemas de gestión de documentos; y
- La legislación específica sobre áreas como la privacidad, la seguridad, la libertad de información y los archivos. Los documentos pueden contener información sensible de tipo personal, comercial u operativa. En algunos casos, no se debería permitir el acceso a los documentos o la obtención de información sobre los mismos.

De acuerdo con lo dicho, los SGDA de las organizaciones españolas diseñados conforme a las normas ISO 15.489:2001 habrán tener en cuenta las disposiciones establecidas en la LOPD y su Reglamento, e implementar las medidas de seguridad que recoge éste, que tendrán que plasmarse en la tabla o cuadro de acceso y seguridad del sistema.

La tabla de acceso y seguridad es el instrumento formal de identificación de los derechos de acceso y del régimen de restricciones aplicables a los documentos (ISO/TR 15489-2:2001, 4.2.5.1). Para su elaboración, la norma describe de forma bastante somera una metodología (ISO/TR 15489-2:2001, 4.2.5.2) que parte –como señalábamos antes- del análisis previo del marco normativo de la organización, de la actividad de la organización y de la evaluación de riesgos, para realizar una clasificación

de categorías de documentos en función de sus restricciones de acceso y condiciones de seguridad. Para ello, se identifican los siguientes procesos:

- a) identificar los derechos y restricciones legalmente reconocidos en materia de acceso a los documentos y a la información de la organización;
- b) identificar las áreas de riesgo de violación de la intimidad y de la confidencialidad comercial, profesional o personal;
- c) identificar las cuestiones de seguridad de la organización;
- d) clasificar las áreas de riesgo de violación de la seguridad de acuerdo con la probabilidad de que suceda y con la evaluación de los daños;
- e) relacionar las áreas de riesgo identificadas y las cuestiones de seguridad con las actividades de la organización;
- f) identificar los niveles de restricción adecuados, desde las áreas de mayor riesgo a las de menor riesgo;
- g) asignar niveles de restricción a las diferentes clases de documentos de acuerdo con la clasificación de los riesgos; y
- h) asociar las restricciones a instrumentos, como los cuadros de clasificación o los tesauros que se usan para describir los documentos. De este modo, las advertencias y restricciones pueden mostrarse automáticamente al incorporar y registrar documentos en el sistema de gestión.

Como señala la propia norma (ISO/TR 15489-2:2001, 4.3.5),

El acceso a los documentos se restringe únicamente cuando así lo requiere la ley o lo imponen las necesidades de la organización. Las categorías de acceso y de seguridad pueden asignarse mediante consulta a la unidad de la organización a la que pertenecen los documentos. Para garantizar que los mecanismos de control y supervisión adicionales que afectan a estos documentos no estén vigentes más tiempo del necesario, se pueden establecer plazos de restricción claramente definidos³⁵⁹.

Otro instrumento necesario para el control de acceso, aunque no específico de la gestión de documentos, es el llamado registro de permisos de usuario, que supone, para el caso que nos ocupa, una categorización de los usuarios en función de sus derechos de acceso³⁶⁰. La norma no establece una metodología para su elaboración, pero su lectura permite

³⁵⁹ Como realizan, por ejemplo, algunas de las normas que regulan el derecho de acceso a los documentos públicos.

³⁶⁰ “Un sistema de gestión de documentos ha de gestionar permisos de usuario que le son propios. Puede utilizarse el registro general de empleados y de permisos de usuario de la organización, pero en los casos que no exista, se tendrá que concebir uno propio. Este registro distingue los permisos de usuario para el acceso, la modificación o eliminación de los documentos, de los [...] de aquellos de sólo lectura” (ISO/TR 15489-2:2001, 4.2.5.2).

reconocer los siguientes procesos: identificar las necesidades de acceso de las distintas áreas funcionales de la organización³⁶¹; identificar distintos perfiles de usuario; identificar los usuarios que tienen acceso a grupos concretos de documentos; asignar perfiles de usuario a los usuarios, teniendo en cuenta que "las restricciones de acceso pueden aplicarse tanto dentro de la organización como a usuarios externos" (ISO 15489-1:2001, 9.7); y asignar permisos de usuario de acuerdo con los distintos perfiles y los derechos de acceso específicos de los usuarios. El control y cotejo entre los permisos de usuario y las responsabilidades vinculadas a las funciones es un proceso constante en todos los sistemas de gestión de documentos (ISO 15489-1:2001, 9.7), ya que estos, al igual que las restricciones a la accesibilidad, pueden variar con el paso del tiempo.

Los procesos y controles de acceso que establecen las normas ISO 15.489 consisten, por tanto, en aplicar a cada documento las condiciones de acceso correspondientes a su clase de acuerdo con la tabla de acceso y seguridad; y permitir a cada usuario el acceso y uso de los mismos de acuerdo con dichas condiciones y los permisos que tienen asignados en el registro de permisos de usuario.

De esta manera, la gestión del proceso de acceso debería garantizar que (ISO 15489-1:2001, 9.7):

- a) los documentos se dividen en categorías de acuerdo con su nivel de acceso en un momento dado;
- b) los documentos sólo se entregan a aquellas personas que estén autorizadas a verlos;
- c) los documentos encriptados pueden leerse cuando así se requiera y autorice;
- d) los procesos y las operaciones relacionados con los documentos sólo son realizados por quienes están autorizados; y
- e) las unidades de la organización responsables de una función concreta atribuyen los permisos de acceso a los documentos de su área de responsabilidad.

Para ello, cuando un documento se incorpora al SGD, se debería (ISO/TR 15489-2:2001, 4.3.5):

³⁶¹ "El modo en que se expresan los niveles de restricción debería reflejar la práctica de la organización. Las áreas de la organización pertinentes deberían ser consultadas a la hora de desarrollar las categorías de restricción del acceso. [...] puede que no resulte adecuado permitir el acceso a los documentos de ciertas actividades de la organización fuera del grupo funcional que las desarrolla y se restrinjan los permisos de los usuarios fuera de este grupo" (ISO/TR 15489-2:2001, 4.2.5.2).

- a) identificar la operación o actividades que el documento atestigua;
- b) identificar la unidad de la organización a la que pertenece el documento;
- c) verificar las categorías de acceso y seguridad asignadas para determinar si la actividad y el área de la organización han sido identificadas como áreas de riesgo, o se les han atribuido consideraciones de seguridad o restricciones por imperativo legal;
- d) asignar al documento un nivel adecuado de acceso o restricción y especificar los mecanismos de control apropiados para su manipulación; y
- e) registrar en el sistema de gestión de documentos la categoría de acceso o de seguridad del documento para establecer, si es necesario, medidas de control adicional

Así mismo, cuando se disponga su eliminación, deberían emplearse métodos acordes con su nivel de confidencialidad (ISO/TR 15489-2:2001, 4.3.9.3).

Además, la norma ISO 15.489 destaca la importancia del control de acceso y la seguridad para determinar la gestión del almacenamiento e instalación de los documentos³⁶² y, especialmente, su uso. La gestión del uso de los documentos comprende (ISO/TR 15489-2:2001, 4.3.8):

- a) la identificación de los permisos de usuario asociados con los diferentes individuos y sus respectivos puestos dentro de la organización;
- b) la identificación de las condiciones de acceso y de seguridad de los documentos;
- c) la identificación de los derechos de acceso de personas ajenas a la organización;
- d) la garantía de que sólo las personas que tienen el perfil de usuario adecuado o que cuenten con los derechos de acceso pertinentes tienen acceso a los documentos restringidos;
- e) la trazabilidad de los documentos para identificar a las personas que han tenido o tienen la custodia de los mismos;
- f) la garantía de que todo uso de los documentos se registra con el nivel de detalle adecuado; y
- g) la revisión de las categorías de acceso asignadas a los documentos para garantizar su actualización y aplicabilidad.

³⁶² "Las condiciones de almacenamiento y los procesos de manipulación deberían diseñarse con el objetivo de proteger los documentos contra el acceso y la destrucción no autorizados, la pérdida, el robo y las catástrofes" (ISO 15489-1:2001, 9.6). "La elección de las condiciones de almacenamiento debería tener en cuenta los requisitos y restricciones en materia de acceso y de seguridad además de las características físicas de los documentos. [...] Entre los factores importantes a la hora de seleccionar las condiciones de almacenamiento y manipulación, se incluyen [...] las necesidades de seguridad y confidencialidad de los documentos. El acceso a algunos documentos está limitado por razones de confidencialidad, propiedad, naturaleza de la información o protección legal" (ISO/TR 15489-2:2001, 4.3.7.1).

Merece una mención especial la gestión de la trazabilidad de los documentos, esto es, la implantación de un sistema de supervisión del uso o movimiento de los mismos mediante la creación, incorporación y conservación de información sobre estos procesos. La norma reconoce su necesidad para supervisar el uso en relación con la seguridad y el mantenimiento de los sistemas, así como para mantener una pista de auditoría de las operaciones relacionadas con la gestión de documentos, entre las que se incluye el acceso y el uso de los documentos (ISO 15489-1:2001, 9.8.1)³⁶³. De hecho, la propia norma destaca su importancia para la protección de datos de carácter personal (ISO/TR 15489-2:2001, 4.3.8):

La trazabilidad de los documentos en un sistema de gestión de documentos es una medida de seguridad para las organizaciones. Garantiza que sólo los usuarios con los permisos adecuados realizan tareas para las que han sido autorizados. El grado de control y el nivel de detalle de registro en el sistema de gestión de documentos depende de la naturaleza de las actividades y de los documentos que generan. Por ejemplo, en muchos casos el ordenamiento jurídico establece medidas obligatorias de protección de la privacidad que exigen que se registre el uso de de los documentos que contengan información personal.

Por último, estas normas recogen también los requisitos relativos a la auditoría de los SGDA (ISO 15489-1:2001, 10; ISO/TR 15489-2:2001, 5) y al programa de formación en materia de gestión de documentos (ISO 15489-1:2001, 11; ISO/TR 15489-2:2001, 6).

Como hemos visto, las normas ISO 15.489 ofrecen un marco para implementar medidas de seguridad y acceso en los sistemas de información basados en documentos de archivo, que se ajusta a lo exigible en la normativa de protección de datos. El desafío para los archivos –en especial para los que constituyen nuestro ámbito de análisis– reside, por tanto, en asumir las responsabilidades que pudieran corresponderle en

³⁶³ “Los sistemas de supervisión del uso o movimiento de los documentos van desde los sistemas físicos de registro en tarjetas, hasta la tecnología de códigos de barras o sistemas de gestión de documentos electrónicos en los que la visualización de un documento se incorpora automáticamente como una operación del sistema” (ISO/TR 15489-2:2001, 4.3.8).

este sentido, ya que cuenta con los conocimientos, la metodología y, en muchos casos, los medios apropiados para hacerlo³⁶⁴.

³⁶⁴ Quizás una futura ley de archivos, como la que hemos reclamado en otros capítulos, podría impulsar este papel de los archivos de la AGE en la protección de datos de carácter personal.

6. CONCLUSIONES

Como resultado del estudio que hemos llevado a cabo a lo largo de las páginas anteriores, podemos extraer una serie de conclusiones generales que vienen a cumplir con el objetivo propuesto de analizar el impacto del derecho a la protección de datos en los archivos públicos, especialmente en los de la Administración General del Estado.

1. Consideramos que la normativa de protección de datos afecta de forma amplia al funcionamiento de los archivos de la AGE. Su impacto se deja notar tanto en las funciones administrativas (tratamientos llevados a cabo para gestionar los recursos humanos y la relación con los usuarios) como en las técnicas (tratamiento de los documentos que contengan datos de carácter personal).
2. Para delimitar esta zona de impacto, nos alineamos con la teoría totalizadora, según la cual, para que entre en juego el régimen de la LOPD es absolutamente necesario que los tratamientos de datos se refieran a ficheros, tal y como los define dicha ley. Para ello, nos apoyamos tanto en el análisis de dicha definición y, en general, del objeto del derecho a la protección de datos; como en la opinión que, refiriéndose expresamente a distintos tipos de documentos de archivo³⁶⁵, ha expresado la doctrina jurídica, las autoridades de control y, finalmente, la jurisprudencia del Tribunal Supremo en torno al caso de los Libros de Bautismo.
3. En el caso de los documentos de archivo –y, de acuerdo con dicha teoría-, consideramos que la legislación de protección de datos afecta a

³⁶⁵ Especialmente, los documentos y expedientes administrativos que constituyen el principal objeto de atención de los archivos de la AGE.

determinadas series cuyos documentos contengan datos de carácter de personal de personas vivas: con carácter general, las series de documentos electrónicos; respecto de las series en papel, las ordenadas físicamente a partir de criterios personales -series de expedientes personales (expedientes evolutivos) y series de expedientes procedimentales o resolutivos referidos a personas (expedientes de caso particular)-, así como las que cuenten con instrumentos que permitan su recuperación a través de dichos criterios.

4. Una vez delimitados los conjuntos de datos sobre los que se realizan tratamientos sujetos al régimen de la protección de datos, creemos que resulta necesario identificarlos en términos de fichero. El análisis habrá de contemplar tanto los datos incorporados a los sistemas de información propios del archivo (creados o adquiridos por el mismo) como al resto de sistemas de su organización que hagan referencia a los documentos que son su objeto de gestión.
5. De esta forma, los archivos podrán dar cumplimiento a las exigencias legales que afectan a los tratamientos sujetos a la normativa de protección de datos:
 - o Creación y declaración de los ficheros sobre los que se realizan dichos tratamientos, mediante disposición general (Orden Ministerial en el caso de los órganos centrales de la AGE) publicada en el BOE; e inscripción en el Registro General de Protección de Datos.
 - o Adopción de medidas destinadas a facilitar el ejercicio por parte de los ciudadanos de los distintos derechos reconocidos por la normativa de protección de datos (y los deberes que conllevan para los archivos), en especial los de acceso, rectificación, cancelación y oposición -con las excepciones y peculiaridades aplicables en cada caso.
 - o Sujeción de los tratamientos que se realicen a los principios de la protección de datos (calidad, consentimiento y finalidad), con las especiales condiciones -menos estrictas- establecidas para los ficheros públicos.

- Implantación de las medidas de seguridad adecuadas, que deberán adaptarse a la mayor o menor sensibilidad de los datos.
6. Respecto a estas exigencias, se han advertido distintas deficiencias que presentan, actualmente, algunos tratamientos de datos que realizan los archivos de la AGE. A lo largo del trabajo se han propuesto medidas para solucionar algunas de estas deficiencias en casos específicos - pertenecientes a archivos gestionados por el Ministerio de Cultura pero que pueden servir de orientación al resto de los archivos de la AGE-. Estos se refieren a:
- Los procesos de gestión de usuarios, especialmente durante las operaciones de recogida de datos.
 - La forma de declarar los ficheros, refiriéndonos expresamente a los ficheros "Gestión General de Archivos Estatales" y "Guerra Civil y Franquismo".
 - La difusión en la Red de los sistemas de descripción archivística, defendiendo en este caso -contra la opinión de la AEPD-, a través del caso del "Portal de Víctimas de la Guerra Civil y Represaliados del Franquismo" que existe una conexión entre la posibilidad de acceso a los documentos referenciado -de conformidad con la legislación vigente en la materia- y la comunicación de los datos presentes en las descripciones de los mismos.
7. Por último, proponemos un modelo de responsabilidades que pueden asumir los archivos en materia de seguridad, para las que cuentan con un marco de aplicación definido en las normas ISO 15.489 de gestión de documentos:
- Identificar los requisitos generales de seguridad del sistema o los sistemas de gestión de documentos de la organización, así como de los sistemas de información propios del archivo que contengan datos de carácter personal afectados por esta normativa. Y colaborar, en este sentido, con otros servicios o unidades de la organización, en lo referido a sus sistemas de información que referencien, afecten o incluyan a documentos de archivo.
 - Definir y controlar la implantación de las medidas de seguridad exigibles en dichos sistemas. Especialmente en lo referido al control del acceso a los mismos y a los recursos que los integran (sobre

todo a los documentos) y a la política de "gestión de soportes y documentos" de la organización. Del mismo modo, podría considerarse la posibilidad -en el caso de que dichos sistemas requieran medidas de seguridad media o alta-, de que el archivo o, más bien, el archivero designado al efecto, ejerza de responsable de seguridad de los mismos.

- Llevar a cabo las auditorías internas de dichos sistemas y colaborar en la ejecución de las externas.
- Integrar las cuestiones de seguridad y acceso requeridas en la normativa de protección de datos en los programas de formación en materia de gestión de documentos que sean responsabilidad del archivo.

Bajo este esquema, los archivos pueden estar llamados a adquirir un peso importante como agentes destinados a proteger los datos personales tratados por la Administración. Para ello, es necesario que abandonen el papel marginal al que se han visto relegados. Debido especialmente a la ausencia, en la Administración General del Estado, de una política integral de gestión de documentos configurada en torno a un sistema de archivos verdaderamente articulado y sin las disfunciones y asimetrías que muestra en la actualidad.

Pero, también, por la desconexión existente entre la normativa de protección de datos y la reguladora de las distintas funciones de los archivos. El mayor peso y desarrollo de la legislación reguladora del derecho a la protección de datos³⁶⁶ hace que, en la mayoría de los casos, se imponga sobre las otras. Así sucede con respecto a la normativa reguladora del patrimonio documental, especialmente en la tensión establecida entre la obligación de cancelación prevista por la LOPD y el deber de conservación dispuesto en la LPHE, como hemos visto a través de varios ejemplos en nuestro trabajo. O con la legislación que regula el derecho de acceso a nuestros archivos, cerrando al público multitud de series documentales que únicamente podrán ser consultadas cuando

³⁶⁶ Reconocido, además, como derecho fundamental, lo cual exige que los límites y las intromisiones que se establezcan al mismo deban estar previstos en una ley, referirse a un bien o valor constitucional y ser proporcionales.

ingresen en un archivo histórico. Algo que, con la situación actual, podría no llegar a suceder nunca³⁶⁷.

Se hace necesaria, en definitiva, una ley de archivos de la AGE que sirva de motor del sistema, defina su funcionamiento y establezca las responsabilidades de cada uno de los actores implicados. Especialmente necesaria resulta también una ley de acceso a la información pública que permita, frente al ansia proteccionista de la normativa de protección de datos, el acceso de los ciudadanos a los documentos obrantes en nuestros archivos, de una forma proporcionada³⁶⁸. Ambas normas deberían contrarrestar, en su justa medida, el excesivo peso que, en nuestra opinión, ha adquirido la normativa de protección de datos. Sólo de esta manera, creemos, los archivos podrán convertirse en eje de las políticas de gestión de documentos e información pública de la AGE; y podrá conservarse y difundirse nuestro patrimonio documental con las debidas garantías para el necesario derecho de los ciudadanos a la protección de sus datos de carácter personal.

Para finalizar, proponemos tres vías para avanzar en el estudio de la relación protección de datos-archivos:

- En primer lugar, creemos necesario analizar la relación entre documentos, sistemas de información para la gestión, sistemas de descripción archivística y sistemas electrónicos de gestión de documentos, con el concepto de fichero, necesario –según nuestro criterio- para que los tratamientos de datos se consideren amparados por la normativa de protección de datos. Este análisis permitiría definir una serie de criterios necesarios para identificar un modelo de fichero de cara a la aplicación homogénea y correcta de la normativa vigente.
- Junto a ello, un estudio de caso que permitiera abordar de forma integral esta problemática en el seno de una única organización, por

³⁶⁷ No solo por el mal funcionamiento del sistema archivístico en lo que se refiere a su régimen de transferencias. Sobre todo, porque pueden ser eliminadas previamente como resultado de la obligación de cancelación expresada antes.

³⁶⁸ “Todo ello debería ser regulado en la normativa sobre acceso y sobre archivos –en una auténtica norma completa y sistemática, y no en un artículo de la Ley de procedimiento administrativo, como hasta ahora-” (Guichot 2009, pp. 272-273).

ejemplo un Ministerio o un Ayuntamiento, facilitaría un modelo concreto de intervención por parte del archivo en materia de protección de datos y la metodología necesaria para llevarla a cabo.

- Por último, una tercera vía de estudio podría venir del análisis de la relación entre la normativa de protección de datos y la legislación sobre archivos y acceso a la información pública en otros países de nuestro entorno. Análisis que podría inspirar los futuros –y necesarios- desarrollos legislativos que hayan de producirse sobre estas cuestiones en nuestro país.

De esta forma podría completarse el esfuerzo de análisis, adaptación y aplicación necesario para cumplir con la normativa vigente sin menoscabo de las funciones atribuidas a los archivos. Queda, no obstante, bastante camino por recorrer. Esperemos que este trabajo haya servido, al menos, para iniciar sus primeros pasos.

7. FUENTES

7.1. Bibliografía

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN Y CERTIFICACIÓN (AENOR). 2006. *UNE-ISO 15489-1. Información y documentación. Gestión de documentos. Parte 1: Generalidades*. Madrid: AENOR [se cita en el texto como ISO 15489-1:2001]

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN Y CERTIFICACIÓN (AENOR). 2006. *UNE-ISO/TR 15489-2. Información y documentación. Gestión de documentos. Parte 2: Directrices*. Madrid: AENOR [se cita en el texto como ISO/TR 15489-2:2001]

AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID (APDCM). 2008. *Protección de datos personales para Administraciones Locales*. Madrid: APDCM

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD). 2010. *Memoria 2009*. Madrid: AEPD

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD). 2011. *Memoria 2010*. Madrid: AEPD

ALBERCH FUGUERAS, R. 2003. *Los archivos, entre la memoria histórica y la sociedad del conocimiento*. Barcelona: UOC

CASADO DE OTAOLA, L. 2009. La documentación administrativa extrajudicial producida en aplicación de la legislación sobre Vagos y Maleantes y Peligrosidad y Rehabilitación Social: problemas de

identificación, localización y acceso. En: LETÓN RUIZ, R. y SÁNCHEZ-CARRETERO, C. (coords.). *IV Jornadas Archivo y Memoria. La memoria de los conflictos: legados documentales para la Historia. Madrid, 19-20 febrero* [en línea]. Madrid: Fundación de los Ferrocarriles Españoles; Consejo Superior de Investigaciones Científicas, pp. 53-68. [Consulta: 18 julio 2010]. Disponible en:

http://www.archivoymemoria.com/jornada_04/docu_04/CDJornadas%20A yM09.pdf

CASTILLO VÁZQUEZ, I.C. del. 2007a. *Protección de datos: cuestiones constitucionales y administrativas. El derecho a saber y la obligación de callar*. Cizur Menor (Navarra): Aranzadi (Thomson-Civitas). Estudios de protección de datos de la Agencia de Protección de Datos de la Comunidad de Madrid

CASTILLO VÁZQUEZ, I.C. del. 2007b. Transparencia, acceso a la documentación administrativa y protección de datos personales de carácter personal. *Foro: Revista de ciencias jurídicas y sociales*, 6, pp. 231-254. [Consulta: 18 julio 2010]. Disponible en:

<http://revistas.ucm.es/der/16985583/articulos/FORO0707220231A.PDF>

COOK, T. 1991. *La evaluación archivística de los documentos que contienen informaciones personales: un estudio del RAMP con directrices*. París: UNESCO

CRUZ MUNDET, J.R. 2003. *Manual de Archivística*. 5ª ed. Madrid: Fundación Germán Sánchez Ruipérez

CRUZ MUNDET, J.R. 2006. *La gestión de documentos en las organizaciones*. Madrid: Pirámide

CRUZ MUNDET, J.R. 2011. *Diccionario de Archivística*. Madrid: Alianza

DAVARA FERNÁNDEZ DE MARCOS, I. 2011. *Hacia la estandarización de la protección de los datos personales*. Las Rozas (Madrid): La Ley

DÍAZ ROJO, J.A. 2002. Privacidad: ¿neologismo o barbarismo? *Espéculo. Revista de estudios literarios* [en línea], 21. [Consulta: 18 julio 2010]. Disponible en: <http://www.ucm.es/info/especulo/numero21/privaci.html>

DUPLÁ DEL MORAL, A. 1997. *Manual de archivos de oficina para gestores*. Madrid: Consejería de Educación y Cultura de la Comunidad de Madrid; Marcial Pons

FARIÑA PESTANO, F.I.; DÍAZ FARIÑA, F.A.; RODRÍGUEZ ACEVEDO, J.M. 2006. ¿Archivos al servicio del ciudadano? Paradojas y contradicciones de una legislación restrictiva e ineficaz. En: *El archivo, ¿un servicio público? Congreso de Archivos de Canarias. Libro de actas. La Oliva, Fuerteventura. 19, 20 y 21 de octubre de 2006*. Las Palmas de Gran Canaria: Anroart, pp. 351-374

FERNÁNDEZ CUESTA, F. 2010. El secreto desvelado. Algunas notas apresuradas sobre el proyecto de ley de acceso a la información pública y los archivos. *Archivamos. Revista trimestral de actualidad de archivos y documentos*, 77, pp.5-7.

FERNÁNDEZ RAMOS, S. 1997. *El derecho de acceso a los documentos administrativos*. Madrid: Marcial Pons

FERNÁNDEZ RAMOS, S. 2002. El Sistema Estatal de Archivos Públicos: pasado, presente y futuro. *Revista d'Arxius*, 1, pp. 127-166

FERNÁNDEZ SALMERÓN, M.; VALERO TORRIJOS, J. 2005. La difusión de información administrativa en Internet y la protección de datos personales: análisis de un proceso de armonización jurídica. *Nuevas políticas públicas. Anuario multidisciplinar para la modernización de las Administraciones Públicas* [en línea], 1, pp. 307-342. [Consulta: 18 julio 2010]. Disponible en: <http://www.juntadeandalucia.es/institutodeadministracionpublica/anuario/jsp/herramientas/verArticulo.jsp?ca=503&anyo=N%BA%201%20A%D10%202005&v=1&url=notas/notas4/notas01.htm>

GÓMEZ-LLERA GARCÍA-NAVA, E. 2007. Aspectos legales del acceso a los documentos en los archivos. En: *Los archivos: un servicio público*. Valladolid: Junta de Castilla y León, pp. 10-30

GÓMEZ-LLERA GARCÍA-NAVA, E. 2009. El problema del acceso a la documentación en los archivos históricos [en línea]. Ponencia presentada en las I Jornadas sobre Acceso a los Documentos Públicos y Oficiales. Madrid: AEFP. [Consulta: 18 julio 2010]. Disponible en:
http://www.aefp.org.es/NS/Documentos/Jornadas-Congresos/2009_IJADPO/IJADPO20090226EGLGN.pdf

GUICHOT, E. 2005. *Datos personales y Administración Pública*. Cizur Menor (Navarra): Aranzadi (Thomson-Civitas). Estudios de protección de datos de la Agencia de Protección de Datos de la Comunidad de Madrid

GUICHOT, E. 2007. Derecho a la privacidad, transparencia y eficacia administrativa: un difícil y necesario equilibrio. *Revista catalana de dret públic* [en línea], 35, pp. 43-74. [Consulta: 18 julio 2010]. Disponible en:
http://www10.gencat.net/eapc_revistadret/revistes/revista/Dret_a_la_privadesa_transparencia_i_eficacia_administrativa_un_equilibri_dificil_i_necessari/es?set_language=es&cl=es

GUICHOT, E. 2009. *Publicidad y privacidad de la información administrativa*. Cizur Menor (Navarra): Aranzadi (Thomson-Civitas). Estudios de protección de datos de la Agencia de Protección de Datos de la Comunidad de Madrid

GUTIÉRREZ CASTILLO, V.L. 2005. Aproximación a la protección jurídica internacional del derecho de acceso y protección de datos en Europa. *Derecho y conocimiento* [en línea], 3 [Consulta: 18 julio 2010]. Disponible en:
http://www.uhu.es/derechoyconocimiento/DyC03/DYC003_A04.pdf

HERNÁNDEZ OLIVERA, L. 2007. Eliminar para proteger: destruir adecuadamente los documentos personales evita fraudes y robos. *Archivamos. Revista trimestral de actualidad de archivos y documentos*, 63, p. 55-56

HEREDIA HERRERA, A. 2007. *¿Qué es un archivo?* Gijón: Trea

HEREDIA HERRERA, A. 2011. Historia, memoria y gestión en el contexto archivístico. En: GALVÁN RIVERO, C.; BARÓ PAZOS, J. (coords.). *La utilidad de los archivos. Estudios en homenaje a Manuel Vaquerizo Gil*. Santander: PUBliCan, pp. 73-82

INTERNATIONAL COUNCIL ON ARCHIVES (ICA). 1997. *Guide for managing electronic records from an archival perspective*. París: ICA

INTERNATIONAL COUNCIL ON ARCHIVES (ICA). 2000. *ISAD(G): Norma Internacional General de Descripción Archivística*. 2ª ed. Madrid: Ministerio de Educación, Cultura y Deporte

INTERNATIONAL COUNCIL ON ARCHIVES (ICA). 2004. *ISAAR (CPF): Norma Internacional sobre los Registros de Autoridad de Archivos relativos a Instituciones, Personas y Familias*. 2ª ed. Madrid: Ministerio de Cultura

INTERNATIONAL COUNCIL ON ARCHIVES (ICA). 2005. *Documentos electrónicos: manual para archiveros*. Traducción de M. Dolores Carnicer Arribas. Madrid: Ministerio de Cultura. Studies, 16

LASO BALLESTEROS, Á. 2009. *Los archivos provinciales. Qué son y cómo se tratan*. Gijón: Trea

LLANSÓ SANJUAN, J. 2006a. Sistemas archivísticos y modelos de gestión de documentos en el ámbito internacional (Parte I). *Revista Códice*, 2 (1), pp. 53-88

LLANSÓ SANJUAN, J. 2006b. Sistemas archivísticos y modelos de gestión de documentos en el ámbito internacional (Parte II). *Revista Códice*, 2 (2), pp. 39-70

MARTÍNEZ GARCÍA, L. 1999. El Sistema Español de Archivos en la Constitución: la confrontación entre teoría y realidad. *Boletín de la ANABAD*, XLIX (3-4), pp. 89-172

MATAS, J. 2009a. Accés amb reserves: llums i ombres de la normativa d'accés a la informació pública. *Lligall*, 29, pp. 11-35

MATAS, J. 2009b. Arxius, ciutadania i accés a la documentació. En: *Manual d'arxivística i gestió documental*. Barcelona: Associació d'Arxivers de Catalunya, pp. 437-463

MESSÍA DE LA CERDA BALLESTEROS, J.A. 2005. El consentimiento y el derecho a la protección de datos de carácter personal. *Nuevas políticas públicas. Anuario multidisciplinar para la modernización de las Administraciones Públicas* [en línea], 1, pp. 267-281. [Consulta: 13 julio 2010]. Disponible en:

<http://www.juntadeandalucia.es/institutodeadministracionpublica/anuario/jsp/herramientas/verArticulo.jsp?ca=503&anyo=N%BA%201%20A%D10%202005&v=1&url=notas/notas2/notas01.htm>

MESSÍA DE LA CERDA BALLESTEROS, J.A. 2008. Protección de datos y libertad religiosa: el tratamiento de los datos de los apóstatas por las confesiones religiosas. *Diario La Ley*, 6595, 11 jun. Sección Doctrina. Disponible también en: *Actualidad Administrativa*, 11, quincena del 1 al 15 jun., t. I.

MINISTERIO DE CULTURA. 2010. *Anuario de estadísticas culturales 2010* [en línea]. Madrid: Ministerio de Cultura. [Consulta: 10 de junio de 2011]. Disponible en:

http://www.mcu.es/estadisticas/docs/capitulos_graficos/AEC2010/Anuario_de_Estadisticas_Culturales_2010.pdf

OCAÑA LACAL, D. de. 1999. Ignorancia, ilegalidad y otros males: panorámica del derecho de acceso a los archivos públicos en España. *Boletín de la ANABAD*, XLIX (3-4), pp. 173-211

PALOMINO DÍEZ, I. 2009. La protección de datos de carácter personal. En: SENDÍN GARCÍA, M.A.; GÓMEZ DÍAZ, R. (dirs.). *Régimen jurídico de los documentos: aspectos administrativos, civiles, penales y procesales*. Granada, Comares, pp. 357-409

PARRA SÁEZ, S. 2008. La IP como dato personal, insuficiente para identificar al infractor. *Samuel Parra. Protección de datos personales* [blog]. 24 de febrero de 2008. [Consulta: 12 junio 2011]. Disponible en: <http://www.samuelparra.com/2008/02/24/la-ip-como-dato-personal-insuficiente-para-identificar-al-infractor/>

PEARCE-MOSES, R. 2005. *A Glossary of Archival and Records Terminology* [en línea]. Chicago: The Society of American Archivists (SAA). [Consulta: 12 junio 2011]. Disponible en: <http://www.archivists.org/glossary/index.asp>

PUENTE ESCOBAR, A. 2008. Aspectos reseñables y cuestiones novedosas. En: *Transparencia administrativa y protección de datos personales. V Encuentro entre Agencias Autonómicas de Protección de Datos Personales*. Madrid: Agencia de Protección de Datos de la Comunidad de Madrid, pp. 415-461.

RALLO LOMBARTE, A. 2009. La garantía del derecho constitucional a la protección de datos personales en los órganos judiciales. *Nuevas políticas públicas. Anuario multidisciplinar para la modernización de las Administraciones Públicas* [en línea], 5, pp. 97-115. [Consulta: 16 julio 2010]. Disponible en: <http://www.juntadeandalucia.es/institutodeadministracionpublica/anuario/jsp/herramientas/verArticulo.jsp?ca=502&anyo=N%BA%205%20A%D10%202009&v=1&url=estudios5/estudio1/estudio01.htm>

RAMS RAMOS, L. 2008. *El derecho de acceso a archivos y registros administrativos*. Madrid: Reus

RIVERO ORTEGA, R. 2007. *El expediente administrativo. De los legajos a los soportes electrónicos*. Cizur Menor (Navarra): Aranzadi (Thomson)

RODRÍGUEZ-ARANA MUÑOZ, J. 2009. Estudio preliminar sobre la transparencia en la Administración Pública. En: SENDÍN GARCÍA, M.A.; GÓMEZ DÍAZ, R. (dirs.). *Régimen jurídico de los documentos: aspectos administrativos, civiles, penales y procesales*. Granada, Comares, pp. 1-17

SENDÍN GARCÍA, M.A. 2009. Derechos de los ciudadanos relativos a la presentación de documentos en los procedimientos administrativos. Derecho de acceso a archivos y registros. En: SENDÍN GARCÍA, M.A.; GÓMEZ DÍAZ, R. (dirs.). *Régimen jurídico de los documentos: aspectos administrativos, civiles, penales y procesales*. Granada, Comares, pp. 287-325

SERRA SERRA, J. 2008. *Los documentos electrónicos. Qué son y cómo se tratan*. Gijón: Trea

SERRANO PÉREZ, M.M. 2003. *El derecho fundamental a la protección de datos. Derecho español y comparado*. Madrid: Civitas (Thomson-Civitas). Estudios de protección de datos de la Agencia de Protección de Datos de la Comunidad de Madrid

SERRANO PÉREZ, M. M. 2005. El derecho fundamental a la protección de datos. Su contenido esencial. *Nuevas políticas públicas. Anuario multidisciplinar para la modernización de las Administraciones Públicas* [en línea], 1, pp. 267-281. [Consulta: 13 julio 2010]. Disponible en: <http://www.juntadeandalucia.es/institutodeadministracionpublica/anuario/jsp/herramientas/verArticulo.jsp?ca=503&anyo=N%BA%201%20A%D1O%202005&v=1&url=notas/notas1/notas01.htm>

SUBDIRECCIÓN GENERAL DE LOS ARCHIVOS ESTATALES. 1995. *Diccionario de Terminología Archivística*. 2ª edición. Madrid: Ministerio de Cultura. Normas técnicas de de la Subdirección General de los Archivos Estatales, 1. [Citado en el texto como DTA-SGAE]

TRONCOSO REIGADA, A. 2008. Transparencia administrativa y protección de datos personales. En: *Transparencia administrativa y protección de datos personales. V Encuentro entre Agencias Autonómicas de Protección de Datos Personales*. Madrid: Agencia de Protección de Datos de la Comunidad de Madrid, pp. 23-188.

YEO, G. 2007. Concepts of record (1): evidence, information, and persistent representations. *The American Archivist*, 70 (2), pp. 315-343

7.2. Documentos de la AEPD mencionados en el texto

Los siguientes documentos se encuentran disponibles en línea en el sitio web de la AEPD:

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD). [s.a.]. *Agencia Española de Protección de Datos* [sitio web]. Madrid: AEPD. [Consulta: 12 junio 2011]. Disponible en: <https://www.agpd.es>

Informes Jurídicos

Informe Jurídico 213/2004, sobre cesión de la dirección IP a las Fuerzas y Cuerpos de Seguridad. Disponible en:

https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/telecomunicaciones/common/pdfs/2004-0213_Cesi-oo-n-de-la-direcci-oo-n-IP-a-las-Fuerzas-y-Cuerpos-de-Seguridad.pdf

Informe Jurídico 285/2006, sobre número de teléfono y concepto de dato personal. Disponible en:

https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2006-0285_N-uu-mero-de-tel-ee-fono-y-concepto-de-dato-personal.pdf

Informe Jurídico 425/2006, sobre matrículas de vehículos y concepto de dato de carácter personal. Disponible en:

https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2006-0425_Matr-ii-culas-de-veh-ii-culos-y-concepto-de-dato-de-car-aa-cter-personal.pdf

Informe Jurídico 182/2008, sobre comunicación de datos relativos a domicilios. Disponible en:

https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/ambito_aplicacion/common/pdfs/2008-0182_La-vivienda-es-un-dato-de-car-aa-cter-personal-sometido-a-la-ley-org-aa-nica-15-b-1999.pdf

Informe Jurídico 319/2008, sobre acceso a datos de identificación de animales de compañía. Disponible en:

https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/ambito_aplicacion/common/pdfs/2008-0319_Acceso-a-datos-de-identificaci-oo-n-de-animales-de-compa-n-ii-a.-Datos-personales-por-asociaci-oo-n-con-el-propietario-en-un-registro-p-uu-blico..pdf

Informe Jurídico 334/2008, sobre creación de una base de datos en la que sólo aparezca el DNI o el NIF. Disponible en:

https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/common/pdfs/2008-0334_La-creaci-oo-n-de-una-base-de-datos-en-la-que-s-oo-lo-aparezca-el-DNI-o-el-NIF-queda-sometida-a-toda-la-normativa-de-Protecci-oo-n-de-Datos.pdf

Informe Jurídico 575/2008, sobre ficheros con números de teléfono móvil. Disponible en:

https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/ambito_aplicacion/common/pdfs/2008-0575_Fichero-con-n-uu-meros-de-tel-ee-fono-m-oo-vil.pdf

Informe Jurídico 82/2010, sobre creación de una base de datos a través de la huella dactilar. Disponible en:

https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/ambito_aplicacion/common/pdfs/2010-0082_Creaci-oo-n-de-una-base-de-datos-a-trav-ee-s-de-la-huella-dactilar-queda-sometido-a-la-LOPD-y-es-desproporcionado.pdf

Informe Jurídico 0285/2010, sobre instalación de una webcam que permita tener una visión panorámica de una localidad. Disponible en:

https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/videovigilancia/common/pdfs/2010-0285_Colocaci-oo-n-de-webcams-para-visionar-panor-aa-micas-de-los-t-ee-rminos-municipales.pdf

Recomendaciones

Recomendación de 23 de diciembre de 2004, al Instituto Nacional de Administración Pública. Disponible en:

http://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones/common/pdfs/Recomendaciones_INAP.pdf

Resoluciones a procedimientos sancionadores

Resolución R/00027/2006, de 8 de febrero (procedimiento PS/00192/2005). Disponible en:

https://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2006/common/pdfs/PS-00192-2005_Resolucion-de-fecha-08-02-2006_Art-ii-culo-10-LOPD.pdf

Resoluciones a procedimientos de tutela de derechos

Resolución R/00108/2005, de 22 de marzo (procedimiento TD/00389/2004). Disponible en:

http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2005/common/pdfs/TD-00389-2004_Resolucion-de-fecha-22-03-2005_Art-ii-culo-16-LOPD.pdf

Resolución R/00357/2005, de 10 de junio (procedimiento TD/00020/2005). Disponible en:

http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2005/common/pdfs/TD-00020-2005_Resolucion-de-fecha-10-06-2005_Art-ii-culo-18-LOPD.pdf

Resolución R/00494/2005, de 12 de julio (procedimiento TD/00151/2005).

Disponible en:

http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2005/common/pdfs/TD-00151-2005_Resolucion-de-fecha-12-07-2005_Art-ii-culo-18.1-LOPD.pdf

Resolución R/00319/2006, de 23 de mayo (procedimiento TD/0046/2006).

Disponible en:

https://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2006/common/pdfs/TD-00046-2006_Resolucion-de-fecha-23-05-2006_Art-ii-culo-16-LOPD_Recurrida.pdf

Resolución R/00666/2007, de 27 de julio (procedimiento TD/00251/2007).

Disponible en:

http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2007/common/pdfs/TD-00251-2007_Resolucion-de-fecha-27-07-2007_Art-ii-culo-16-LOPD.pdf

Resolución R/00319/2008, de 24 de marzo (procedimiento TD/00785/2007). Disponible en:

http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2008/common/pdfs/TD-00785-2007_Resolucion-de-fecha-24-03-2008_Art-ii-culo-15-y-16-LOPD.pdf

Resolución R/00431/2009, de 4 de marzo (procedimiento TD/01520/2008). Disponible en:

https://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2009/common/pdfs/TD-01520-2008_Resolucion-de-fecha-04-03-2009_Art-ii-culo-15-LOPD.pdf

Resolución R/00662/2009, de 1 de abril (procedimiento TD/00482/2009).

Disponible en:

https://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2009/common/pdfs/TD-00482-2009_Resolucion-de-fecha-01-04-2009_Art-ii-culo-16-LOPD.pdf

ANEXOS

Anexo 1. Formulario de recogida de datos para la apertura de expediente de usuario de los Archivos Estatales



DATOS PARA LA APERTURA DEL EXPEDIENTE DE USUARIO

DATOS PERSONALES

D.N.I./Pasaporte Fecha de expedición

Primer apellido Segundo apellido

Nombre Fecha y lugar de nacimiento

Nacionalidad Profesión

Organismo o Centro de trabajo

Domicilio habitual: Calle/Plaza/Avenida N.º

Población Provincia

Código postal País

Teléfono Fax

Domicilio temporal: Calle/Plaza/Avenida N.º

Población Provincia Código postal

Teléfono Fax

E-mail

INVESTIGACIÓN (OPCIONAL)

Persona o entidad para la que realiza la investigación

Título o tema

Objeto de la investigación

Tema (a rellenar por el Archivo)

EJEMPLAR PARA EL ARCHIVO



El acceso a los archivos de titularidad estatal se rige por lo dispuesto en la legislación vigente y sólo podrá ser restringido por las excepciones contempladas en el artículo 37 de la *Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común*, y por los artículos 57 y 62 de la *Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español*, y en las normas de desarrollo de las mismas.

El interesado declara conocer las disposiciones señaladas anteriormente sobre el acceso a los archivos y documentos, así como la *Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen*. Asimismo, declara conocer y aceptar las normas de acceso de los Archivos Estatales y se compromete a no dañar sus fondos, que constituyen el Patrimonio Documental y Bibliográfico, y que la consulta que va a realizar sobre la documentación está relacionada con sus trabajos de investigación, teniendo la obligación de entregar al Archivo un ejemplar de aquellos trabajos que hayan sido realizados utilizando sus fondos.

En el caso de solicitar reproducciones, manifiesta expresamente que destina las mismas únicamente a fines de estudio o investigación sin finalidad lucrativa, según lo dispuesto en el *Real Decreto 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad intelectual*, que regula, aclara y armoniza las disposiciones vigentes sobre la materia. Además, declara conocer el contenido de esta normativa, respetando lo que en ella y en otras normas se establece con respecto a los derechos de autor y demás aspectos de la propiedad intelectual.

Por otro lado, se compromete a no publicar ni ceder a terceras personas las reproducciones suministradas por el Archivo sin la debida autorización de éste, en cumplimiento de lo dispuesto en la *Orden Ministerial de 20 de enero de 1995 sobre la utilización de espacios de museos y otras instituciones culturales y establecimiento de los precios públicos de determinados servicios*; en la *Circular de 23 de julio de 1997 de la Dirección General del Libro, Archivos y Bibliotecas sobre criterios para la tramitación unificada y uniforme de los convenios de reproducción de documentos*, o en virtud de cualquier otra disposición establecida por los organismos competentes en la materia.

En _____, a _____ de _____ de _____
(Firma)

Los datos de carácter personal consignados en la presente solicitud son necesarios para garantizar el control y la seguridad de la documentación y se utilizan exclusivamente con fines estadísticos.

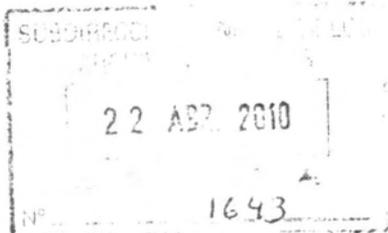
El firmante autoriza su inclusión en los ficheros automatizados cuya finalidad consiste en facilitar la gestión administrativa del Archivo. No obstante, el afectado podrá expresar su oposición por escrito en cualquier momento. El interesado tiene derecho a acceder a sus datos personales obrantes en los ficheros automatizados y a solicitar su rectificación o cancelación cuando los datos sean erróneos, según lo dispuesto en la *Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*, y demás disposiciones vigentes en la materia. A este efecto se dirigirán a la Dirección del Archivo o, en su caso, al Departamento de Referencias.

Para toda cuestión que pueda surgir sobre el acceso a los documentos o cualquier información del Archivo, el interesado podrá dirigirse a la Dirección del Centro o a la persona en quien delegue ésta. Asimismo, existe un Libro de Quejas y Sugerencias a disposición de todos los ciudadanos para las reclamaciones y/o comentarios que consideren oportunos.

Anexo 2. Oficio del Subdirector General de los Archivos Estatales, de 22 de abril de 2010, solicitando a la AEPD informe jurídico sobre la publicación en la Red de una base de datos sobre víctimas de la Guerra Civil y la represión franquista



MINISTERIO
DE CULTURA



DIRECCIÓN GENERAL DEL LIBRO,
ARCHIVOS Y BIBLIOTECAS

SUBDIRECCIÓN GENERAL DE LOS
ARCHIVOS ESTATALES

Agencia Española de Protección de Datos
C/ Jorge Juan, 6
28001 - Madrid

Madrid, a 22 de abril de 2010

Consulta sobre interpretación normativa conjunta de los preceptos de la LOPD 15/1999 y la Ley de Patrimonio Histórico Español, 16/1985.

La Subdirección General de los Archivos Estatales tiene previsto publicar una página web denominada *Portal de Víctimas de la Guerra Civil y Represaliados del Franquismo*, cuyo principal contenido es la difusión en Internet de una base de datos en la que se recogen las referencias de archivo de más de 500.000 personas, por el momento. Esta base de datos recoge el trabajo que durante los últimos años se ha estado realizando por parte de este Ministerio en el marco de la Comisión Interministerial para el estudio de la situación de las víctimas de la Guerra Civil y del franquismo (RD 1891/2004, de 10 de septiembre).

Con base en lo dispuesto en el art. 37 de la Ley Orgánica de Protección de Datos, esta Subdirección General de Archivos Estatales, del Ministerio de Cultura, solicita informe de la Agencia, respecto de las siguientes cuestiones, relativas al citado Portal de Víctimas de la Guerra Civil y Represaliados del Franquismo:

La base de datos fue declarada en agosto de 2009 a la Agencia de Protección de Datos (ORDEN CUL/2211/2009, de 22 de junio, por la que se regulan los ficheros de datos de carácter personal del Ministerio de Cultura). Según esta declaración, el fichero contiene datos identificativos de la persona y las referencias documentales a los hechos delictivos por los que fue investigada por organismos judiciales y administrativos conforme a la legislación preconstitucional. Tanto estos organismos como sus sentencias y resoluciones han sido declarados ilegítimos por la Ley de la Memoria Histórica (Ley 52/2007, de 26 de diciembre, que reconoce y amplía derechos y establece medidas en favor de quienes padecieron persecución o violencia durante la guerra civil y la dictadura (BOE de 27 de diciembre de 2007).

El fichero, además, tiene una doble finalidad, por un lado, la educación y la cultura, y, por otro, la comunicación de datos a los descendientes directos y afectados por la Ley de la Memoria Histórica con vista a los distintos derechos establecidos en su articulado, como las declaraciones de reparación y reconocimiento personal y el cobro de prestaciones derivadas.

Los expedientes referenciados en el fichero se encuentran todos depositados en archivos históricos y la gran mayoría de ellos han superado el plazo de los 50 años que marca el art. 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español, por lo que la difusión de dichas referencias no plantea duda alguna, ya que el acceso al contenido de los documentos es libre.



Sin embargo, hay 11.329 registros que referencian los sumarios y rollos generados por los Juzgados y Tribunales de Orden Público que actuaron en España entre 1963 y 1977. Su difusión puede afectar a algunos de los supuestos establecidos en el artículo mencionado, y en concreto al derecho a la intimidad de los procesados.

La Ley 16/1985 enuncia que no podrán ser públicamente consultados sin que medie consentimiento expreso de los afectados o hasta que haya transcurrido un plazo de veinticinco años desde su muerte, si su fecha es conocida, o, en otro caso, de cincuenta años, a partir de la fecha de los documentos. En cualquier caso, los registros de la base de datos no muestran en ningún momento la documentación, sino tan solo la referencia a la custodia de los expedientes en archivos estatales. Asimismo, la Ley de la Memoria Histórica en el art. 22 establece el derecho de acceso a este tipo de documentación, y para dar acceso hay que indicar dónde poder encontrarla.

Por otra parte, los fondos documentales generados por estas instituciones represoras han sido y están siendo estudiados por investigadores, en su gran mayoría ligados a proyectos científicos de las distintas universidades españolas. En este sentido, hay que destacar la tesis doctoral del Magistero de lo Social, D. Juan José del Águila, defendida en la Universidad de Sevilla en 1997, y posteriormente publicada en 2001 con el título *El Top. La represión de la libertad (1963-1977)* por la editorial Planeta. En esta monografía, en concreto, en su Apéndice 5 (páginas 446-559), se hace relación de aproximadamente 8.300 procesados por el TOP, indicándose sus apellidos y nombre, datos que también aparecerían en la base de datos de Víctimas de la Guerra Civil, realizada por este Ministerio.

Otro producto informativo de los documentos generado a partir de los documentos del TOP, es una base de datos que muestra el contenido íntegramente las sentencias del TOP. Esta base de datos ha sido publicada en CD por la Universidad de Oviedo y la Consejería de Justicia del Asturias en 2006.

En resumen:

- 1.- El Ministerio tiene previsto hacer público un fichero que contiene datos personales conectados a datos archivísticos de procedimientos judiciales y administrativos que, en algunos casos, podrían suponer una vulneración de la intimidad. Los expedientes referenciados se encuentran depositados todos en archivos históricos.
- 2.- Estos expedientes fueron generados por instituciones que han sido declaradas ilegítimas en la Ley de Memoria Histórica (art. 3)
- 3.- El fichero tiene una doble finalidad, por un lado, la educación y la cultura, y, por otro, la comunicación de datos a los descendientes directos y afectados por la Ley de la Memoria Histórica con vista a los distintos derechos establecidos en su articulado, como las declaraciones de reparación y reconocimiento personal y el cobro de prestaciones derivadas.
- 4.- La Ley de la Memoria Histórica determina el derecho de acceso a estos fondos documentales (art. 22)
- 5.- Algunos de estos datos referencian expedientes que no han superado 50 años, por lo que no podrían consultarse de acuerdo a los supuestos de la Ley del Patrimonio Histórico, y en estos casos, no está previsto dar acceso a imágenes digitales de los documentos.



6.- Existen estudios que ya han difundido, de manera sistemática y exhaustiva, los nombres y apellidos de las persona implicados en procedimientos posteriores a 1960.

La pregunta que se eleva a la consulta es la siguiente: ¿La difusión pública de los datos personales que referencien expedientes posteriores a 1960, a través del *Portal Víctimas de la Guerra civil y Represaliados del Franquismo*, es pertinente y no vulnera los preceptos de la Ley 15/1999 o su normativa de desarrollo?

Dada la naturaleza del tema, le ruego informe jurídico sobre los aspectos citados, agradeciendo de antemano toda su colaboración.

Severiano Hernández Vicente
Subdirector General de los Archivos Estatales

**Anexo 3. Informe de la Agencia Española de Protección de Datos,
de 25 de mayo de 2010 (ref. de entrada 142746/2010) sobre la
consulta del Subdirector General de los Archivos Estatales**



Ref. de entrada 142746/2010 (Mº Cultura)

Examinada su solicitud de informe, remitida a este Gabinete Jurídico, referente a la consulta formulada por el Ministerio de Cultura, cúmpleme informarle lo siguiente:

La consulta plantea si resulta conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal y su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre, la difusión pública en Internet de datos personales referidos a las víctimas de la Guerra Civil y represaliados de Franquismo. En particular se hace referencia a los datos referidos a expedientes respecto de los que no hubieran transcurrido más de cincuenta años y más en concreto a los sumarios generados por los Juzgados y Tribunales de Orden Público, que teniendo en cuenta la fecha de creación de dichos órganos tendrán siempre una antigüedad inferior a la mencionada.

I

Con carácter previo, debe señalarse que el presente informe únicamente analizará la cuestión planteada desde el punto de vista de las normas de protección de datos anteriormente referenciadas. Ello resulta especialmente relevante si se tiene en cuenta el tenor literal de la consulta en la que, si bien se hace exclusiva referencia a tales normas en la cuestión finalmente planteada, se realizan determinados razonamientos vinculados no sólo al derecho fundamental a la protección de datos de carácter personal, sino también al derecho fundamental a la intimidad de las personas cuyos datos pudieran incorporarse al portal.

En este sentido, debe recordarse que el Tribunal Constitucional ha venido considerando que ambos derechos deben considerarse como diferenciados. Así, en la Sentencia 292/2000, de 30 de noviembre, se señala que "el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 CE. Dicha peculiaridad radica en su contenido, ya que a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido (SSTC 73/1982, de 2 de diciembre, F. 5; 110/1984, de 26 de noviembre, F. 3; 89/1987, de 3 de junio, F. 3; 231/1988, de 2 de diciembre, F. 3; 197/1991, de 17 de octubre, F. 3, y en general las SSTC 134/1999, de 15 de julio, 144/1999, de 22 de julio, y 115/2000, de 10 de mayo), el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que



desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales (STC 254/1993, F. 7)”

Esta consideración resulta especialmente relevante en el supuesto que nos ocupa, por cuanto las conclusiones que se alcancen en este informe se referirán únicamente al modo en que la publicación pretendida resultará respetuosa con el derecho fundamental a la protección de datos, sin analizar si dicha publicación, aún siendo conforme a la Ley Orgánica en su caso, supondrá o no un perjuicio al derecho a la intimidad personal y familiar de los interesados

II

La premisa que acaba de indicarse lleva aparejadas dos consecuencias esenciales y derivadas directamente de la aplicación de la normativa de protección de datos de carácter personal.

La primera, de carácter más general es que las cuestiones planteadas deberán ser analizadas en lo que respecta a la publicación en un sitio web de los datos referidos a las personas que pudieran aparecer en los expedientes. En este sentido, es preciso diferenciar entre el derecho de acceso a la documentación vinculada con los mencionados expedientes del tratamiento de datos que supondrá la inserción de los datos personales en el portal al que se refiere la consulta.

Ello implicará, por una parte, que no sean relevantes para determinar la legitimación para el tratamiento de los datos efectuado mediante la inserción de los mismos en el portal las normas que legitiman el acceso al fondo documental o archivo en que se encuentre el expediente. El presente informe deberá analizar si la inclusión de tales datos en un portal situado en una página web es un tratamiento conforme o no con la legislación de protección de datos, sin perjuicio de que pueda coadyuvar a la respuesta que haya de darse la legislación especial que pueda resultar aplicable en la materia y, fundamentalmente, la prevista en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español y la Ley 52/2007, de 26 de diciembre, por la que se reconocen y amplían los derechos y se establecen medidas a favor de quienes padecieron persecución o violencia durante la Guerra Civil y la Dictadura.

III

La segunda consecuencia de la acotación efectuada en el apartado I del presente informe aparece relacionada con la aplicación de la normativa de



protección de datos de carácter personal y, en particular, con la delimitación de los sujetos titulares del mencionado derecho fundamental.

En relación con esta segunda cuestión, el artículo 2.4 del Reglamento de desarrollo de la Ley Orgánica 15/1999 dispone que “este Reglamento no será de aplicación a los datos referidos a personas fallecidas”, añadiendo que “no obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos”.

El primer inciso reproducido no es sino la manifestación en la norma reglamentaria de la posición tradicionalmente mantenida por esta Agencia. Así la cuestión referente a la aplicabilidad de las normas de protección de datos a las personas fallecidas ha sido objeto de estudio reiterado por parte de esta Agencia en diversos informes y resoluciones en que se ha manifestado en la práctica totalidad de los supuestos en el sentido de considerar excluidos de la aplicación de la Ley Orgánica 15/1999 los datos referidos a quienes hubieran fallecido.

Así, incluso durante la vigencia de la derogada Ley Orgánica 5/1992, la Agencia analizó esta cuestión en informe de 20 de mayo de 1999, en que se plantaba la creación por una determinada entidad de un fichero de personas fallecidas a partir de los datos cedidos por diversos clientes, generándose así una suerte de “lista Robinson” de personas fallecidas a las que no procedía remitir publicidad. El citado informe sienta las bases de lo que luego sería doctrina habitual de la Agencia, indicando lo siguiente:

“La citada Ley Orgánica (5/1992) tiene por objeto la protección de la “privacidad”. Así, según su artículo primero, la LORTAD tiene por finalidad la protección del honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos, según se establece en el artículo 1 de la citada Ley Orgánica.

Sentados así los términos de la presente consulta, la resolución de la misma deberá efectuarse en función de la naturaleza misma del derecho protegido por la norma, lo que conduce a la necesidad de determinar si la muerte de las personas da lugar a la extinción del derecho a la protección de la “privacidad”, ya que el artículo 32 del Código Civil dispone que “ la personalidad civil se extingue por la muerte de las personas”, lo que determinaría, en principio, la extinción con la muerte de los derechos inherentes a la personalidad.

Sin perjuicio de lo anteriormente expuesto, debe recordarse que la protección otorgada por la Ley frente a las intromisiones que supongan una vulneración de los derechos al honor y a la intimidad subsiste con



posterioridad a la muerte de las personas. En ese sentido, cabe destacar que la Ley Orgánica 1/1885, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, pone de manifiesto en sus artículos 4 a 6 que el fallecimiento no impide que por las personas que enumera el primero de los preceptos citados puedan ejercitarse las acciones correspondientes, siendo éstas la persona que el difunto haya designado a tal efecto en testamento, su cónyuge, ascendientes, descendientes o hermanos que viviesen al tiempo de su fallecimiento o, a falta de las personas anteriormente citadas, el Ministerio Fiscal.

Como anteriormente se expuso, la LORTAD tiene como objeto esencial (por imperativo del artículo 18.4 de la Constitución) la protección del honor y la intimidad, estableciendo a lo largo de su articulado las medidas precisas para asegurar que dicha protección se lleva plenamente a efecto.

Del análisis conjunto de las disposiciones contenidas en ambas Leyes se desprende que la legitimación conferida para el ejercicio de las acciones reconocidas en la Ley Orgánica 1/1982 existirá, en el ámbito de la LORTAD, cuando la actuación de las personas legitimadas tenga por directo y exclusivo objeto el ejercicio de las acciones tendentes a la protección del honor, la intimidad personal y familiar y la propia imagen de las personas fallecidas, no siendo posible la actuación de éstas en cualquier otro supuesto en que la finalidad de su actividad difiera de la antedicha protección.

Ello supone que, las personas legitimadas por la Ley Orgánica 1/1982 carecerán de legitimación para el ejercicio de los derechos reconocidos por la LORTAD, salvo en los supuestos en que esos derechos se ejerciten como instrumento para la realización de alguna de las finalidades protectoras indicadas que la Ley les atribuye. Fuera de estos supuestos no será posible entender que la actividad de los herederos o personas referidas en el artículo 4 de la Ley Orgánica 1/1982 se encuentra amparada por la LORTAD.

En el presente caso, tratándose de una cesión de datos producida entre dos entidades de naturaleza jurídico privada, resulta de aplicación, como se dijo, el artículo 11 de la LORTAD, que exige consentimiento del afectado por la cesión, salvo en los supuestos excluidos por el artículo 11.2. No siendo, lógicamente, posible la prestación del consentimiento por parte del afectado, deberá determinarse si es posible la sustitución de dicho consentimiento por el de las personas legitimadas por el artículo 4 de la Ley Orgánica 1/1982”.

Quiere todo ello decir que la problemática planteada por a presente consulta, en lo que a la garantía del derecho fundamental a la protección de



datos se refiere, únicamente resulta relevante cuando se esté haciendo referencia a datos relativos a personas que no hubieran fallecido, dado que en caso de fallecimiento no son aplicables las previsiones de la Ley Orgánica 15/1999 y su normativa de desarrollo, salvo en lo previsto en el inciso segundo del artículo 2.4 del Reglamento y la posible solicitud de la cancelación de los datos, si ello fuera procedente, por las personas enumeradas en dicho precepto.

Por ello, la primera consecuencia que debe extraerse de lo que se ha indicado es que será fundamental para tomar en consideración las conclusiones que se alcancen en el presente informe la determinación de si las personas a las que se refieran los datos de carácter personal objeto de publicación en el portal descrito en la consulta han fallecido o no, dado que en el primer caso, y reiterando que el informe no analiza las consecuencias del tratamiento en el derecho a la intimidad personal y familiar de las personas, las cuestiones relacionadas con la citada publicación de los datos no resultan relevantes desde el punto de aplicación de la Ley Orgánica 15/1999.

IV

Una vez acotado el objeto del presente informe, debe ahora analizarse si resulta conforme a lo dispuesto en la Ley Orgánica 15/1999 y su normativa de desarrollo la publicación en el portal al que se refiere la consulta de los datos personales a los que la misma se refiere y, en particular, los relacionados con los sumarios tramitados por los Juzgados y Tribunales de Orden Público que la consulta menciona expresamente, siempre referidos a personas que no hubieran fallecido al tiempo de verificarse la publicación.

La puesta en el portal de los mencionados datos constituye una cesión o comunicación de datos de carácter personal, definida por el artículo 3 i) de la Ley Orgánica 15/1999 como "toda revelación de datos realizada a una persona distinta del interesado".

En relación con las cesiones, el artículo 11.1 de la Ley indica que "los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado". No obstante, este consentimiento no será preciso en los supuestos enumerados por el artículo 11.2 de la Ley, de entre los cuales únicamente podría resultar aplicable al presente supuesto el contemplado en la letra a); es decir, que exista una norma con rango de Ley que otorgue cobertura a la cesión planteada.

La afirmación que acaba de realizarse implica que la publicación planteada no podrá ampararse en el hecho de que los datos figuren recogidos en fuentes accesibles al público, prevista en el artículo 11.2 b) de la Ley Orgánica 15/1999 y a la que parece hacer alusión la consulta, al mencionar la



existencia de dos estudios publicados sobre las actividades de los Tribunales de Orden Público.

En este sentido, debe recordarse que el artículo 7 del Reglamento de desarrollo de la Ley Orgánica 15/1999 ha venido a clarificar el concepto de fuentes accesibles al público establecido en el artículo 3 j) de la Ley Orgánica, aclarando que las mismas constituyen una lista taxativa, de modo que ningún fichero que no aparezca expresamente recogido o amparado por la misma podrá ser considerado fuente accesible al público, siendo además necesario que el acceso al fichero sea libre, mediando o no el pago de una contraprestación.

Pues bien, los supuestos analizados podrían cumplir el segundo de los requisitos enumerados, pero en ningún caso se encuentran entre los ficheros enumerados taxativamente como fuentes accesibles al público.

Así, la existencia de un trabajo publicado en que se incluyen "aproximadamente 8300 procesados por el TOP, indicándose sus apellidos y nombre" no puede ser catalogado como fuente accesible al público, dado que dicho estudio no puede tener la consideración de medio de comunicación social, en los términos establecidos por el artículo 7.1 e) del Reglamento de desarrollo de la Ley Orgánica 15/1999, con independencia del derecho a la libertad de expresión que pueda corresponder a su autor al amparo del artículo 20 de la Constitución.

Por otra parte, respecto de la publicación en soporte electrónico de las sentencias del Tribunal de Orden Público, esta Agencia ha manifestado reiteradamente que dicha publicación debería llevarse a cabo previa disociación de los datos de carácter personal contenidos en las mismas, por lo que la posible existencia de una publicación en que no se tiene en cuenta el criterio de esta Agencia no puede ser tenida en consideración para amparar o legitimar el tratamiento de datos que serían similares a los contenidos en la misma y que, además, no se obtendrían de dicha publicación sino de otras fuentes distintas.

V

Dicho esto, procede analizar si existe una norma con rango de Ley que habilita la cesión derivada de la publicación a la que se refiere la consulta.

El análisis de dicha cuestión deberá retomar la premisa que ya se incluyó con anterioridad en el presente informe: la publicación de los datos en el portal al que se refiere la consulta no ha de entenderse en términos similares al acceso a la documentación contenida en los archivos públicos o privados donde se encuentre el documento vinculado a cada supuesto concreto.



Al propio tiempo, la publicación deberá respetar el principio de proporcionalidad consagrado por el artículo 4.1 de la Ley Orgánica 15/1999, que dispone que “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”.

Esta acotación resulta igualmente relevante, dado que la consulta pone de manifiesto que las finalidades del fichero serán dos: “por un lado la educación y la cultura y, por otro, la comunicación de datos a los descendientes directos y afectados por la Ley de Memoria Histórica con vista a los distintos derechos establecidos en su articulado, como las declaraciones de reparación y reconocimiento personal y el cobro de prestaciones derivadas”.

En este sentido, debe recordarse que la Ley 52/2007 delimita en su artículo 1 las finalidades que podrían justificar el tratamiento de los datos, al dispone que:

“1. La presente Ley tiene por objeto reconocer y ampliar derechos a favor de quienes padecieron persecución o violencia, por razones políticas, ideológicas, o de creencia religiosa, durante la Guerra Civil y la Dictadura, promover su reparación moral y la recuperación de su memoria personal y familiar, y adoptar medidas complementarias destinadas a suprimir elementos de división entre los ciudadanos, todo ello con el fin de fomentar la cohesión y solidaridad entre las diversas generaciones de españoles en torno a los principios, valores y libertades constitucionales.

2. Mediante la presente Ley, como política pública, se pretende el fomento de los valores y principios democráticos, facilitando el conocimiento de los hechos y circunstancias acaecidos durante la Guerra civil y la Dictadura, y asegurando la preservación de los documentos relacionados con ese período histórico y depositados en archivos públicos.”

VI

Dos serían las normas con rango de Ley que podrían ser invocadas para encontrar la habilitación otorgada por el artículo 11.2 a): la Ley 16/1985 y la Ley 52/2007, debiendo analizarse si efectivamente tales normas otorgarían cobertura a la mencionada cesión.

Comenzando nuestro análisis por la Ley 52/2007, el artículo 22 de la misma, al que se refiere la consulta, dispone que:



“1. A los efectos de lo previsto en esta Ley, se garantiza el derecho de acceso a los fondos documentales depositados en los archivos públicos y la obtención de las copias que se soliciten.

2. Lo previsto en el apartado anterior será de aplicación, en sus propios términos, a los archivos privados sostenidos, total o parcialmente, con fondos públicos.

3. Los poderes públicos adoptarán las medidas necesarias para la protección, la integridad y catalogación de estos documentos, en particular en los casos de mayor deterioro o riesgo de degradación.”

De los dos primeros apartados del precepto reproducido se deduce la existencia de un derecho al acceso a los documentos referidos a los procesos tramitados por los Tribunales de Orden Público, “a los efectos de lo previsto en esta Ley”. Este derecho a conocer los documentos que debe, como se ha venido indicando en lugares anteriores, diferenciarse del tratamiento consistente en la publicación de los datos personales de los implicados en un portal web, se encuentra, como se ha visto, limitado en cuanto a la finalidad que lo justifica, que deberá derivar directamente de lo dispuesto en la propia Ley 52/2007.

De este modo, el acceso a los documentos no será ilimitado sino que debe tener por objeto la obtención de las medidas de reconocimiento y compensación establecidas en la propia Ley o la divulgación de los hechos acaecidos en los períodos a los que la misma se refiere.

Al propio tiempo, como se ha indicado, el artículo 22 regula el derecho a acceder a los documentos, a los efectos previstos en la propia Ley, pero no podría considerarse norma legitimadora del tratamiento de los mismos, consistente en la publicación de los datos asociados al documento en un portal, por cuanto dicha publicación, distinta del acceso al documento, supondría una divulgación universal de la información básica asociada al expediente respecto del que se reconoce el acceso. De este modo, no sería posible considerar dicha divulgación generalizada, incluso sin contar con la voluntad del interesado no fallecido, amparada en los objetivos previstos en la Ley.

Debe, igualmente recordarse que, dado que en la consulta se señala que en la base de datos cuya publicación se pretende se incluirán datos referidos a los “hechos delictivos por los que (la persona interesada) fue investigada por organismos judiciales y administrativos”, se estará procediendo al tratamiento de datos que en un momento dado, sin perjuicio de lo dispuesto en el artículo 3 de la Ley 52/2007, se consideraron constitutivos de delito o infracción administrativa, debiendo a tal efecto recordarse que el artículo 7.5 de la Ley Orgánica 15/1999 dispone que “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”.

Por otra parte, y atendiendo a las disposiciones contenidas en la Ley 16/1985, debe efectuarse la misma precisión que se ha señalado anteriormente respecto de la Ley 52/2007: la citada Ley regula el derecho a acceder a los documentos, pero no autoriza ni legitima la difusión universal de los datos asociados a su contenidos a cualquier persona, tenga o no interés en conocer dicho contenido.

Al propio tiempo, la citada Ley establece normas más restrictivas en relación con dicho acceso, dado que tras establecer su artículo 57 que los documentos del patrimonio documental “serán de libre consulta a no ser que afecten a materias clasificadas de acuerdo con la Ley de Secretos Oficiales o no deban ser públicamente conocidos por disposición expresa de la Ley, o que la difusión de su contenido pueda entrañar riesgos para la seguridad y la defensa del Estado o la averiguación de los delitos”, añade, en su apartado 1 c), que “los documentos que contengan datos personales de carácter policial, procesal, clínico o de cualquier otra índole que puedan afectar a la seguridad de las personas, a su honor, a la intimidad de su vida privada y familiar y a su propia imagen, no podrán ser públicamente consultados sin que medie consentimiento expreso de los afectados o hasta que haya transcurrido un plazo de veinticinco años desde su muerte, si su fecha es conocida o, en otro caso, de cincuenta años, a partir de la fecha de los documentos.”

De este modo, la citada previsión, como de hecho reconoce la consulta, no podría legitimar la publicación de los datos relativos a las personas relacionadas con los documentos en cuestión en un portal, restringiéndose incluso dicha información en relación con las personas fallecidas respecto de las que no es aplicable la normativa de protección de datos.

VII

Como ya se ha indicado, el artículo 22 de la Ley 52/2007 no parece legitimar la divulgación a través de Internet de los datos referidos a las personas vinculadas con los expedientes a los que se refiere la consulta sin contar con el consentimiento de las personas a las que dichos procedimientos se refieren. Sin embargo, ya efectos de completar el análisis que se ha venido realizando, debería finalmente analizarse si en caso de venir esa norma referida no a los documentos obrantes en los archivos, sino a los datos personales de los propios interesados, la misma otorgaría cobertura a la cesión.

Como ya se ha indicado, el acceso previsto en el artículo 22 se establece “a los efectos de lo previsto en esta Ley”, es decir, para el cumplimiento de las finalidades descritas en el artículo 1 de la misma. Esta referencia resulta esencial por cuanto, como se anticipó, incluso la habilitación



legal para el tratamiento debería darse únicamente en cuanto resulte adecuada, pertinente y no excesiva en relación con la finalidad que la justifica, conforme dispone el artículo 4.1 de la Ley Orgánica 15/1999.

Pues bien, tratándose de personas no fallecidas el artículo 4.2 de la Ley 52/2007, en relación con la declaración de reparación y reconocimiento personal, dispone que "Tendrá derecho a solicitar la Declaración las personas afectadas y, en caso de que las mismas hubieran fallecido, el cónyuge o persona ligada por análoga relación de afectividad, sus ascendientes, sus descendientes y sus colaterales hasta el segundo grado".

Quiere ello decir que cuando se trate de personas no fallecidas será únicamente el interesado quien podrá solicitar la declaración a la que el precepto se refiere, por lo que el acceso a los datos por parte de los restantes sujetos designados por el precepto, y aún en menor medida por las organizaciones a las que se refiere el artículo 4.3, que sólo podrán solicitar la declaración respecto de quienes hubiesen desempeñado un cargo relevante en las mismas una vez fallecido el interesado y faltando alguna de las personas a las que se refiere el artículo 4.2, no será relevante para obtener el reconocimiento y reparación establecidos en la Ley.

Por su parte, en relación con la finalidad descrita en el artículo 1.2 de la Ley 52/2007, descrita en la consulta como "la educación y la cultura", cabe considerar que lo relevante a tal efecto no son los datos personales concretos de la totalidad de las personas relacionadas con los expedientes, sino las causas que pretendieron justificar su tramitación o incluso las circunstancias en que el procedimiento se desarrolló.

De este modo, la inclusión de los datos personales de un interesado sin recabar su consentimiento, o pudiendo incluso constar su voluntad de no aparecer en el portal, resultaría excesiva para el cumplimiento de la finalidad de "educación y cultura" pretendida por la Ley 52/2007.

En consecuencia, y en relación con los datos referidos a personas no fallecidas, cabe concluir que la inclusión de sus datos en el portal únicamente debería llevarse a cabo con su consentimiento, no siendo posible, sin más, dicha inclusión en los términos previstos en la consulta, dado que, sin perjuicio de la existencia o inexistencia de una merma del derecho a la intimidad de los interesados, se estaría produciendo una vulneración de su derecho fundamental a la protección de datos de carácter personal.

VIII

Tomado en cuenta todo lo que se ha venido señalando hasta este momento, cabe concluir que, desde la perspectiva de la aplicación de las normas de protección de datos de carácter personal, sólo será posible la publicación en el portal al que se refiere la consulta de los datos relativos a las



personas que tengan la condición de víctimas de la Guerra Civil o represaliados del Franquismo, y en particular, los vinculados con los sumarios tramitados por los Juzgados y Tribunales de Orden Público si se cumplen las siguientes condiciones:

- 1) Que se trate de personas fallecidas, debiendo contrastarse los datos que obren en poder de la consultante con los resultantes de otros registros que permitan acreditar esta circunstancia cuando sea necesario.
- 2) Tratándose de personas no fallecidas, que se haya obtenido el consentimiento de los interesados para que sus datos sean incluidos en el portal, debiendo informarse al interesado de todos los extremos relacionados con ese tratamiento en los términos previstos por el artículo 5 de la Ley Orgánica 15/1999.
- 3) En caso de no contarse con el consentimiento, la información que conste en el portal en relación con las personas que no lo hubieran prestado deberá constar de forma disociada, de forma que no resulte posible identificar directa o indirectamente al interesado.

Es cuanto tiene el honor de informar,

Madrid, 25 de mayo de 2010.

EL ABOGADO DEL ESTADO
JEFE DEL GABINETE JURIDICO

Fdo.- Agustín Puente Escobar.

SR. DIRECTOR DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS