



LA DISTRIBUCIÓN COMPETENCIAL ENTRE EL ESTADO Y LAS COMUNIDADES AUTÓNOMAS EN PROTECCIÓN DE DATOS PERSONALES

Antonio Troncoso Reigada

Profesor Titular de Derecho Constitucional. Universidad de Cádiz

Director Agencia Protección de Datos. Comunidad Autónoma de Madrid



sumario

1 ■ LA PROTECCIÓN DE DATOS PERSONALES COMO MATERIA CONSTITUCIONAL: MARCO DE LEGITIMIDAD Y POSIBILIDADES PARA EL FUTURO

- 1.1. Las competencias legislativas y las competencias de ejecución administrativa en protección de datos personales
- 1.2. La protección de datos personales como materia y como actividad subsidiaria y la Sentencia del Tribunal Constitucional 290/2000, de 30 de noviembre
- 1.3. Marco constitucional y reforma estatutaria: posibilidades para el futuro

2 ■ LA CREACIÓN DE AGENCIAS AUTONÓMICAS DE PROTECCIÓN DE DATOS Y LA GARANTÍA DE LA INDEPENDENCIA

3 ■ LAS FUNCIONES DE LAS AGENCIAS DE PROTECCIÓN DE DATOS AUTONÓMICAS Y LA DELIMITACIÓN DE COMPETENCIAS ENTRE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS Y LAS AGENCIAS AUTONÓMICAS EFECTUADA EN LAS LEYES ESTATALES Y AUTONÓMICAS: LA VISIÓN DEL LEGISLADOR

4 ■ PRINCIPIOS DE COORDINACIÓN Y DE COOPERACIÓN EN LAS RELACIONES ENTRE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS Y LAS AGENCIAS AUTONÓMICAS

5 ■ UN ÁMBITO CONFLICTIVO: LAS RELACIONES ENTRE EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS PERSONALES Y LOS REGISTROS AUTONÓMICOS

- 5.1. Acerca de la obligación de inscribir los ficheros públicos competencia de las Agencias Autonómicas en el Registro General de Protección de Datos
- 5.2. Función de los Registros de Datos Personales de las Comunidades Autónomas y relación entre estos Registros y el Registro General de Protección de Datos
- 5.3. La publicidad como competencia del Registro General de Protección de Datos y las competencias plenas de control de las Agencias Autonómicas de Protección de Datos sobre los ficheros públicos de su ámbito territorial

resumen

La jurisprudencia del Tribunal Constitucional ha afirmado la existencia en el art. 18.4 CE de un derecho fundamental a la protección de datos personales. Este derecho fundamental exige no una conducta pasiva sino una actividad de los poderes públicos de garantía y control. Esta actividad administrativa de protección de datos personales lógicamente tiene que respetar el marco constitucional de distribución de materias y competencias entre el Estado y las Comunidades Autónomas, es decir, tiene que respetar plenamente el bloque de la constitucionalidad. Esto es especialmente importante en un periodo donde se inicia previsiblemente la creación de Autoridades de protección de datos de carácter autonómico.

1 ■ LA PROTECCIÓN DE DATOS PERSONALES COMO MATERIA CONSTITUCIONAL: MARCO DE LEGITIMIDAD Y POSIBILIDADES PARA EL FUTURO

La jurisprudencia del Tribunal Constitucional ha afirmado la existencia en el art. 18.4 CE de un derecho fundamental a la protección de datos personales¹. Este derecho fundamental exige no una conducta pasiva sino una actividad de los poderes públicos de garantía y control. Esta actividad administrativa de protección de datos personales lógicamente tiene que respetar el marco constitucional de distribución de materias y competencias entre el Estado y las Comunidades Autónomas; es decir, tiene que respetar plenamente el bloque de la constitucionalidad. Esto es especialmente importante en un periodo donde se inicia previsiblemente la creación de Autoridades de protección de datos de carácter autonómico.

La distribución de materias y competencias entre el Estado y las Comunidades Autónomas que refleja el texto constitucional hace que España sea un país claramente descentralizado. Así, la Constitución reserva en exclusiva determinadas materias al Estado y a las Comunidades Autónomas; son materias en las que el Estado o las Comunidades Autónomas disponen de la competencia exclusiva para desarrollar las funciones legislativas y ejecutivas. Sin embargo, la Constitución establece que en la mayoría de las materias exista un reparto de atribuciones o de funciones entre el Estado y las Comunidades Autónomas. Estas son materias en las que, por expreso deseo del constituyente, tanto el Estado como las Comunidades Autónomas ostentan competencias y ejercen funciones. Son materias en las que las competencias se encuentran compartidas entre el Estado y las Comunidades Autónomas. Este

reparto de competencias hace referencia: por una parte, a las funciones legislativas, es decir, a quién –Cortes Generales o Parlamento Autonómico– le corresponde la competencia para aprobar las leyes que regulen una materia; por otra, a las funciones ejecutivas, es decir, a qué Administración Pública –estatal o autonómica– le corresponde la actividad administrativa de ejecución. Así, puede existir un reparto de funciones, por ejemplo, que atribuya la función legislativa para el Estado y la función ejecutiva para las Comunidades Autónomas. Por último, y dentro de la misma función legislativa, puede existir una división de atribuciones, perteneciendo al Estado la legislación básica y a las Comunidades Autónomas la legislación de desarrollo².

1.1. LAS COMPETENCIAS LEGISLATIVAS Y LAS COMPETENCIAS DE EJECUCIÓN ADMINISTRATIVA EN PROTECCIÓN DE DATOS PERSONALES

No existe en la Constitución una mención expresa a la protección de datos personales ni entre las materias que son competencia exclusiva del Estado –art. 149 CE–, ni entre las materias que podrán ser asumidas por las Comunidades Autónomas –art. 148 CE–. Esto es lógico ya que, como hemos señalado en otra ocasión, este es un derecho fundamental cuyo contenido tiene un origen principalmente jurisprudencial. Tampoco existe ninguna referencia expresa a la protección de datos personales en los Estatutos de Autonomía, todos ellos anteriores a las primeras sentencias del Tribunal Constitucional que delimitaron este derecho fundamental³. Esto hace que la atribución por parte del legislador estatal y autonómico de potestades y funciones de control sobre ficheros a autoridades de carácter estatal o autonómico pueda resultar problemática al no existir una delimitación material y competencial clara. Esta dificultad no es, como es sabido, característica exclusiva de esta materia sino que entra dentro de la complejidad del sistema constitucional y estatutario de distribución de competencias.

La primera Ley que cumplió la previsión del art. 18.4 CE y desarrolló este derecho en nuestro país es la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal –LORTAD–. Esta Ley estableció en el Título VI “Agencia de Protección de Datos”, la existencia de una Agencia estatal de Protección de Datos, así como de unos órganos correspondientes de las Comunidades Autónomas –art. 40–. Así este precepto señalaba: “1. Las funciones de la Agencia de Protección de Datos reguladas en el artículo 36, a excepción de las mencionadas en los apartados j), k) y l) y en los apartados f) y g) en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 45 y 48, en relación con sus específicas competencias, serán ejercidas, cuando afecten a ficheros automatizados de datos de carácter personal creados o gestionados por las Comunidades Autónomas, por los órganos correspondientes de cada Comunidad, a los que se garantizará plena independencia y objetividad en el ejercicio de sus funciones. 2. Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros públicos para el ejercicio de las competencias que se les reconoce sobre los mismos, respecto a los archivos informatizados de datos personales cuyos titulares sean los órganos de las respectivas Comunidades Autónomas o de sus Territorios Históricos”. Por tanto, correspondía a la autoridad nacional el control de los ficheros privados y de los ficheros de los Ayuntamientos, lo que implica el desarrollo de la actividad de policía administrativa –inspección, supervisión y sanción–, así como las competencias administrativas relativas a la inscripción registral –arts. 38, 45 y 48 LORTAD–. En cambio, correspondía únicamente a las autoridades autonómicas el control de los ficheros de la Administración Pública regional⁴.

Esta regulación en lo que afecta a las autoridades de control ha sido sustancialmente mantenida –aunque con algunas modificaciones como las relativas al control por parte de las autoridades autonómicas de los ficheros de los entes locales– por la Ley Orgánica

15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. De esta forma, en España, como ocurre en otros países con modelo federal o autonómico como es el caso de Alemania, Suiza y Canadá, junto con la Agencia de Protección de Datos de la Federación o de la Nación, coexisten Agencias de Protección de Datos de cada una de las CCAA o de los Estados que componen la Federación. Son las que el Consejo de Europa califica como Agencias subestatales o subnacionales. En esta misma dirección, la Directiva 95/46 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 datos establece en el art. 28 "Autoridades de control" que "los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva". Igualmente se señala en el mismo artículo que "los Estados miembros dispondrán que se consulte a las autoridades de control en el momento de la elaboración de las medidas reglamentarias o administrativas relativas a la protección de los derechos y libertades de las personas en lo que se refiere al tratamiento de datos de carácter personal".

La justificación constitucional de la *competencia legislativa* del Estado para aprobar la LORTAD y la LOPD proviene, esencialmente, del propio art. 18.4 CE que establece que "la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de los derechos". Como es sabido, la afirmación de la existencia de un derecho fundamental a la protección de datos personales está sometido a reserva de Ley Orgánica –ex art. 53.1 y 81 CE–. Pero especialmente, el art. 149.1.1 CE atribuye al Estado la competencia exclusiva sobre la "regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales". Este precepto habilitaría a

las Cortes Generales para legislar sobre esta materia, estableciendo principios y derechos de protección de datos. Esta competencia legislativa del Estado para regular las condiciones básicas del ejercicio de este derecho fundamental a la protección de datos personales no excluye la competencia de las Comunidades Autónomas para dictar una legislación de desarrollo sobre esta materia. No debe confundirse la igualdad de derechos y obligaciones de todos los españoles en cualquier parte del territorio nacional con la existencia de ordenamiento jurídico rigurosamente uniforme, pues esto sería contrario al propio principio de autonomía –art. 2 CE–. Las Comunidades Autónomas puedan desarrollar también funciones legislativas en protección de datos personales que desarrollen los derechos y los principios, funciones legislativas que no tienen porque limitarse a tener como contenido la creación de Agencias Autonómicas pero que no pueden suponer en ningún caso el establecimiento de "condiciones básicas" de las que se derive, en su aplicación, que el derecho a la protección de datos no sea igual para todos los españoles.

La primera Ley autonómica de protección de datos fue la Ley 13/1995, de 21 de abril, de tratamiento automatizado de ficheros con datos personales por la Comunidad de Madrid. Esta Ley, de una gran calidad técnica, no sólo creó la Agencia de Protección de Datos de la Comunidad de Madrid como Ente de Derecho Público, sino que desarrolló los principios y los derechos de protección de datos, reforzando las garantías establecidas en la LORTAD, por ejemplo, en lo relativo al principio de información, al consentimiento de los interesados, a las medidas de seguridad, y a los procedimientos de ejercicio de los derechos de acceso, rectificación y cancelación⁵. En cambio, la Ley 8/2001, de 13 de julio, de protección de datos de carácter personal de la Comunidad de Madrid suprimió todas las referencias contenidas en la Ley 13/1995, de 21 de abril, relativas a la recogida de datos de carácter personal, derechos de los ciudadanos, principio del consentimiento, ejercicio de los derechos de acceso, cancelación y rectificación o

cesión de datos. La Ley 8/2001, de 13 de julio, entendía que estos elementos “ya están regulados en la Ley Orgánica, pues son aspectos esenciales que delimitan el sistema de protección de las libertades públicas y los derechos fundamentales de las personas físicas, especialmente el derecho al honor y a la intimidad personal y familiar, en el tratamiento de los datos personales”⁶. Sin embargo, las referencias contenidas en la Ley 13/1995, de 21 de abril, ni eran aspectos esenciales ni estaban ya contenidas en la LOPD. La Ley 8/2001, de 13 de julio, optó por circunscribir su contenido a la delimitación de las funciones, organización y régimen jurídico básico de la Agencia de Protección de Datos de la Comunidad de Madrid, así como a aquellas materias para las cuales entendía que había una habilitación concreta en la LOPD, como la regulación del procedimiento de elaboración de las disposiciones de carácter general de creación, modificación o supresión de ficheros de titularidad de la Comunidad de Madrid; la cooperación interadministrativa y otros aspectos relacionados con la seguridad⁷. La Ley 8/2001, de 13 de junio, contiene una repetición de las definiciones recogidas en el artículo 3 LOPD, con el “fin de facilitar la comprensión del texto de la Ley sin necesidad de acudir a la Ley Orgánica para precisar el significado de esos términos y expresiones”.

El problema reside principalmente en la habilitación constitucional para que el Estado se reserve la *competencia de ejecución administrativa* de la legislación de protección de datos personales sobre los ficheros privados. No existe ningún precepto constitucional que faculte al Estado, a través de la Agencia Española de Protección de Datos, a reservarse de manera íntegra el control de los ficheros privados y de los ficheros de las Administraciones Locales. El alcance del art. 149.1.1 CE es “esencialmente normativo”, como no podía ser de otro modo ya que estamos hablando de la “regulación” de las condiciones básicas⁸. Es decir, el art. 149.1.1 CE afirma la competencia del Estado para la legislación básica, ya que una interpretación extensiva vaciaría de competencias a las

Comunidades Autónomas. La regulación de las condiciones básicas no puede extenderse de ninguna manera a la actividad ejecutiva de policía administrativa ni a las normas organizativas que atribuyen funciones a la Agencia Española de Protección de Datos. Por tanto, la atribución al Estado de competencias ejecutivas exclusivas para el control sobre los ficheros privados y los ficheros de los Ayuntamientos no es una exigencia constitucional. No es una materia cerrada por el constituyente sino que hay un ámbito de libertad para el estatuyente y para el legislador. De hecho, la LORTAD no cita ningún precepto constitucional concreto a este respecto. Por tanto, la atribución en la LORTAD de estas competencias de control a la Agencia Española responde a un juicio de oportunidad del Legislador –y del Gobierno al aprobar el proyecto de Ley en esos términos– que consideraba que la garantía de la aplicación de los mismos derechos de protección de datos en todo el territorio nacional recomendaba la atribución a autoridades nacionales de esta función de control.

No obstante, una cosa es que la atribución al Estado de las competencias de ejecución administrativa sobre protección de datos personales no sea una exigencia constitucional, y otra cosa distinta es que sea inconstitucional. Son dos los argumentos que se pueden manejar para justificar la legislación que atribuía la competencia ejecutiva al Estado. Es decir, son dos los títulos competenciales que el Estado puede esgrimir para sustentar en su momento la LORTAD y en la actualidad la LOPD:

El primer título que puede fundamentar la atribución de la competencia de control sobre los ficheros privados y sobre los ficheros de los Ayuntamientos a la Agencia Española sería el art. 149.3 CE que establece que “las materias no atribuidas expresamente al Estado por esta Constitución podrán corresponder a las Comunidades Autónomas en virtud de sus respectivos Estatutos. La competencia sobre las materias que no se hayan asumido por los Estatutos de Autonomía corresponderá al Estado,

cuyas normas prevalecerán, en caso de conflicto, sobre las de las Comunidades Autónomas en todo lo que no esté atribuido a la exclusiva competencia de éstas. [...]”. La protección de datos personales, como hemos señalado, es una materia no atribuida expresamente al Estado por la Constitución y tampoco asumida por las Comunidades Autónomas a través de sus respectivos Estatutos, además de que ni siquiera puede ser subsumida entre otras materias ya asumidas. Las Comunidades Autónomas sólo tienen las competencias de atribución, es decir, aquellas competencias específicas y explícitamente enumeradas en los Estatutos. Por ello, se trata de una materia que corresponde al Estado, que ejercerá todas las competencias sobre la misma y cuyas normas prevalecerán en caso de conflicto⁹. Así, el Estado puede reservarse legítimamente las competencias de ejecución administrativa de la legislación de protección de datos personales sobre los ficheros privados. Obviamente, todo ello mientras que esta materia no sea asumida por las Comunidades Autónomas en virtud de las próximas reformas estatutarias.

El segundo título que puede justificar la legitimidad constitucional de la atribución de la competencia de ejecución administrativa al Estado es, aunque en menor medida por lo ya señalado, el art. 149.1.1 CE. Hemos dicho que este precepto no puede interpretarse como una *exigencia* para la atribución de competencias ejecutivas a la Agencia Española de Protección de Datos, lo que es compatible con su utilización como *habilitación* para que el legislador estatal pueda atribuir estas funciones de control a la Agencia Española de Protección de Datos para preservar la igualdad de los españoles en la protección de sus datos personales, creando, de esta forma, condiciones institucionales que permitan excluir ejecuciones plurales y divergentes por las diferentes Comunidades Autónomas¹⁰. Además, en el caso de que se mantenga que la protección de datos personales no es una materia sino una actividad instrumental de otras materias, el art. 149.1.1 CE emergería para habilitar al Estado para garantizar

condiciones uniformes para el disfrute de los derechos fundamentales en todo el territorio nacional.

1.2. LA PROTECCIÓN DE DATOS PERSONALES COMO MATERIA Y COMO ACTIVIDAD SUBSIDIARIA Y LA SENTENCIA DEL TRIBUNAL CONSTITUCIONAL 290/2000, DE 30 DE NOVIEMBRE

La distribución de competencias entre el Estado y las Comunidades Autónomas que llevó a cabo la LORTAD –y que continuó esencialmente la LOPD– fue impugnada ante el Tribunal Constitucional, a través de los recursos de inconstitucionalidad interpuestos por el Consejo Ejecutivo de la Generalidad de Cataluña y el Parlamento de Cataluña, al entender que la regulación legal vulneraba el reparto constitucional de competencias al atribuir al Estado, a través de la Agencia Española de Protección de Datos, el control exclusivo sobre los ficheros de datos personales de titularidad privada y sobre los ficheros de los Ayuntamientos, otorgando únicamente a las Comunidades Autónomas, a través de las Autoridades Autonómicas, el control de los tratamientos de datos personales creados por la propia Administración autonómica. El objeto del recurso era, esencialmente, el art. 40 LORTAD que limitaba las competencias autonómicas a sus propios ficheros, excluyendo el resto de los tratamientos de datos personales. Es decir, no se cuestiona la competencia legislativa del Estado –la legitimidad de la existencia de una legislación básica de protección de datos personales– sino la atribución al Estado de la práctica totalidad de las competencias de ejecución administrativa en este ámbito.

Este planteamiento afirmaba que la protección de datos personales no es una materia en si misma objeto de competencia sino que tiene que encuadrarse en el resto de las materias que ya han sido objeto de reparto de competencias y que se delimitan en el bloque de constitucionalidad. Así, desde esta posición, la información almacenada en

ficheros es instrumental para el ejercicio de competencias sobre las distintas materias que corresponden tanto al Estado como a las Comunidades Autónomas. Este sería el motivo por el que no existe previsión constitucional ni estatutaria al respecto y este es el motivo por el que la clave de la delimitación de las competencias administrativas de protección de datos personales sea deudora y dependa de cada una de las materias para cuyo ejercicio los ficheros son instrumentales. La reivindicación de las competencias administrativas de la Comunidad Autónoma no proviene de la existencia de un título competencial específico en el Estatuto de Autonomía sino desde la posición de que las potestades de ejecución administrativa y de tutela administrativa de la LORTAD sobre los ficheros de datos personales tienen que ser ejercidas por la Administración, estatal o autonómica, que tenga la titularidad competencial sobre esa materia. Así, si una Comunidad Autónoma tiene la competencia ejecutiva sobre una materia, también la tiene sobre la actividad instrumental relativa a los ficheros de datos personales y a la protección de los datos personales. Por consiguiente, la titularidad de la competencia de la actividad administrativa de regulación y control sobre los ficheros privados y sobre los ficheros de los Ayuntamientos –la tutela administrativa de los ficheros de datos personales– dependerá de la titularidad de la competencia para cuyo ejercicio los ficheros son instrumentales. De lo contrario, la titularidad del instrumento se convertiría en el criterio determinante de la distribución de competencias y no la materia sobre la que verse el fichero.

Desde esta posición, se entiende que las potestades de ejecución administrativa de la LORTAD –la actividad de control y sanción por las infracciones cometidas en los tratamientos de datos personales, además de la inscripción de los ficheros– están vinculadas a las competencias administrativas sobre esa materia establecida en la Constitución y en los Estatutos de Autonomía. Por lo tanto, a los efectos de la competencia de control sobre los ficheros de datos personales, es indiferente que un fichero sea de

titularidad pública o de titularidad privada. Lo determinante es la titularidad competencial que en cada caso le venga atribuida al Estado o a la Comunidad Autónoma en atención a la materia principal de la que dicho fichero sólo es un instrumento técnico.

Este es el planteamiento que justificó que el Gobierno y el Parlamento de Cataluña afirmaran la inconstitucionalidad de la LORTAD por atribuir en exclusiva a la Agencia Española de Protección de Datos el control de todos los ficheros de titularidad privada, cualquiera que fuera la materia sobre la que versen, así como las competencias relativas a la inscripción registral. La LORTAD sería inconstitucional porque niega a las Comunidades Autónomas la facultad de controlar y de inscribir en el Registro autonómico los ficheros de naturaleza privada que versen sobre materias de competencia de las Comunidades Autónomas. Para los recurrentes, la distribución de competencias entre la Agencia Española y las Agencias Autonómicas debe responder y respetar el ámbito competencial en el cual cada fichero opere. La protección de datos no es en sí una materia competencial, por lo que el Estado no puede atribuírsela en virtud de la cláusula residual –art. 149.3 CE– a pesar de que no este expresamente atribuida a las Comunidades Autónomas en sus Estatutos. Los ficheros automatizados no son en sí mismos materia objeto de distribución de competencias, sino más bien instrumento para realizar determinadas actividades. El tratamiento de datos y su protección, como actividades instrumentales, deben subsumirse en el título competencial específico correspondiente, formando parte indisoluble del mismo. Por ello, cualquier Ley que regule la actividad instrumental de tratamiento de datos y el control de los ficheros no puede desconocer la distribución de esas competencias entre el Estado y las Comunidades Autónomas.

Así, las Comunidades Autónomas, a través de las autoridades de control que creen, deberían tener la competencia de control no sólo sobre los ficheros

públicos sino también sobre los ficheros privados que presten servicios en ámbitos materiales sobre los que las Comunidades Autónomas tienen competencias en virtud de lo dispuesto en su Estatuto de Autonomía. Las competencias administrativas de protección de datos de la Comunidad Autónoma, ejercidas a través de sus autoridades de control, serán la que resulten del bloque de la constitucionalidad, de manera que si la Comunidad Autónoma tiene competencias ejecutivas sobre una materia, también las tendrá ejecutivas en lo que respecta al control sobre los ficheros. En cambio, será competencia de la Agencia Española de Protección de Datos el control de los ficheros relativos a actividades de titularidad estatal.

Desde esta perspectiva, no tendría sentido que la Comunidad Autónoma no pudiera inspeccionar y sancionar los ficheros que versen sobre materias atribuidas en exclusiva a la Administración Autonómica, a través de autoridades de control creadas por los Parlamentos autonómicos. Se daría así el sin sentido de que las Comunidades Autónomas podrían inspeccionar determinados ámbitos materiales pero no los ficheros necesarios para su ejercicio. La actividad de control de la Comunidad Autónoma sobre los ficheros en materias de su competencia se vería desnaturalizada. Esto mismo ocurre en relación con el control y a la inscripción registral de los ficheros de las entidades locales, que debe corresponder a la autoridad autonómica de control en virtud de las competencias asumidas en régimen Local por las Comunidades Autónomas a través de sus respectivos Estatutos¹¹.

Sin embargo, la consideración de la protección de datos personales como un derecho fundamental exige un tratamiento conjunto, como el que tiene el régimen jurídico de los demás derechos fundamentales. El derecho fundamental a la protección de datos aconseja su consideración como materia. La materia sometida a distribución competencial no es la informática sino la protección de los datos personales frente al uso de la informática. Lo determinante en este caso, como

señala la STC 290/2000, de 30 de noviembre, es la existencia de un mandato constitucional establecido en el art. 18.4 CE que ha obligado al legislador a limitar el uso de la informática para garantizar el derecho a la intimidad y el libre ejercicio de los derechos. La LORTAD y la LOPD son, pues, Leyes que desarrollan el mandato constitucional de proteger los derechos frente al uso de la informática. Su objetivo no es el uso de la informática, que podría ser accesorio al resto de las materias, sino la protección de los datos personales, protección que como bien constitucional no puede diluirse ni ser medio o instrumento para cualquier otra actividad¹². Así, el art. 1 LORTAD señala que ésta tiene “por objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de los derechos”. Igualmente el art. 1 LOPD señala que ésta “tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar”. Además, el reconocimiento de un derecho fundamental a la protección de datos personales por el Tribunal Constitucional o, al menos, de un bien constitucional como la protección de datos personales frente a los tratamientos de datos que pueden lesionarlo puede quedar desvirtuado o vacío de contenido si la protección de los datos queda relegada a una actividad instrumental de otras materias competenciales. Considerar la protección de datos personal como algo accesorio al resto de las materias –para el Tribunal Constitucional– “soslaya la función que nuestra Constitución ha atribuido a los derechos fundamentales y, en correspondencia, la necesidad de que sean protegidos, incluso en el ámbito del reparto competencial (art. 149.1.1 CE)”¹³.

Las consideraciones acerca de la inconstitucionalidad de la LORTAD parten de que la protección de datos personales no es una materia en sentido estricto lo que impediría su calificación de competencia residual

reclamada por el Estado al no haber sido asumida por los Estatutos de Autonomía –art. 149.3 CE–. La aceptación de que la protección de datos personales es una mera actividad instrumental absorbida por la materia a la que sirve el fichero en cuestión no conllevaría directamente la disgregación del régimen jurídico de la protección de datos, poniendo en riesgo el fin garantista del art. 18.4 CE –como afirma el Tribunal Constitucional–, ya que quedaría la legislación básica del Estado que establece los principios y los derechos de protección de datos personales en todo el territorio nacional, sin perjuicio de que exista una legislación de desarrollo en las distintas Comunidades Autónomas. No obstante, sí obligaría a determinar para cada fichero la existencia o no de una legislación autonómica de desarrollo y cuál es la autoridad administrativa competente que ejerce en ese fichero las funciones administrativas de regulación, supervisión y sanción, ya que esta autoridad variaría dependiendo de los concretos títulos competenciales de cada actividad que justifica la creación de un fichero.

No olvidemos, como hemos señalado antes, que la distribución constitucional de competencias entre el Estado y las Comunidades Autónomas permite tanto la reserva en exclusiva de materias al Estado y a las Comunidades Autónomas –donde cada instancia tiene la competencia exclusiva para desarrollar las funciones legislativas y ejecutivas– como la existencia de competencias compartidas sobre una misma materia, de forma que la función legislativa le corresponda, por ejemplo, al Estado y la función ejecutiva a las Comunidades Autónomas, o incluso, que la competencia legislativa se encuentre también compartida, atribuyéndose al Estado la legislación básica y a las Comunidades Autónomas la legislación de desarrollo. Por ello, hacer depender la competencia sobre la legislación de desarrollo y sobre la ejecución administrativa de protección de datos de la titularidad de la materia sobre la cual el fichero es instrumental supondría establecer una gran complejidad en el mapa de distribución de competencias al trasladar toda la complejidad

constitucional del deslinde competencial de todas las materias a un mismo ámbito. Así, habría ficheros privados cuya competencia exclusiva le correspondería al Estado, ficheros privados donde la competencia legislativa le correspondería al Estado y la ejecutiva a las Comunidades Autónomas, y ficheros privados donde el Estado tendría sólo la legislación básica, atribuyéndose a las Comunidades Autónomas la legislación de desarrollo y la competencia administrativa de control. O dicho de otro modo, la Comunidad Autónoma tendría la competencia legislativa de desarrollo y la competencia de ejecución administrativa sobre algunos ficheros, mientras que para otros tendría únicamente la competencia ejecutiva. Igualmente, el Estado tendría la competencia de la legislación básica sobre todos los ficheros, manteniendo únicamente la competencia de ejecución administrativa sobre algunos de ellos. Lógicamente, esta distribución podría variar en cada Comunidad Autónoma dependiendo de las competencias asumidas por éstas últimas.

Este modelo tendría como único común denominador –como régimen jurídico común– la legislación básica del Estado que desarrolla el contenido del derecho fundamental a la protección de datos personales, al tiempo que se generaría una gran variabilidad en el régimen jurídico de protección de datos aplicable a cada fichero –de las facultades de desarrollo legislativo y de ejecución administrativa–. Se trasladaría, así, a la protección de datos la misma variabilidad que presentan las distintas materias en relación al reparto de funciones legislativas y ejecutivas entre el Estado y las Comunidades Autónomas. Así, la regulación y la ejecución administrativa de protección de datos variaría dependiendo en cada materia, de las competencias de tipo funcional –legislación y ejecución, y de las propias bases, que pueden variar en intensidad y ejecución. Por tanto, la consideración de la protección de datos no como materia sino absorbida por las distintas materias facilita no tanto la configuración de una pluralidad de regímenes

jurídicos estatales y autonómicos en cada una de las materias –ya que el régimen jurídico estatal o autonómico puede mantenerse– sino una falta de homogeneidad en el régimen jurídico de protección de datos en cada uno de los ámbitos en los que existen ficheros, con los riesgos que esto supone para la seguridad jurídica. Este planteamiento representaría una fragmentación competencial de la protección de datos compleja de gestionar. Así, un mismo responsable podría tener algunos ficheros sometidos a la legislación de desarrollo autonómica mientras que otros no, y ficheros cuya competencia de control la ejerce la Agencia Española y la Agencia Autonómica. Esto afectaría no sólo al responsable del fichero sino al propio titular de los datos que debería averiguar en cada caso a quién le corresponde la competencia para la legislación de desarrollo, para las funciones de inspección, supervisión, sanción e inscripción registral, lo que podría dificultar en una materia de por sí compleja, la tutela de los derechos en este ámbito. En todo caso, hay que reconocer que parte de la complejidad expuesta se da en la actualidad, por ejemplo, en los ficheros de los Colegios Profesionales, ya que sus ficheros públicos están sometidos a la legislación de desarrollo y a la competencia administrativa de control de la Comunidad Autónoma, mientras que en los ficheros privados de los Colegios Profesionales ambas funciones le corresponden al Estado¹⁴.

1.3. MARCO CONSTITUCIONAL Y REFORMA ESTATUTARIA: POSIBILIDADES PARA EL FUTURO.

Hemos visto que el derecho a la protección de datos personales es una materia constitucional y que, como derecho fundamental, le corresponde al Estado “la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales” –art. 149.1.1 CE–. Por tanto, le corresponde al Estado la competencia de la legislación básica sobre esta materia, que ha sido

desarrollada sucesivamente a través de la LORTAD y de la LOPD.

La Constitución no dice nada acerca de a quién le corresponde la competencia de ejecución administrativa de protección de datos personales, es decir, las funciones de regulación, supervisión, sanción e inscripción de ficheros. Tampoco dicen nada los Estatutos de Autonomía por lo que, a partir de la cláusula residual del art. 149.1.3º CE, estas competencias corresponderían al Estado. Este es el motivo por el que el Estado ha atribuido a la Agencia Española las competencias de ejecución administrativa de protección de datos personales sobre los ficheros privados y, en la primera regulación llevada a cabo por la LORTAD, también sobre los ficheros de los Ayuntamientos. La LORTAD y la LOPD materializan, de esta forma, la distribución competencial sobre protección de datos personales.

Este es el actual marco constitucional, desarrollado legalmente, que no atribuye el control sobre los ficheros privados a las Agencias Autonómicas de Protección de Datos Personales. Lógicamente, este marco puede ser modificado en el futuro de dos formas distintas: por una parte, a través de las reformas de los Estatutos de Autonomía, que podrían asumir la materia de protección de datos personales; por otra, a través de una modificación de la LOPD, que atribuyera a las Agencias Autonómicas mayores competencias de ejecución administrativa sobre protección de datos personales.

La asunción por las Comunidades Autónomas de la protección de datos personales en sus respectivos Estatutos de Autonomía tiene la virtualidad de otorgar una mayor estabilidad a la distribución competencial, al incluirla dentro del bloque de la constitucionalidad. Las reformas estatutarias actualmente en perspectiva pueden ser una buena oportunidad para la inclusión de esta materia por el estatuyente. De hecho, los proyectos de Estatuto de Autonomía para Cataluña y para Canarias incluyen la protección de datos personales como competencia de estas

Comunidades Autónomas, extendiendo el ámbito de control de las autoridades autonómicas a los ficheros privados. No hacen lo mismo los distintos proyectos de reforma del Estatuto de Autonomía del País Vasco, de Andalucía o de Valencia. En este ámbito no existe hasta el momento un título competencial claro, por lo que en ausencia de asunción de las competencias por los Estatutos de Autonomía se debe estar a la legislación orgánica del Estado, que tanto podría ampliar las competencias de las Comunidades Autónomas como reducirlas¹⁵.

Otra vía para la atribución a las Comunidades Autónomas de mayores facultades de control sobre los tratamientos de datos personales reside en la modificación de la legislación estatal –la LOPD– a estos efectos. Esta vía tiene la dificultad de que no supone una asunción de la competencia de ejecución administrativa por parte de la Comunidad Autónoma, ya que ésta siempre estaría a expensas de que no se produjera una reforma *in peius* –poco probable– de la legislación estatal en el futuro.

Por tanto, la decisión acerca del concreto modelo de distribución de competencias entre el Estado y las Comunidades Autónomas en protección de datos personales le corresponde al estatuyente y al legislador. A ellos les toca definir cuál debe ser el modelo organizativo y de policía administrativa más adecuado para el respeto al derecho fundamental a la protección de datos personales. A ellos les corresponde en virtud de criterios de oportunidad política, administrativa y organizativa establecer qué autoridad, estatal o autonómica está mejor situada comparativamente y más capacitada para hacer respetar el derecho. Esta no es una cuestión que deje cerrada la Constitución y entenderlo así es un claro quebranto del orden constitucional que también establece un Estado autonómico.

En este punto, la Sentencia del Tribunal Constitucional 290/2000, de 30 de noviembre, comete a nuestro juicio varios errores que se evidencian especialmente en los F. J. 8º y 9º. Es cierto que en las normas legales

de los países europeos que desarrollan el derecho fundamental a la protección de datos personales está presente el elemento institucional que ha creado instituciones especializadas de derecho público. El proyecto de Constitución Europea, además del reconocimiento del derecho a la protección de datos de carácter personal, establece que “el respeto de estas normas estará sujeto al control de una autoridad independiente”. Sin embargo, no se puede afirmar como hace la Sentencia que a las instituciones nacionales se le atribuyen funciones de control sobre los ficheros de datos personales susceptibles de tratamiento automatizado, tanto de titularidad pública como privada, ya que, por ejemplo, en Alemania, país citado expresamente por la Sentencia, el control de los ficheros privados le corresponde a las Agencias de los Länder o Estados, y no a la autoridad federal. Una cosa es que las leyes europeas regulen a la vez los tratamientos públicos y los privados, y otra cosa distinta es que atribuyan la labor de policía administrativa a la misma autoridad de control.

De hecho, como hemos señalado anteriormente, no es una exigencia constitucional la atribución exclusiva a la Agencia Española de la función de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial respecto a los derechos de información, acceso, rectificación y cancelación de datos. Así, las distintas funciones de intervención y control como la función de inscripción registral en lo relativo a los ficheros públicos y privados pueden ser desarrolladas igualmente por las autoridades autonómicas de control. La determinación de quién debe ejercer estas potestades administrativas le corresponde al legislador, o al estatuyente autonómico, ya que no existe mandato ni límite constitucional alguno.

Tampoco es acertada la afirmación de la Sentencia del Tribunal Constitucional 290/2000, de 30 de noviembre, de que hay “un rasgo significativo de la Agencia de Protección de Datos: el carácter básicamente preventivo de sus funciones en orden a

la protección de datos personales”. De hecho, el rasgo que distingue a las autoridades autonómicas de protección de datos personales y que las diferencia de la Agencia Española, es la labor preventiva, desarrollada a través de una intensa actividad consultiva –de resolución de consultas–, de consultoría y apoyo a los responsables de ficheros y de formación a los empleados públicos. En cambio, la Agencia Española se encuentra más centrada en el aspecto subjetivo –de protección jurisdiccional– y menos preventivo del derecho fundamental a la protección de datos personales¹⁶. Así, han sido principalmente las autoridades autonómicas las que han puesto en marcha la voluntad de la LORTAD¹⁷ de “implantar mecanismos cautelares que prevengan las violaciones de los derechos fundamentales”¹⁸. Por ello, no es correcto afirmar como hace el Tribunal que es “este carácter tuitivo o preventivo el que, en última instancia, justifica la atribución de tales funciones y potestades a la Agencia de Protección de Datos para asegurar, mediante su ejercicio, que serán respetados tanto los límites al uso de la informática como la salvaguardia del derecho fundamental a la protección de datos personales en relación con todos los ficheros, ya sea de titularidad pública o privada”. El carácter tuitivo y preventivo justificaría, en todo caso, la atribución de estas funciones a las autoridades autonómicas.

El error de mayor calado se encuentra en el Fundamento Jurídico 13º de la Sentencia del Tribunal Constitucional 290/2000, de 30 de noviembre, donde se afirma que la justificación de las competencias que la LORTAD atribuye a la Agencia Española de Protección de Datos “se halla estrechamente relacionado no sólo con el mandato del art. 18.4 CE sino con el primero de dichos presupuestos, el derecho fundamental a la protección de datos personales frente al uso de la informática”. Es decir, las funciones de control de los ficheros privados y de los ficheros de los Ayuntamientos es una consecuencia de la necesidad de garantizar a los ciudadanos el ejercicio del haz de facultades que integra el contenido del derecho fundamental. Para el

Alto Tribunal, mediante la creación de la Agencia de Protección de Datos se ha querido velar por la puntual observancia de los límites al uso de la informática que la LORTAD establece para los responsables de los ficheros de datos personales, y garantizar también el ejercicio por los ciudadanos del derecho fundamental a la protección de dichos datos mediante la actuación preventiva por parte de los citados órganos. Esto lleva a decir al Tribunal Constitucional que “junto a la normación como aspecto esencial del art. 149.1.1 CE las regulaciones estatales dictadas al amparo de este precepto también pueden contener, cuando sea imprescindible para garantizar la eficacia del derecho fundamental o la igualdad de todos los españoles en su disfrute, una dimensión institucional”. La Agencia Española de Protección de Datos sería para el Alto Tribunal el órgano adecuado para la ejecución administrativa y de garantía de este derecho fundamental¹⁹. De ahí, el Tribunal Constitucional afirma que “la exigencia constitucional de protección de los derechos fundamentales en todo el territorio nacional requiere que éstos, en correspondencia con la función que poseen en nuestro ordenamiento (art. 10.1 CE), tengan una proyección directa sobre el reparto competencial entre el Estado y las Comunidades Autónomas «ex» art. 149.1.1 CE para asegurar la igualdad de todos los españoles en su disfrute. Asimismo, que dicha exigencia faculta al Estado para adoptar garantías normativas y, en su caso, garantías institucionales”. Y continúa: “A este fin la LORTAD ha atribuido a la Agencia de Protección de Datos diversas funciones y potestades, de información, inspección y sanción, para prevenir las violaciones de los derechos fundamentales antes mencionados. Y dado que la garantía de estos derechos, así como la relativa a la igualdad de todos los españoles en su disfrute es el objetivo que guía la actuación de la Agencia de Protección de Datos, es claro que las funciones y potestades de este órgano han de ejercerse cualquiera que sea el lugar del territorio nacional donde se encuentren los ficheros automatizados conteniendo datos de carácter personal y sean quienes sean los responsables de tales ficheros”.

Esto es resaltado en el F. J. 15º: “En definitiva, es la garantía de los derechos fundamentales exigida por la Constitución así como la de la igualdad de todos los españoles en su disfrute la que en el presente caso justifica que la Agencia de Protección de Datos y el Registro Central de Protección de Datos pueden ejercer las funciones y potestades a las que antes se ha hecho referencia respecto a los ficheros informatizados que contengan datos personales y sean de titularidad privada”.

Sin embargo, como hemos reiterado anteriormente, el derecho fundamental a la protección de datos personales puede ser igualmente tutelado a través de las autoridades autonómicas de control, que pueden ejercer las funciones propias de la Agencia Española de Protección de Datos, y cuyas decisiones están sometidas al control de los órganos jurisdiccionales. Lo trascendental del mandato constitucional del art. 18.4 CE de limitar el uso de la informática para garantizar los derechos y libertades de las personas, en relación con el art. 149.1.1 CE que exige la regulación de las condiciones básicas que garanticen la igualdad en el ejercicio de los derechos, es que los límites al uso de la informática sean los mismos en todo el territorio nacional y que estén vigentes en todo el territorio los mismos principios de protección de datos y los mismos derechos de los titulares de los datos. Es la proyección general de la LORTAD y de la actual LOPD en todo el territorio nacional lo que materializa el cumplimiento de estas exigencias constitucionales. La cláusula del art. 149.1.1 CE va encaminada a buscar la igualdad en el ejercicio de los derechos fundamentales por todos los españoles a través de la existencia de una legislación básica del Estado, de forma que la existencia de un Estado descentralizado no suponga una merma en el disfrute de los derechos. En ningún caso trata de prejuzgar la distribución de las competencias de ejecución administrativa ni supone una exigencia para que estas funciones sean desarrolladas por la Agencia Española de Protección de Datos y no por las Agencias Autonómicas. La regulación de las condiciones básicas que garanticen la igualdad de

todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales se produce ya a través de la LORTAD y de la LOPD, que establecen unos principios y unos derechos de protección de datos comunes en todo el territorio nacional. Así, la normativa de protección de datos es lo suficientemente clara para que las funciones de ejecución administrativa –de inspección, de sanción y de inscripción de los ficheros– puedan ser aplicadas por las autoridades autonómicas sin mayor riesgo de discrecionalidad que pueda vulnerar la igualdad en el ejercicio de este derecho fundamental, o por lo menos, no mayor riesgo que otros ámbitos que son competencia de las Comunidades Autónomas²⁰.

Así, el Estado no puede erigirse en garante último y único del derecho fundamental a la protección de datos personales porque esta es una función que corresponde a todos los poderes públicos ex art. 9.2 CE, especialmente a las Comunidades Autónomas en el ámbito de sus competencias. La actividad administrativa de control de los ficheros y de ejecución de la legislación también puede ser desarrollado por las Comunidades Autónomas en el ámbito de los ficheros de titularidad privada de su territorio. Como hemos señalado, la atribución de competencias ejecutivas a la Agencia Española de Protección de Datos no puede considerarse regulación de las “condiciones básicas” a los efectos del art. 149.1.1 CE. La regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio del derecho fundamental a la protección de datos personales hacen referencia no a la organización administrativa de la protección de datos, sino al desarrollo de los principios y de los derechos de protección de datos personales, tanto por la LORTAD como por la LOPD, lo que obliga a las Comunidades Autónomas, tanto en su actividad legislativa, como en la actividad de ejecución administrativa y de control de ficheros a respetar siempre el desarrollo legislativo del derecho fundamental a la protección de datos personales. En apoyo de esta posición, se puede añadir que estamos hablando de un ámbito como la protección

de datos, que tiene la consideración de derecho fundamental a través de una compleja hermenéutica constitucional y no de una interpretación literal de la Constitución, donde no se reconoce abiertamente el derecho, sino que sólo se indica que la ley “limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de los derechos”. Por eso, no puede derivarse de este derecho fundamental nuevo una extensa regulación de las condiciones básicas que limite las competencias ejecutivas de las Comunidades Autónomas.

La mejor demostración de que no existe un mandato constitucional que imponga un determinado modelo de distribución competencial entre el Estado y las CCAA en materia de protección de datos y de que no es imprescindible el control de la Agencia Española sobre los ficheros para garantizar la vigencia del derecho fundamental es la propia modificación de la LORTAD, a través de la LOPD, que ha atribuido a las autoridades autonómicas el control sobre los tratamientos de datos personales de titularidad municipal. Por tanto, tampoco sería inconstitucional que las autoridades autonómicas controlaran los ficheros privados y desempeñaran las competencias de ejecución administrativa en este ámbito. Esta es, sencillamente, una decisión política cuya oportunidad debe valorarse. Además, la LOPD ha modificado la redacción inicial de la LORTAD para atribuir a las autoridades autonómicas las potestades de inspección que solo tenía la Agencia Española²¹.

Analizado ya cuál es el marco constitucional y legal de distribución de competencias entre el Estado y las Comunidades Autónomas en protección de datos personales y cuáles son los procedimientos para su modificación, nos corresponde ahora llevar a cabo una valoración sobre la mayor o menor oportunidad para su alteración. Es decir, desarrollado ya el análisis de constitucionalidad y de legalidad sobre el actual marco jurídico, vamos a llevar a cabo ahora un juicio de oportunidad sobre la conveniencia de su reforma, de las posibles direcciones en el futuro, desde un

planteamiento de ciencia política o de ciencia de la Administración²².

Son distintos los argumentos que se pueden esgrimir para justificar una mayor centralización en esta materia y para que corresponda a la Agencia Española de Protección de Datos las competencias de ejecución administrativas relativas a los ficheros privados:

En primer lugar, esta opción facilita la unidad de criterio y la uniformidad en la ejecución de la legislación, lo que favorece –aunque no sea un requisito *sine qua non*– la igualdad de todos los españoles en este derecho fundamental.

En segundo lugar, hay que tener en cuenta que el tráfico de datos entre ficheros privados desborda habitualmente el espacio de una sola Comunidad Autónoma, por lo que la atribución de facultades de control a una autoridad central asegura una mejor tutela de las lesiones de derechos de personas provenientes de diferentes Comunidades Autónomas. Las empresas privadas tienen una actividad que se desarrolla habitualmente en más de una Comunidad Autónoma, consecuencia también del principio de unidad de mercado²³. Es decir, los titulares de los datos que figuran en un fichero privado residen habitualmente en más de una Comunidad Autónoma. En cambio, los titulares de los datos que figuran en ficheros públicos tienen la vecindad en una única Comunidad Autónoma. De hecho, el criterio de la vecindad es definitivo a la hora de empadronarse en un Municipio y pertenecer a una Comunidad Autónoma. Además, las frecuentes externalizaciones de servicios provocan en muchos casos que el responsable del fichero resida en una Comunidad Autónoma, perteneciendo el encargado de tratamiento a otra Comunidad, lo que dificultaría el control por parte de las Agencias Autonómicas²⁴.

Por eso, a nuestro parecer, el criterio de distribución competencial establecido en el art. 41 LOPD, si bien no es el único posible, es razonable. Al mismo tiempo,

no hay que desmerecer las competencias de control de las Agencias Autonómicas sobre los ficheros públicos, en un país en el que el sector público ocupa el 40% del Producto Interior Bruto. Eso no obsta para que las Agencias Autonómicas puedan colaborar, a través de Convenios con la Agencia Española, en la actividad inspectora sobre ficheros privados en su ámbito territorial. Esta posibilidad parece más adecuada que el establecimiento de delegaciones de la Agencia Española de Protección de Datos en las Comunidades Autónomas, posibilidad ésta que iría en dirección contraria en una etapa caracterizada por la descentralización de competencias por parte de la Administración General del Estado y por la Administración única, a partir sobre todo de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado. A nuestro modo de ver, la principal ampliación de las competencias de las Agencias Autonómicas de Protección de Datos debe de venir, no del control de los ficheros privados, sino de la garantía del derecho de acceso a archivos y documentos administrativos –arts. 105.b) CE y art. 37 LRJAPyPAC–, y de la compatibilidad entre la protección de datos personales y el principio de transparencia administrativa. Hay que recordar, como ya hemos hecho en otras ocasiones, la compleja distinción existente entre el derecho de acceso a archivos y documentos administrativos y el derecho fundamental a la protección de datos personales, especialmente desde que la Directiva 95/46/CE y la LOPD han extendido la protección no sólo a los tratamientos automatizados sino también a los manuales.

No obstante, también hay razones que aconsejan la atribución de las principales competencias de ejecución administrativa a las autoridades autonómicas de control. Entre esas razones estaría la dificultad para que la Agencia Española pueda hacer cumplir la legislación y garantizar los derechos de las personas en este ámbito, debido tanto a los incrementos de los tratamientos de datos personales en soporte informático consecuencia de la sociedad de la información y la comunicación, como a la

ampliación del ámbito de aplicación de la LOPD –art. 2– que modifica la LORTAD para extenderlo a los ficheros manuales, y, por último, a la atribución de nuevas competencias a la Agencia Española de Protección de Datos relativas a los correos electrónicos no deseados. Por ello, una solución intermedia podría ser la atribución a las Agencias Autonómicas de la competencia de control de algunos ficheros privados muy concretos –los relativos a pequeñas empresas y comercios–, correspondiendo a la Agencia Española el control sobre los ficheros de empresas privadas de nivel nacional o que prestan servicios públicos en el ámbito nacional –telecomunicaciones, suministro eléctrico, correos, etc–.

2 ■ LA CREACIÓN DE AGENCIAS AUTONÓMICAS DE PROTECCIÓN DE DATOS Y LA GARANTÍA DE LA INDEPENDENCIA

En España, como es sabido, la Agencia Española de Protección de Datos se crea en 1992, al amparo de la Ley Orgánica 5/1992 –LORTAD–, y se pone en funcionamiento en 1994²⁵. La primera Agencia de Protección de Datos Autonómica se crea en la Comunidad de Madrid, en virtud de la Ley 13/1995, de 21 de abril, de regulación del uso de la informática en el tratamiento de datos personales por la Comunidad de Madrid, modificada por la Ley 13/1997, de 16 de junio, todo ello al amparo de la LORTAD²⁶. Posteriormente se ha aprobado la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid –LPD de la Comunidad de Madrid–, ya mencionada, al amparo de la Ley 15/1999. La Agencia de Protección de Datos de la Comunidad de Madrid se puso en funcionamiento en julio de 1997, con el nombramiento de los primeros miembros del Consejo de Protección de Datos, quienes, en sesión constitutiva propusieron al Presidente de la Comunidad el nombramiento del primer Director²⁷. Es decir, la Agencia de Protección de Datos de la

Comunidad de Madrid tiene una antigüedad de ocho años²⁸. Posteriormente se ha aprobado la Ley de la Comunidad Autónoma de Cataluña 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos²⁹, que entró en funcionamiento en junio de 2003 con la sesión constitutiva del Consejo Asesor de Protección de Datos de Cataluña³⁰. Por último, se ha aprobado recientemente la Ley de la Comunidad Autónoma Vasca 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 Datos³¹. En esta misma dirección se están moviendo otras Comunidades Autónomas³². En la Comunidad de Valencia se está elaborando el Anteproyecto de creación de la Agencia Valenciana de Protección de Datos³³, en Castilla-la Mancha, de la Agencia Castellano-Manchega de Protección de Datos³⁴. En Galicia el Gobierno aprobó el Proyecto de Ley de creación de la *Autoridade Galega de Protección de Datos*, que decayó en su tramitación parlamentaria por la disolución del Parlamento Gallego³⁵. Igualmente, entró en el Parlamento Andaluz, en el año 2003 una proposición de Ley de creación de la Agencia Andaluza de Protección de Datos, que decayó al finalizar la legislatura³⁶. El término Agencia, en todo caso, no parece el más adecuado para definir a una Administración independiente, ya que esa misma expresión se emplea para otros organismos públicos que carecen de esa independencia como la Agencia Tributaria, la Agencia del Menor, las Agencias de Desarrollo regional, etc, que en muchos casos –como las dos últimas– no desarrollan funciones de regulación, supervisión y sanción. Una expresión más adecuada a las funciones y a la organización podría ser la de Autoridad.

Tanto el proyecto de Constitución Europea como la Directiva Comunitaria y la legislación española establecen que los órganos de tutela de este derecho fundamental tendrán la consideración de autoridades de control y deben de tener como característica la independencia³⁷. El proyecto de Constitución Europea afirma en el art I-51 que el respeto al derecho a la

protección de datos personales “estará sometido al control de autoridades independientes”. Así, la Exposición de Motivos (52) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo señala que “la creación de una autoridad de control que ejerza sus funciones con plena independencia en cada uno de los Estados miembros constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales”. El art. 41.1 *in fine* LOPD señala que las Agencias Autonómicas tienen “la consideración de autoridades de control, a los que [las Comunidades Autónomas] garantizarán plena independencia y objetividad en el ejercicio de su cometido”, Esto obliga a que la Legislación autonómica establezca para estas Agencias un conjunto de garantías de independencia, de la misma manera que lo hizo la LORTAD y la LOPD para la Agencia Española de Protección de Datos del Estado. Así, el art. 35 LOPD señala que la Agencia Española de Protección de Datos “actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones”. Al mismo tiempo, el Director de la Agencia Española es nombrado por un período de cuatro años y ejerce sus funciones con plena independencia y objetividad, no estando sometido “a instrucción alguna en el desempeño de aquéllas”. Estas garantías de independencia son refrendadas y ampliadas por el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.

Así, el art. 1.1 de la LPD de la Comunidad de Madrid señala que la Agencia de Protección de Datos de la Comunidad de Madrid es un Ente de Derecho Público, con personalidad jurídica propia y plena capacidad de obrar, que “actúa en el ejercicio de sus funciones con plena independencia de la Administración de la Comunidad de Madrid”. El art. 2 de la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos señala que esta institución “actúa con objetividad y plena independencia de las Administraciones Públicas en el ejercicio de sus funciones”. La Ley de la Comunidad Autónoma Vasca 2/2004, de 25 de febrero, afirma que

la Agencia Vasca de Protección de Datos “actúa con plena independencia de las administraciones públicas en el ejercicio de sus funciones”³⁸. Por tanto, estas Agencias autonómicas, como la Agencia Española de Protección de Datos, forman parte de la categoría de las Administraciones independientes. Están dotadas de un conjunto de garantías formales de independencia –autonomía de personal, autonomía normativa, autonomía presupuestaria–, entre la que destacaría la inamovilidad del Director de la Agencia durante su mandato, que sólo puede verse limitado por unas causas tasadas de cese, susceptibles de revisión jurisdiccional³⁹. Es decir, no existe poder de remoción del Gobierno de la Comunidad Autónoma sobre el Director de la Agencia de Protección de Datos de la Comunidad de Madrid –art. 15 LPD de la Comunidad de Madrid–, sobre el Director de la Agencia Catalana de Protección de Datos –art. 13 Ley 5/2002, de 19 de abril– o sobre el Director de la Agencia Vasca –art. 15.3 de la Ley 2/2004–⁴⁰. Al mismo tiempo, las Agencia de Protección de Datos Autonómicas disponen de una garantía sustancial de independencia, al no estar sometidas a órdenes, instrucciones ni a directrices administrativas. Así, el Director de la Agencia de Protección de Datos de la Comunidad de Madrid ejerce sus funciones “con plena independencia y objetividad, sin estar sujeto a mandato imperativo o instrucción alguna en el desempeño de aquéllas” –art. 16.2 LPD de la Comunidad de Madrid–; el Director de la Agencia Catalana “ejercerá sus funciones con plena independencia y objetividad sin estar sujeto a mandato imperativo ni a instrucción” –art. 13.2 de la Ley 5/2002, de 19 de abril–; el Director de la Agencia Vasca “ejercerá sus funciones con plena independencia y objetividad y no estará sujeto a instrucción alguna en el desempeño de aquella” –art. 15.2 de la Ley 2/2004–⁴¹. Esto significa que la relación que hay entre el Gobierno de la Comunidad y las Agencias de Protección de Datos autonómicas no es de jerarquía –como es la relación entre el Consejo de Gobierno, las Consejerías y las Direcciones Generales de la Comunidad Autónoma–, ni de tutela –como es la relación entre el Gobierno de

la Comunidad Autónoma y su Administración institucional–⁴².

La independencia de las Agencias de Protección de Datos de las Comunidades Autónomas del Gobierno de la Comunidad facilita el trabajo de inspección y su legitimidad como Autoridad de control de cara a otras Entidades públicas como las Administraciones Locales, las Universidades Públicas y los Colegios Profesionales, que tienen en algunos casos una autonomía constitucionalmente reconocida a través de una garantía institucional –arts. 27.10, 137 y 140 de la Constitución Española–. De igual forma, la independencia de la Agencia Española de Protección de Datos del Gobierno facilita su actividad de control sobre los ficheros públicos de aquellas Comunidades Autónomas que no hayan creado todavía su Agencia de Protección de Datos de carácter autonómico.

3 ■ LAS FUNCIONES DE LAS AGENCIAS DE PROTECCIÓN DE DATOS AUTONÓMICAS Y LA DELIMITACIÓN DE COMPETENCIAS ENTRE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS Y LAS AGENCIAS AUTONÓMICAS EFECTUADA EN LAS LEYES ESTATALES Y AUTONÓMICAS: LA VISIÓN DEL LEGISLADOR

El art. 37 LOPD ⁴³– establece como funciones de la Agencia de Protección de Datos: “a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos. b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias. c) Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley. d) Atender las peticiones y reclamaciones formuladas por las personas afectadas. e) Proporcionar información a las personas acerca de sus derechos

en materia de tratamiento de los datos de carácter personal. f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones. g) Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley⁴⁴. h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley. i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones. j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine. k) Redactar una memoria anual y remitirla al Ministerio de Justicia. l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales⁴⁵. m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46. n) Cuantas otras le sean atribuidas por normas legales o reglamentarias”.

La LOPD en el art. 41 atribuye a los órganos correspondientes de las Comunidades Autónomas todas las funciones propias de la Agencia Española de Protección de Datos, recogidas en el art. 37 LOPD, a excepción de tres funciones: velar por la publicidad de la existencia de los ficheros de datos de carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información que el Director de la Agencia determine –j–; redactar una

memoria anual y remitirla al Ministerio de Justicia –k–; ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales –l–, y, en relación con estas mencionadas transferencias internacionales de datos, requerir a los responsables y encargados de los tratamientos para adoptar las medidas necesarias para adecuar los tratamientos de datos a las disposiciones de esta Ley, ordenar la cesación de los tratamientos y la cancelación de los ficheros cuando no se ajusten a sus disposiciones y ejercer la potestad sancionadora⁴⁶.

La excepción del art. 41 relativa a las transferencias internacionales de datos es consecuencia, no sólo de que las relaciones internacionales son competencia exclusiva del Estado –art. 149.1.3º Constitución Española–, sino de un principio de eficacia práctica y de unicidad de interlocutor para cada uno de los Estados⁴⁷. El propio Estatuto de la Agencia de Protección de Datos señala –art. 9– que corresponde a la Agencia la cooperación con organismos internacionales y órganos de las Comunidades Europeas en materia de protección de datos. Eso no obsta para que las Agencias Autonómicas intervengan progresivamente en la definición de la posición española en materia de protección de datos en el ámbito de la Unión Europea y de los organismos internacionales, dentro de la tendencia hacia una mayor implicación de las Comunidades Autónomas en el ámbito internacional⁴⁸. Las otras dos competencias que inicialmente aparecen excepcionadas –publicación de una Memoria y publicidad de los ficheros– no son tanto competencias reservadas a la Administración del Estado –de hecho las Agencias Autonómicas también elaboran una memoria anual y velan por la publicidad de los ficheros⁴⁹– sino materias que, en todo caso, deben ser desarrolladas por la Agencia Española de Protección de Datos, sin perjuicio de que también sean desarrolladas por las Agencias de Protección de Datos Autonómicas.

Es decir, todas las funciones de la Agencia Española de Protección de Datos reguladas en el art. 37 LOPD pueden ser desarrolladas en su ámbito competencial definido legalmente por los Organos correspondientes de las Comunidades Autónomas: velar por el cumplimiento de la legislación y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación y cancelación; emitir las autorizaciones previstas en la Ley; dictar las instrucciones para adecuar los tratamientos a los principios de la Ley; atender las peticiones y reclamaciones formuladas por las personas afectadas; dar información a las personas acerca de sus derechos; requerir a los responsables y los encargados de los tratamientos para adoptar las medidas necesarias para adecuar los tratamientos a las disposiciones de la Ley, ordenar la cesación de los tratamientos y la cancelación de los ficheros; ejercer la potestad sancionadora⁵⁰; informar con carácter preceptivo de los proyectos de disposiciones generales que desarrollen esta Ley, etc.⁵¹.

El hecho de que las Agencias de Protección de Datos Autonómicas desarrollen también como la Agencia Española funciones de inspección, supervisión y sanción, que pueden ser consideradas materialmente jurisdiccionales, es lo que justifica que estas Agencias Autonómicas dispongan de algunas de las garantías de independencia de los órganos jurisdiccionales. Las razones que justifican la independencia de la que gozan las Agencias de Protección de Datos Autonómicas en relación con los Gobiernos de sus Comunidades Autónomas son las mismas que justifican la independencia de la Agencia Española de Protección de Datos, con respecto al Gobierno del Estado.

Además, hay otros preceptos de la LOPD que mencionan o reiteran competencias de las Agencias de Protección de Datos tanto española como autonómicas, éstas últimas siempre en el ámbito competencial del art. 41 LOPD, es decir, en relación con los ficheros creados y gestionados por la propia Comunidad Autónoma o por las entidades

integrantes de la Administración Local, dentro de su ámbito territorial. Así, la LOPD se refiere a las Agencias Autonómicas para la tutela de los derechos de acceso, rectificación, cancelación y oposición –art. 18.2–; en lo relativo a las excepciones a esos derechos –art. 23.2 LOPD–; en lo relativo a la inscripción de los códigos de tipo que podrán inscribirse en los registros autonómicos –art. 32.3 LOPD–; en relación al ejercicio de las potestades de inspección por las autoridades de control –art. 40.1 LOPD; o en lo que respecta a las Resoluciones de las Agencias autonómicas que finalizan la vía administrativa en el procedimiento sancionador –art. 48 LOPD–.

Nos corresponde ahora analizar la delimitación de las competencias entre la Agencia Española y las Agencias Autonómicas de Protección de Datos que han efectuado las leyes estatales y autonómicas. El art. 41 LOPD señala que los órganos correspondientes de las Comunidades Autónomas ejercerán las funciones ya mencionadas sobre los ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial. En esta dirección, el art. 2.1 LPD de la Comunidad de Madrid establece que la Agencia de Protección de Datos de la Comunidad de Madrid ejerce sus funciones de control sobre los ficheros de datos de carácter personal creados o gestionados por las Instituciones de la Comunidad de Madrid y por los Organos, Organismos, Entidades de Derecho Público y demás Entes públicos integrantes de su Administración Pública, exceptuándose las sociedades mercantiles que formen parte de la Administración Institucional de la Comunidad de Madrid. Asimismo, la Agencia de Protección de Datos ejerce sus funciones de control sobre los ficheros de datos de carácter personal creados o gestionados por los Entes que integran la Administración Local del ámbito territorial de la Comunidad de Madrid, así como los ficheros creados o gestionados por las Universidades públicas y por las Corporaciones de derecho público representativas de intereses

económico y profesionales de la Comunidad de Madrid, en éste último caso siempre y cuando dichos ficheros sean creados o gestionados para el ejercicio de potestades de derecho público –art. 2.2 LPD de la Comunidad de Madrid–. Este ha sido también el criterio seguido por la Ley Vasca 2/2004, de 25 de febrero, en la atribución de competencias a la Agencia Vasca de Protección de Datos. En ella se afirma el control de esta Agencia sobre los ficheros de la Administración General de la Comunidad Autónoma, los órganos forales de los territorios históricos y las administraciones locales del ámbito territorial de la Comunidad Autónoma del País Vasco, así como los entes públicos de cualquier tipo, dependientes o vinculados a las respectivas administraciones públicas, en tanto que los mismos hayan sido creados para el ejercicio de potestades de derecho público; el Parlamento Vasco; el Tribunal Vasco de Cuentas Públicas; el *Ararteko*; el Consejo de Relaciones Laborales; el Consejo Económico y Social; el Consejo Superior de Cooperativas; la Agencia Vasca de Protección de Datos; la Comisión Arbitral; las corporaciones de derecho público representativas de intereses económicos y profesionales de la Comunidad del País Vasco y cualesquiera otros organismos o instituciones, con o sin personalidad jurídica, creados por ley del Parlamento Vasco, salvo que ésta disponga lo contrario –arts. 2 y 17–. En estos mismos términos se mueven también los Anteproyectos de creación de Autoridades autonómicas de protección de datos⁵².

Como se puede comprobar, la línea divisoria entre el ámbito competencial de la Agencia Española de Protección de Datos y las Agencias Autonómicas que han establecido el legislador del Estado y los legisladores del País Vasco y de la Comunidad de Madrid es la distinción entre lo público y lo privado. Es decir, los ficheros públicos que existan dentro del territorio de una región son competencia de la Agencia Autónoma de Protección de Datos –con una única excepción, que son los ficheros de la propia Administración General del Estado que se mantengan en el territorio de una Comunidad

Autónoma y que son competencia de la Agencia Española de Protección de Datos–; en cambio, los ficheros privados son competencia de la Agencia Española de Protección de Datos. Como hemos señalado anteriormente, este modelo de distribución de competencias en materia de protección de datos personales entre la Agencia Española y las Agencias Autonómicas ha sido considerado constitucional por el Alto Tribunal en la Sentencia 290/2000, de 30 de noviembre, ya analizada pormenorizadamente, que resolvió un recurso de inconstitucionalidad presentado por el Gobierno de Cataluña. Ahora bien, conviene no confundirse. Como hemos indicado, que la distribución competencial establecida en la LORTAD –y después en la LOPD– fuera constitucional no quiere decir que sea la única constitucional. Caben en la Constitución otros modelos posibles de distribución competencial entre el Estado y las Comunidades Autónomas.

La legislación de la Comunidad de Madrid interpreta como ficheros públicos no sólo los ficheros de los que son titulares la Administración autonómica o las Entidades Locales del territorio de la Comunidad de Madrid –a los que se refiere expresamente el art. 41 LOPD–, sino también los ficheros de las Universidades públicas y los ficheros de las Corporaciones de Derecho Público –Colegios profesionales y Cámaras– siempre y cuando dichos ficheros sean creados o gestionados para el ejercicio de potestades de derecho público, en la medida en que estas entidades son Administraciones públicas vinculadas o dependientes de la Comunidad de Madrid, sometidas al derecho administrativo y que ejercen potestades de derecho público en desarrollo de competencias que están previstas en el Estatuto de Autonomía de la Comunidad de Madrid y han sido transferidas a la Comunidad de Madrid.

Por tanto, no basta el carácter público del fichero para que éste esté sometido al control de la Agencia Autónoma de Protección de Datos. Es necesario que el responsable del fichero público –el Ayuntamiento, la Universidad Pública, el Colegio

Profesional, la Cámara– se encuentre vinculado a la propia Administración Autónoma. El criterio delimitador es, en este caso, que el responsable cree el fichero para el desarrollo de una competencia atribuida a la Comunidad Autónoma. Tanto los Ayuntamientos como las Universidades Públicas o las Corporaciones de Derecho Público desarrollan competencias transferidas a las Comunidades Autónomas y que se encuentran recogidas en sus Estatutos de Autonomía. Es indispensable, por tanto, que la entidad de Derecho Público desarrolle competencias reconocidas a la Comunidad en su Estatuto de Autonomía y que hayan sido debidamente transferidas. Así, las Agencias Autónomas ejercen el control sobre los ficheros de las Universidades Públicas de su Comunidad, al ser estas entidades Administraciones Públicas que desarrollan competencias que han sido transferidas a las Comunidades Autónomas. Por ello, para que los ficheros de las universidades públicas sean competencia de la autoridad autonómica, es necesario que la universidad pública esté vinculada a una Comunidad Autónoma, es decir, que desarrolle competencias reconocidas para esa Comunidad en su Estatuto de Autonomía y que hayan sido debidamente transferidas a aquella⁵³. De hecho, las Universidades Públicas sólo podrían ser controladas por las Agencias Autónomas a partir de las transferencias de competencias, pero nunca antes. Así, se puede afirmar la existencia de una relación de tutela entre la Administración de la Comunidad Autónoma y las universidades públicas de su territorio⁵⁴. El problema se plantea principalmente en los Colegios Profesionales que extienden su ámbito territorial más allá de una Comunidad Autónoma y que están excluidos del control de una Agencia Autónoma⁵⁵.

En el caso de las Corporaciones de Derecho Público –Colegios Profesionales, Cámaras de Comercio, Industria y Navegación y Cámara Agraria–, hay que recordar que el derecho público califica a estas entidades como Administración Corporativa. Ahora bien, las Corporaciones de Derecho Público no sólo

desarrollan una actividad administrativa sino también una actividad privada sometida al Derecho privado, para la que crean ficheros de naturaleza privada⁵⁶. Las Agencias de Protección de Datos de las Comunidades Autónomas sólo podrán ejercer sus competencias de control sobre los ficheros públicos de estas Entidades, es decir, por aquellos ficheros creados o gestionados para el ejercicio de potestades de derecho público y de competencias administrativas. El control de los ficheros privados de estas Entidades le corresponde a la Agencia Española de Protección de Datos. Es decir, para que la Agencia de Protección de Datos de una Comunidad Autónoma tenga competencia no basta con que sea un fichero de una Corporación de Derecho Público; es necesario que sea un fichero creado o gestionado para el ejercicio de funciones públicas⁵⁷. Igualmente, esta separación competencial afecta a la inscripción de los ficheros. Los Colegios Profesionales que desarrollen su actuación exclusivamente en el ámbito territorial de una Comunidad Autónoma tendrán que inscribir sus ficheros públicos en el Registro de Ficheros de Datos Personales Autónomo y en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos. En cambio, los ficheros privados de los Colegios Profesionales se inscribirán únicamente en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos⁵⁸. En todo caso, la principal consecuencia de la consideración como público o como privado del fichero de un colegio profesional es el régimen jurídico –la exención del consentimiento para los ficheros públicos, el procedimiento de creación del fichero y el régimen de infracciones y sanciones–.

Por tanto, si la delimitación competencial entre la Agencia Española de Protección de Datos y las Agencias Autónomas está en la frontera entre lo público y lo privado, se puede afirmar, como hemos señalado anteriormente, que las Universidades Públicas son competencias de las Agencias Autónomas –dada la previsión de las leyes autonómicas de protección de datos– al ser

Entidades de Derecho Público con personalidad jurídica propia vinculadas o dependientes de una Administración territorial y que desarrollan competencias transferidas a una Comunidad Autónoma. En cambio, las Universidades Privadas son competencia inicialmente de la Agencia Española de Protección de Datos. Esto es así porque éstas son entidades privadas –no tienen el carácter de Administraciones Públicas–, sus ficheros no son públicos sino privados y todos los ficheros privados son competencia de la Autoridad Estatal de control. Así, sus ficheros no son creados a través de disposiciones de carácter general sino que son notificados a la Agencia Española. Esta es la distribución competencial que se refleja en la Ley 8/2001, de 13 de julio, de Protección de Datos Personales de la Comunidad de Madrid –art. 2.1– y art. 2.1 de la Ley Vasca 2/2004, de 25 de febrero⁵⁹.

Esta delimitación competencial entre público y privado se encuentra, como ya hemos señalado, no sólo en la legislación de la Comunidad de Madrid, sino también la legislación del País Vasco de Protección de Datos Personales. La Ley Vasca 2/2004, de 25 de febrero es aún más precisa en la atribución de competencias a la Agencia Vasca de Protección de Datos, al enumerar expresamente dentro de su ámbito de control no sólo a la Administración Autónoma, a la Local –en este caso, Administración General del País Vasco, órganos forales de los territorios históricos y las administraciones locales–, a las corporaciones de derecho público representativas de intereses económicos y profesionales, sino también a un conjunto de instituciones y órganos como el Parlamento Vasco, el Tribunal Vasco de Cuentas Públicas, el *Ararteko*, el Consejo de Relaciones Laborales, el Consejo Económico y Social, el Consejo Superior de Cooperativas, la Agencia Vasca de Protección de Datos y la Comisión Arbitral⁶⁰. La LPD de la Comunidad de Madrid se refiere más concisamente y sin enumerar a las “Instituciones de la Comunidad de Madrid” y a los “Organos, Organismos, Entidades de Derecho Público y demás

Entes Públicos integrantes de su Administración Pública”⁶¹.

Sin embargo, la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos, a diferencia de la legislación de la Comunidad de Madrid y de la legislación vasca, ha extendido más allá de los ámbitos señalados su esfera de control. Así esta Ley establece dentro de las competencias de la Agencia Catalana el control de los ficheros de las Universidades “del ámbito territorial de Cataluña” –art. 3.1–, sin distinguir entre Universidades Públicas y Privadas⁶². Así, si bien las Universidades Privadas no son Administración Pública, hay que tener en cuenta que la Administración de cada Comunidad Autónoma ejerce una función de control sobre las Universidades Privadas de su ámbito territorial, en virtud de las previsiones de los distintos Estatutos de Autonomía, de los decretos de transferencia y de la propia legislación autonómica. No hay que olvidar que las Universidades Privadas han sido reguladas por Ley⁶³.

La atribución del control de los ficheros de las Universidades Privadas a las Agencias Autonómicas plantea algunos problemas. Así, si bien estos ficheros son objeto de control por la Agencia Catalana, al tener el carácter de privados, tienen que ser creados a través de una notificación a la Agencia Española de Protección de Datos –art. 25 LOPD–. La Agencia Española ejerce un control material en el procedimiento de inscripción de los ficheros privados, no ocurriendo lo mismo con los ficheros públicos⁶⁴. Podría existir, por tanto, una doble instancia de control sobre los ficheros de las Universidades Privadas, y una divergencia de criterios que puede ocasionar conflictos en la práctica⁶⁵. Igualmente, existe un diferente régimen sancionador aplicable a las Universidades Públicas –al ser ficheros públicos– y a las Universidades Privadas –al ser ficheros privados–, de manera que la competencia de control de la Agencia Catalana sobre los ficheros de las Universidades Privadas obligaría a ésta a aplicar las sanciones económicas establecidas en la legislación por incumplimientos de la legislación por parte del

responsable de ficheros privados –art. 45 LOPD–, a menos que se entienda estas Universidades Privadas como Administraciones Públicas en sentido material y sus ficheros como ficheros públicos.

Existen también otros supuestos donde esta diferenciación entre lo público y lo privado no es a simple vista evidente⁶⁶. Además de los supuestos problemáticos de las Federaciones Deportivas –que podrían ser consideradas Corporaciones de Derecho Público– y de las Fundaciones Sanitarias, hay actividades que desarrollan los poderes públicos no sólo en régimen jurídico privado sino acudiendo a formas jurídicas privadas de personificación, como la sociedad mercantil. Así, existen casos de sociedades mercantiles donde la totalidad de las acciones pertenecen a los poderes públicos, casos de participación pública mayoritaria, y casos de participación pública minoritaria pero de control. La legislación de la Comunidad de Madrid y la legislación Vasca han acudido para diferenciar los sujetos públicos de los sujetos privados al criterio de la forma jurídica de personificación –art. 2 de ambas Leyes–. Así, sólo serán Administraciones públicas las Administraciones territoriales –autonómica y local–, la Administración Corporativa y la Administración institucional, incluyendo en ésta sólo a los Entes públicos –forma jurídica pública– y excluyendo de ésta a las sociedades mercantiles públicas –forma jurídica privada–⁶⁷. De esta forma, la LPD de la Comunidad de Madrid y la Ley Vasca han extendido sus competencias a las personas jurídicas públicas⁶⁸.

En cambio, la Ley 5/2002, de 19 de abril, ha dado en esta materia un paso más, extendiendo la competencia de esa Agencia –y, lógicamente, restándosela a la Agencia Española– a algunos ámbitos de frontera. Así, el art. 3.2 de esta Ley establece que “la Agencia Catalana de Protección de Datos también ejerce sus competencias con relación a los ficheros creados por las administraciones, los organismos y las entidades a que se refiere el apartado 1 cuando sean gestionados por entidades públicas o privadas en la prestación de servicios

públicos, sean o no concesionarias de éstos, o por asociaciones o fundaciones, o por las sociedades civiles o mercantiles en las cuales la Generalidad o los entes locales tengan la participación mayoritaria del capital, cuando llevan a cabo actividades por cuenta de una administración pública”. Esto significa que la Agencia Catalana extiende su ámbito de control también a entidades privadas que presten servicios públicos aunque no sean concesionarios de éstos, y a las sociedades civiles o mercantiles de participación pública mayoritaria, cuando éstas lleven a cabo una actividad por cuenta de una administración pública y gestionen ficheros creados por las Administraciones Públicas catalanas. Estas entidades, que podrían ser consideradas encargadas del tratamiento de ficheros públicos, serían controladas por la Agencia Catalana.

Como hemos señalado antes, la legislación de la Comunidad de Madrid y la legislación Vasca han considerado que estas entidades, aunque gestionaran ficheros creados por las Administraciones Públicas, serían controladas por la Agencia Española al no ser Administraciones Públicas. La atribución de los ficheros de entidades privadas que prestan servicios públicos a la Agencia Española no está tampoco exenta de problemas derivados de la necesidad de ceder información por parte de las Administraciones autonómicas a estas entidades privadas que les prestan el servicio. Pensemos, por ejemplo, en ficheros públicos centralizados de historias clínicas de pacientes dentro de un modelo de concierto con hospitales privados. La consideración de estos ficheros como privados plantea importantes límites al control de las Agencias de Protección de Datos Autonómicas, ya que muchos datos utilizados por estas empresas privadas que prestan servicios públicos provienen de ficheros públicos y han sido cedidos por las Administraciones autonómicas⁶⁹. Igualmente, el hecho de que muchas actividades administrativas están siendo externalizadas por la Administración autonómica, que también acude frecuentemente a encargados de tratamiento privados para ficheros que desarrollan

competencias administrativas, pueden dificultar la propia actividad de control de las Agencias de Protección de Datos Autonómicas sobre los ficheros públicos de su territorio. En todo caso, esta disparidad de criterios, frecuente en los modelos de Estado descentralizados, en el caso de extenderse, rompería la homogeneidad y la claridad del deslinde competencial entre la Agencia de Protección de Datos del Estado y las Agencias de Protección de Datos de las distintas Comunidades Autónomas y puede llegar a confundir a los ciudadanos y a los distintos operadores jurídicos.

Por último, la atribución a la Agencia Catalana del control de los ficheros públicos gestionados por entidades privadas, asociaciones, fundaciones o sociedades mercantiles con participación pública no necesariamente debe ser considerada inconstitucional por vulneración de la distribución competencial efectuada en el art. 41 LOPD⁷⁰. Recuérdese que este artículo atribuye a las Agencias Autonómicas el control no sólo de los ficheros gestionados por las Administraciones Públicas, sino también de los ficheros creados por las Administraciones Públicas, lo que permitiría el control por parte de las Agencias Autonómicas de entidades privadas siempre que gestionen ficheros creados por las Administraciones Públicas –en el caso de que esté previsto en la legislación autonómica, cosa que sólo ocurre hasta ahora en la Ley Catalana–. Esto legitima que la Agencia Catalana extienda su ámbito de control también a entidades privadas que presten servicios públicos aunque no sean concesionarios de éstos, y a las sociedades civiles o mercantiles de participación pública mayoritaria, cuando éstas lleven a cabo una actividad por cuenta de una administración pública y gestionen ficheros creados por las Administraciones Públicas catalanas.

4 ■ PRINCIPIOS DE COORDINACIÓN Y DE COOPERACIÓN EN LAS RELACIONES ENTRE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS Y LAS AGENCIAS AUTONÓMICAS

Es sabido que la relación entre el Estado y las CCAA no es de jerarquía sino de competencia. Esta es la misma relación que hay entre las Leyes del Estado y las Leyes de las Comunidades Autónomas. Por ello, las relaciones entre la Agencia Española de Protección de Datos y las Agencias de Protección de Datos de las Comunidades Autónomas se deben regir por el criterio de la competencia. No existe una relación de jerarquía ni de tutela entre la Agencia Española de Protección de Datos y las Agencias Autonómicas. No hay que olvidar que las Autoridades Autonómicas tienen la consideración de Administraciones independientes, independencia que se puede esgrimir no sólo frente a sus Gobiernos sino frente a otras autoridades de control.

Como hemos señalado anteriormente, corresponde al Estado la garantía de que el ciudadano tiene el mismo –igual– derecho fundamental de protección de los datos de carácter personal cualquiera que sea su lugar de residencia, es decir, la regulación de un sistema de protección de datos en todo el territorio nacional, evitando discriminaciones territoriales⁷¹. Le corresponde al Estado –en este caso a las Cortes Generales– la legislación básica de protección de datos y su desarrollo reglamentario principalmente a través de Reales Decretos del Consejo de Ministros. La Agencia Española de Protección de Datos, además del informe sobre esta normativa, tiene la competencia de interpretación, a través de Instrucciones y Recomendaciones del Director –art. 5 del Estatuto de la Agencia de Protección de Datos, aprobado por Real Decreto 428/1993, de 26 de marzo EAPD–, de forma que se garantice que todos los ciudadanos del Estado Español tienen el mismo contenido de derecho fundamental a la protección de datos, cualquiera que sea el territorio o la Comunidad Autónoma donde residan.

Así, es competencia de la Agencia Española de Protección de Datos la interpretación y desarrollo de algunas definiciones contenidas en la legislación como la de fuentes accesibles al público –art. 3 LOPD–, del ámbito de aplicación de la legislación –art. 2 LOPD–, de los principios de protección de Datos –arts. 4-12 LOPD, calidad, información, consentimiento, datos especialmente protegidos, deber de secreto, comunicación de los datos, acceso a los datos por cuenta de terceros–, y de los derechos de protección de datos –art. 13-19 impugnación de valoraciones, consulta al registro general, tutela de derecho, derecho a indemnización, acceso, rectificación, oposición y cancelación–. Así, el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan Datos de Carácter Personal, tiene aplicación para todo el territorio nacional, tanto en el ámbito de los ficheros públicos como en el ámbito de los ficheros privados⁷², sin perjuicio de que las CCAA puedan exigir más medidas de seguridad para los ficheros públicos en el ámbito de sus competencias⁷³. Igualmente, el desarrollo reglamentario de los derechos de acceso, rectificación o cancelación, realizado por el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, y la Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación tiene el carácter de regulación básica para todo el territorio nacional, sin perjuicio de que pueda existir regulación autonómica complementaria en el ámbito de sus competencias. En la actualidad, la Agencia Española se encuentra preparando un borrador de Reglamento de desarrollo de la LOPD.

Corresponde a las Comunidades Autónomas, a través de sus Consejos de Gobierno, el desarrollo normativo de algunas funciones que cumplen las Agencias Autonómicas de Protección de Datos: por ejemplo, el procedimiento de declaración de ficheros

y de inscripción en el Registro de Ficheros de la Comunidad Autónoma o el procedimiento de control y tutela de los ficheros públicos. Así, en lo relativo al procedimiento de declaración de ficheros, la Comunidad de Madrid ha aprobado el Decreto 99//2002, de 13 de junio, de regulación del procedimiento de elaboración de disposiciones de carácter general de creación, modificación y supresión de ficheros que contienen datos de carácter personal, así como su inscripción en el Registro de Ficheros de Datos Personales⁷⁴. Así, la Ley Catalana señala que “se ha de establecer por reglamento el procedimiento de inscripción en el Registro de Protección de Datos de Cataluña, su contenido, la modificación, la cancelación, las reclamaciones, los recursos y los demás aspectos pertinentes” –art. 15.3–. En la misma dirección, la Ley Vasca establece que “reglamentariamente se regulará el procedimiento de inscripción de los ficheros, a los que se refiere el artículo 2.1 de esta Ley, en el Registro de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes” –art. 18.4–. Igualmente, en relación con el control de ficheros y la tutela de derechos, el Consejo de Gobierno de la Comunidad de Madrid aprobó el Decreto 67/2003, de 22 de mayo, por el que se aprueba el Reglamento de Desarrollo de las Funciones de la Agencia de Protección de Datos de la Comunidad de Madrid de tutela de derechos y de control de ficheros de datos de carácter personal.

En general, si al Estado le corresponde la regulación general del derecho a la autodeterminación informativa y la garantía de la igualdad del derecho en todo el territorio nacional, las Comunidades Autónomas a través de sus Autoridades de Control, desarrollan una labor de prestacional y preventiva del derecho fundamental. Las Comunidades Autónomas deben velar por el pleno desenvolvimiento de los derechos dentro del ámbito de sus respectivas competencias y de las condiciones que establezcan las normas del Estado reguladoras de dichos

derechos fundamentales. El Estado social se ha caracterizado no sólo por la inclusión de nuevos derechos económicos y sociales sino por el reconocimiento de que todo derecho de la esfera personal y de libertad tiene también una vertiente prestacional, que es responsabilidad de los poderes públicos. Como ya hemos señalado en otra ocasión, la noción derecho fundamental implica que todo derecho, a partir de su reconocimiento constitucional, no sólo tiene una vertiente subjetiva –un substrato subjetivo que exige la abstención de los poderes públicos en unas esferas de libertad individuales–, sino también una vertiente objetiva, que implica la obligación de los poderes públicos de desarrollar una actividad prestacional en garantía de la efectividad del derecho. Todo derecho fundamental es, a la vez, un derecho de libertad y un derecho de prestación.⁷⁵ Así, las Agencias de Protección de Datos Autonómicas, a través de su actividad administrativa ordinaria, desarrollarían un aspecto prestacional del derecho fundamental a la autodeterminación informativa del art. 18.4 CE para el ámbito de los ficheros públicos⁷⁶. Esta actividad prestacional también sería desarrollada, aunque a nuestro parecer en menor medida, por la Agencia Española de Protección de Datos, a través del mantenimiento de determinados procedimientos. Realmente, la Agencia de Protección de Datos del Estado está centrada principalmente en la garantía de la vertiente subjetiva del derecho fundamental –su parte de derecho de libertad, que es más directamente accionable ante los poderes públicos y exigible ante los tribunales–.

Este criterio de la competencia que caracteriza las relaciones entre la Agencia de Protección de Datos del Estado y las Agencias de Protección de Datos de las Comunidades Autónomas se desarrolla a través de dos principios: un principio de coordinación, cuando una materia es competencia del Estado, y un principio de cooperación, cuando una materia es competencia de las Comunidades Autónomas.

Le corresponde al Estado, como hemos señalado antes, la garantía de que existe un sistema de

protección de datos en todo el territorio nacional, es decir, de que el ciudadano tiene el mismo derecho fundamental de protección de los datos de carácter personal cualquiera que sea su lugar de residencia. Esto es competencia del Estado, lo que le permite actuar bajo la cobertura de un principio de coordinación⁷⁷. El Estado debe desarrollar un conjunto de instrumentos de dirección y ordenación para que la protección de datos funcione como un auténtico sistema nacional. Por tanto, tienen que existir unos mecanismos que permitan un funcionamiento integrado de la protección de datos en cada país. La coordinación debe tratar de que todas las gestiones públicas de protección de datos –estatales y autonómicas–, que a primera vista parecen actividades parciales, se conecten dentro de la globalidad del modelo, evitando disfunciones y contradicciones. La Agencia Española de Protección de Datos debe ser eje vertebrador de este sistema de protección de datos, que lo que trata es de asegurar la igualdad de todos los españoles en el contenido del derecho fundamental. La Agencia Española de Protección de Datos cumple, sobre todo, una función de cohesión. La descentralización administrativa en éste o en otros ámbitos no puede hacerse en ninguna medida en perjuicio de los derechos de los ciudadanos. Es imprescindible evitar que se produzcan discriminaciones por razones territoriales, asegurando el acceso equitativo a unos contenidos materiales concretos del derecho fundamental de protección de datos. Lo contrario puede suponer afectar al principio de igualdad en la titularidad del derecho fundamental de protección de datos⁷⁸.

La coordinación implica que la Administración General del Estado pueda llegar a adoptar decisiones obligatorias por encima de la voluntad de las Comunidades Autónomas⁷⁹. El Tribunal Constitucional ha señalado expresamente que una de las diferencias entre la coordinación y la cooperación es que la primera admite la imposición de las decisiones –STC 214/1984–⁸⁰. Así, en el mismo artículo donde se recogen la existencia de Autoridades Autonómicas de Protección de Datos se establece que “el Director de

la Agencia de Protección de Datos podrá convocar regularmente a los órganos correspondientes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación” –art. 41.3 LOPD–. Las facultades de coordinación competencia exclusiva del Estado se desarrolla principalmente a través de normas jurídicas promovidas por la Agencia Española de Protección de Datos, lo que no implica una sumisión jerárquica ni una relación de tutela entre ésta y las Agencias Autonómicas. El Estatuto de la Agencia de Protección de Datos –EAPD–, aprobado por Real Decreto 428/1993, de 26 de marzo señala en su art. 2 que “la Agencia ejercerá sus funciones por medio del Director, a cuyo efecto los actos del Director se consideran actos de la Agencia”. El art. 12 –EAPD– establece que “el Director de la Agencia de Protección de Datos dirige la Agencia” –lo que es una obviedad– y es al que le corresponde “dictar las resoluciones e instrucciones que requiera el ejercicio de las funciones de la Agencia y, en especial, convocar regularmente a los órganos competentes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación –e)– y recabar de las distintas Administraciones Públicas la información necesaria para el cumplimiento de sus funciones, así como facilitar a aquéllos la información que le soliciten a idénticos efectos –f)–. En ejercicio de la función de coordinación, el Director de la Agencia de la Agencia Española de Protección de Datos puede recabar la opinión del Consejo de Protección de Datos, donde están representadas las Agencias Autonómicas y otras instituciones, pero con opinión no vinculante en una competencia que le corresponde al Estado. En todo caso, las facultades de coordinación que posee la Agencia Española de Protección de Datos están sometidas también al principio de legalidad, que se extiende tanto a la legislación estatal como a la autonómica. Las facultades de coordinación tienen que materializarse a través de normas jurídicas. La Agencia Española de Protección de Datos podrá, en esta dirección, promover la aprobación de Reales Decretos que desarrollen

reglamentariamente los principios y los derechos de la LOPD, pero que deberán respetar también la legislación autonómica en este ámbito, especialmente en lo relativo a la distribución competencial.

Las Comunidades Autónomas que creen Agencias no deben adoptar decisiones que vayan encaminadas indirectamente a dificultar las posibilidades de coordinación y de cohesión del modelo nacional de protección de datos. En todo caso, la Agencia Española de Protección de Datos siempre podrá impugnar estas decisiones, como garante de la equidad en el contenido del derecho. En este caso, la Agencia Española de Protección de Datos puede llegar a configurarse como una especie de Alta Inspección, que puede no limitarse sólo a una supervisión normativa, sino que puede actuar como coadyuvante en los distintos procesos judiciales ante denegaciones de tutela de derechos por parte de las Agencias de Protección de Datos Autonómicas, para no hacer recaer sobre en el ciudadano el coste económico del funcionamiento del sistema nacional de protección de datos.

La legislación española de protección de datos no ha desarrollado extensamente estas funciones de coordinación. Únicamente regula un supuesto excepcional: el ejercicio de competencias de coordinación coercitivas por parte de la Agencia Española de Protección de Datos sobre ficheros de Comunidades Autónomas en materia de su exclusiva competencia. Así, cuando el Director de la Agencia de Protección de Datos constate que el mantenimiento o uso de un determinado fichero de las Comunidades Autónomas contraviene algún precepto de esta Ley en materia de su exclusiva competencia podrá requerir a la Administración correspondiente que se adopten las medidas correctoras que determinen en el plazo que expresamente se fije en el requerimiento. Si la Administración pública correspondiente de la Comunidad Autónoma no cumpliera el requerimiento formulado, el Director de la Agencia de Protección de

Datos podrá impugnar la resolución adoptada por aquella Administración –art. 42 LOPD–. Parece que este precepto es de aplicación en el caso de que la Comunidad Autónoma no tenga Agencia de Protección de Datos, ya que las competencias relativas al control del cumplimiento de la legalidad de los ficheros públicos de los que son titulares las Comunidades Autónomas le corresponden a las Agencias de Protección de Datos Autonómicas. Es decir, este precepto está previsto para aclarar la relación entre la Agencia Española de Protección de Datos y las Comunidades Autónomas que no tengan creadas todavía Agencias de Protección de Datos. Así, a pesar del modelo autonómico, es posible la existencia de competencias de control de la Agencia Española sobre los ficheros públicos de esas Comunidades Autónomas. El hecho de que la Agencia de Protección de Datos esté configurada como una Autoridad independiente de la Administración General del Estado –aunque dentro del Poder Ejecutivo–, legitima más su función de control sobre los ficheros públicos de las Comunidades Autónomas, ya que éstas no deben ver en el ejercicio de esa función de control una intromisión del poder político del Gobierno del Estado.

Corresponde a las Comunidades Autónomas, como hemos señalado antes, el desarrollo y la gestión de la actividad de control sobre los ficheros públicos de su territorio. En este ámbito desarrollan una actividad autónoma, que abarca incluso un desarrollo normativo que afecte al procedimiento de declaración de ficheros –con inclusión de requisitos como un informe preceptivo de la Agencia autonómica para la aprobación de la disposición de carácter general–, al procedimiento de inscripción en el Registro de ficheros de la Agencia autonómica o a la función de control y tutela de derechos.

Las relaciones entre la Agencia Española de Protección de Datos y las Agencias de Protección de Datos de las Comunidades Autónomas sobre materias competencia de éstas últimas deben desarrollarse a través del principio de cooperación⁸¹.

Así, como hemos señalado antes, el Director de la Agencia Española de Protección de Datos podrá convocar regularmente a los órganos correspondientes de las Comunidades Autónomas a efectos de cooperación institucional. La Ley habilita tanto a la Agencia Española de Protección de Datos como a las Agencias de Protección de Datos de las Comunidades Autónomas a solicitarse mutuamente la información necesaria para el cumplimiento de sus funciones –art. 41.3 LOPD–. Esta facultad de pedir información debe interpretarse como una obligación de informar que recae sobre las distintas Agencias de Protección de Datos.

La cooperación entre la Agencia Española de Protección de Datos y las Agencias de Protección de Datos de las Comunidades Autónomas se materializa en la actualidad a través del Consejo Consultivo de Protección de Datos, donde están presentes representantes de las Agencias Autonómicas. El art. 38 LOPD señala que el Director de la Agencia estará asesorado por un Consejo Consultivo compuesto por un Diputado, un Senador, un representante de la Administración Central, un representante de la Administración Local, un miembro de la Real Academia de la Historia, un experto en la materia, un representante de los usuarios y consumidores y un *representante de cada Comunidad Autónoma que haya creado una agencia de protección de datos en su ámbito territorial, propuesto de acuerdo con el procedimiento que establezca la respectiva Comunidad Autónoma*, y un representante del sector de los ficheros privados. Como hemos señalado anteriormente, este Consejo Consultivo no ejerce funciones de coordinación, ni de toma de decisiones. Así, el Estatuto de la Agencia de Protección de Datos señala en su art. 18 que el Consejo Consultivo es “un órgano colegiado de asesoramiento del Director de la Agencia de Protección de Datos”, “emitirá informe en todas las cuestiones que le someta el Director de la Agencia de Protección de Datos y podrá formular propuestas en temas relacionados con las materias de competencia de esta”.

No obstante, es necesario plantearse la configuración de un órgano que facilite la comunicación, coordinación y cooperación entre la Agencia Española de Protección de Datos y las Agencias Autonómicas. Esto no era preciso en un escenario donde sólo existía una Agencia Autónoma ya que estas relaciones se desarrollaban de manera bilateral. La creación de más Agencias de Protección de Datos en otras Comunidades Autónomas hace necesaria un órgano que facilite estas relaciones entre la Autoridad Estatal y las Autoridades Autonómicas. La actual configuración del Consejo Consultivo, donde están presentes representantes que nada tienen que ver con la distribución territorial del poder y con el Estado autonómico, hacen que éste no sea un foro adecuado que permita el desarrollo de políticas de colaboración y cooperación en competencias transferidas a las Comunidades Autónomas. La configuración de este nuevo órgano no debe separarse en exceso del modelo de Conferencias Sectoriales previsto sobre otras materias que también corresponden a las Comunidades Autónomas⁸². La búsqueda del consenso debe ser prioritaria ya que las decisiones sólo son vinculantes para las Comunidades Autónomas que las acepten, al sustanciarse la cooperación sobre competencias atribuidas por el art. 41 LOPD a las Comunidades Autónomas. El principio que debe regir estas relaciones es el de colaboración leal entre las distintas Agencias de Protección de Datos.

5 ■ UN ÁMBITO CONFLICTIVO: LAS RELACIONES ENTRE EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS PERSONALES Y LOS REGISTROS AUTONÓMICOS

Uno de los principales aspectos conflictivos en las funciones y las competencias de la Agencia Española de Protección de Datos y las Agencias Autonómicas ha sido las relaciones entre el Registro General de Protección de Datos de la Agencia Española y los Registros de las Autoridades Autonómicas de

Control⁸³. Vamos a analizar seguidamente algunas de las posibles controversias entre las que se encuentran: la obligación de inscribir los ficheros públicos de las Comunidades Autónomas en el Registro General de Protección de Datos; la función de los Registros autonómicos y relación entre estos registros y el Registro General de Protección de Datos; y, por último, la publicidad como competencia del Registro General de Protección de Datos y las competencias plenas de control de las Agencias Autonómicas de Protección de Datos Personales.

5.1. ACERCA DE LA OBLIGACIÓN DE INSCRIBIR LOS FICHEROS PÚBLICOS COMPETENCIA DE LAS AGENCIAS AUTONÓMICAS EN EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS.

El derecho fundamental a la protección de datos personales, como ha señalado la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, atribuye a la persona el control sobre los datos relativos a la propia persona, facultándola para decidir quién posee esos datos y para qué los va a usar, pudiendo oponerse a esa posesión o uso y atribuyendo a su titular la capacidad de imponer a terceros la realización y la omisión de determinados comportamientos. Por ello, la legislación española de protección de datos desarrolla un conjunto de principios de protección de datos y reconoce unos derechos a los afectados. Entre estos derechos destaca el derecho de consulta al Registro General de Protección de Datos. Así, el art. 14 LOPD señala que "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". Este derecho, si bien no forma parte del contenido esencial del derecho fundamental a la protección de datos personales –a tenor de la Sentencia del Tribunal Constitucional antes citada–, es un derecho

instrumental esencial para el ejercicio de facultades que sí integran dicho contenido esencial, como son las de acceso, rectificación y cancelación de los datos personales. Difícilmente puede ejercitarse estos derechos si se desconocen los tratamientos de datos personales llevados a cabo por los poderes públicos y por los particulares en nuestro país.

La existencia de este derecho de consulta –y en el fondo, de los demás derechos de los titulares de los datos– ha animado al legislador al establecimiento de un *Registro General de Protección de Datos*. Así, el art. 39 LOPD señala que “el Registro General de Protección de Datos es un órgano integrado en la Agencia de Protección de Datos. Serán objeto de inscripción en el Registro General de Protección de Datos: a) Los ficheros de que sean titulares las Administraciones Públicas. b) Los ficheros de titularidad privada[...]. e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición”⁸⁴.

La existencia de este Registro General es, por tanto, una garantía del derecho de consulta y están obligados a inscribirse en él todos los ficheros públicos y privados que entren dentro del ámbito de aplicación de esta Ley –art. 2 LOPD–. Están excluidos 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 y los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada, sin perjuicio de que en estos últimos ficheros el responsable deberá comunicar a la Agencia Española de Protección de Datos la existencia del mismo, sus características generales y su finalidad –art. 2.2 LOPD–.

La Directiva 95/46/CE ha insistido en la importancia de la publicidad de los tratamientos de datos personales. Esta Directiva señala en el Considerando 48 de su Exposición de Motivos que “los

procedimientos de notificación a la autoridad de control tienen por objeto asegurar la publicidad de los fines de los tratamientos y de sus principales características a fin de controlarlos a la luz de las disposiciones nacionales adoptadas en aplicación de la presente Directiva”. El art. 21 de esta Directiva señala que “los Estados miembros adoptarán las medidas necesarias para garantizar la publicidad de los tratamientos” y que “los Estados miembros establecerán que la autoridad de control lleve un registro de los tratamientos notificados con arreglo al art. 18”. Se señala igualmente que “el registro podrá ser consultado por cualquier persona”. Por tanto, la existencia de un Registro General de Protección de Datos en nuestro país tiene por finalidad velar por la publicidad de los tratamientos de datos personales.

El art. 39.3 LOPD establece que “por vía reglamentaria, se regulará el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones y demás extremos pertinentes”. Este procedimiento ha sido desarrollado en los arts. 5 a 10 del Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal⁸⁵. Este Real Decreto establece la notificación a la Agencia Española de Protección de Datos de todo fichero de datos de carácter personal de titularidad pública “para su inscripción en el Registro General de Protección de Datos, mediante el traslado, a través del modelo normalizado que al efecto elabore la Agencia, de una copia de la disposición de creación del fichero” –art. 5 RD 1332/1994–. Además, los ficheros privados deberán inscribirse igualmente en el Registro General de Protección de Datos –art. 6 RD 1332/1994–.

En esta misma dirección, el art. 23 del Estatuto de la Agencia Española de Protección de Datos, aprobado por Real Decreto 428/1993, de 26 de marzo, señala

que “el Registro General de Protección de Datos es el órgano de la Agencia de Protección de Datos al que corresponde velar por la publicidad de la existencia de los ficheros automatizados de carácter personal, con miras a hacer posible el ejercicio de los derechos de información, acceso, rectificación y cancelación”. El art. 24 de dicho Estatuto indica que deben ser objeto de inscripción todos los tratamientos automatizados, que abarca tanto aquellos de los que son titulares las Administraciones públicas, como las empresas privadas y los particulares, e incluyendo dentro de los ficheros inscribibles dentro del Registro General de Protección de Datos los ficheros de las Administraciones de las Comunidades Autónomas y de sus entes y organismos dependientes, así como los ficheros de las Administraciones Locales.

Por tanto, todos los tratamientos de datos personales tanto públicos como privados que están dentro del ámbito de aplicación de la LOPD deben estar inscritos de manera obligatoria en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos. Es decir, los ficheros públicos sometidos a control de las Autoridades Autonómicas deben inscribirse en el Registro General de Protección de Datos.

5.2. FUNCIÓN DE LOS REGISTROS DE DATOS PERSONALES DE LAS COMUNIDADES AUTÓNOMAS Y RELACIÓN ENTRE ESTOS REGISTROS Y EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS

La Legislación estatal de Protección de Datos, como ya hemos señalado anteriormente, no obliga a la creación de Autoridades Autonómicas de control. Así, si bien la LORTAD preveía la existencia de Agencias de Protección de Datos de carácter autonómico, sólo fue puesta en funcionamiento en aplicación de esa Ley la Agencia de Protección de Datos de la Comunidad de Madrid, a través de la Ley 13/1995, de 21 de abril, de regulación del uso de la informática

en el tratamiento de datos personales por la Comunidad de Madrid, modificada parcialmente por la Ley 13/1997, de 16 de junio y por la Ley 6/1999, de 30 de marzo. Actualmente, como ya hemos señalado, está en vigor la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid. Posteriormente, se han aprobado, como hemos indicado, la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos y la Ley de la Comunidad Autónoma Vasca 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 Datos⁶⁶. La LOPD permite que las funciones de la Agencia Española de Protección de Datos puedan ser ejercidas por órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control, cuando afecten a ficheros de datos personales creados o gestionados por las Comunidades Autónomas o por la Administración Local de su ámbito territorial –art. 41.1–.

La LOPD no obliga a las Agencias Autonómicas a la creación de Registros de Ficheros de Datos Personales en las mismas. Así, el art. 41.2 LOPD señala que “las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros para el ejercicio de las competencias que se les reconoce sobre los mismos”. Sin embargo, en el caso de que la legislación autonómica establezca Registros de Ficheros en las autoridades de control autonómicas, estos Registros tienen la característica fundamental de haber sido creados por normas con rango de Ley. Este es el caso del Registro de Ficheros de Datos Personales de la APDCM. El art. 18 de la LPD de la Comunidad de Madrid señala: “La Agencia de Protección de Datos de la Comunidad de Madrid llevará un Registro de Ficheros de Datos de carácter personal”. La existencia de un Registro de Ficheros de Datos Personales en la Comunidad de Madrid no es una decisión de la propia Agencia Autonómica sino una exigencia establecida en la Ley 8/2001, de 13 de julio; el Legislador autonómico ha querido que “la Agencia cuente para el cumplimiento de sus

funciones” con un Registro de Ficheros de Datos Personales⁸⁷. Igualmente, la Exposición de Motivos de 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 afirma que “es de resaltar la creación del Registro de Protección de Datos, como órgano necesario de la agencia”. Así, el art. 18 de esta Ley establece que “se crea el Registro de Protección de Datos, como órgano integrado en la Agencia Vasca de Protección de Datos en los términos que se establezcan en los estatutos de ésta”. En la misma dirección, el art. 15 de la Ley 5/2002, de 19 de abril, de creación de la Agencia Catalana de Protección de Datos titulado “el Registro de Protección de Datos de Cataluña” señala que “el Registro de Protección de Datos de Cataluña es un órgano integrado en la Agencia Catalana de Protección de Datos⁸⁸. Por tanto, no parece adecuado calificar como “meros instrumentos internos” y “meros registros administrativos” a un Registro de Ficheros de Datos Personales establecido con rango de Ley⁸⁹.

La legislación de protección de datos de la Comunidad de Madrid establece específicamente las funciones de este Registro. Así, en el caso del Registro de Ficheros de Datos Personales de la Comunidad de Madrid, la finalidad del mismo es garantizar el derecho de consulta. Así, el art. 18.4 de la LPD de la Comunidad de Madrid afirma que “cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro de Ficheros de Datos Personales, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El registro será de consulta pública y gratuita”. Es, por tanto, un Registro de Ficheros de Datos Personales que trata de facilitar el ejercicio del derecho de consulta del art. 15 LOPD y del resto de los derechos de los afectados. La voluntad del Legislador regional de establecer un Registro con la finalidad de facilitar los derechos de los ciudadanos se afirma igualmente en el art. 18.2.b) de la LPD de la Comunidad de Madrid, que señala: “Serán objeto de inscripción en el Registro de

Ficheros de Datos de carácter personal. [...] b) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición”. La Ley Vasca establece igualmente en el art. 18.5 que “el Registro de Protección de Datos será de consulta pública y gratuita. Cualquier persona podrá conocer, recabando la información oportuna del citado Registro, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. Serán objeto de inscripción los datos relativos a los ficheros inscritos, “que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición” –art. 18.2.d)–⁹⁰. Por tanto, no se puede afirmar que estos registros autonómicos son algo “meramente instrumental” para el mejor desempeño de las competencias del art. 37 LOPD, ya que su función es garantizar en el ámbito competencial de la autoridad autonómica tanto el derecho de consulta como los derechos de acceso, rectificación y cancelación.

El art. 41.2 de la LOPD señala que los Registros Autonómicos sirven “para el ejercicio de las competencias que se les reconoce sobre los mismos”. Estas competencias son, lógicamente, las de control sobre los tratamientos de datos personales realizados por las Administraciones públicas –o por otras entidades privadas en el caso de la Ley Catalana–, que implica la verificación del cumplimiento de la legislación de protección de datos en los ficheros del ámbito competencial de cada una de las autoridades autonómicas de control. Por tanto, las funciones de los Registros Autonómicos son dos: facilitar el ejercicio del derecho de consulta y de los derechos de información, acceso, rectificación, cancelación y oposición; y servir para el ejercicio de las funciones de control y supervisión de las Agencia de Protección de Datos de las Comunidades Autónomas sobre los ficheros de su ámbito competencial.

Esta inscripción en los Registros de Ficheros

Autonómicos no es potestativa para los responsables públicos sometidos a control por la Agencia Autonómica sino una obligación establecida en la legislación autonómica correspondiente. Así el art. 18.2 de la LPD de la Comunidad de Madrid señala: "Serán objeto de inscripción en el Registro de Ficheros de Datos de Carácter personal: a) Los ficheros de datos de carácter personal de que sean titulares las Instituciones, Organos, Organismos y Empresas referidas en el art. 2 de la presente Ley"⁹¹. El art. 18.2 de la Ley Vasca señala que "serán objeto de inscripción en el Registro de Protección de Datos: Los ficheros a los que se refiere el art. 2.1 de esta Ley. Las autorizaciones a las que se refiere la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Los códigos tipo que afecten a los ficheros inscritos". El art. 15 de la Ley Catalana señala que "son objeto de inscripción en el Registro de Protección de Datos de Cataluña: a) Los ficheros de datos personales incluidos en el ámbito de aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que sean de titularidad de la Generalidad de Cataluña, de los entes que integran la Administración local en el ámbito territorial de Cataluña y de los demás organismos y entidades a que se refiere el artículo 3, así como los datos relativos a estos ficheros que sean necesarios para el ejercicio de los derechos de información, de acceso, de rectificación, de cancelación y de oposición. b) Los códigos tipo definidos por el artículo 32 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, formulados por la Generalidad de Cataluña o por los entes que integran la Administración local en el ámbito territorial de Cataluña"⁹².

La LPD de la Comunidad de Madrid señala en su art. 18.3 que "por vía reglamentaria se regulará el procedimiento de inscripción de los ficheros en el Registro de Ficheros de Datos Personales, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes". Este desarrollo reglamentario se ha

producido por el Real Decreto 99/2002, de 13 de junio, de regulación del procedimiento de elaboración de disposiciones de carácter general de creación, modificación y supresión de ficheros que contienen datos de carácter personal, así como su inscripción en el Registro de Ficheros de Datos Personales, que dedica al procedimiento de inscripción los arts. 13 al 17. Así este Decreto 99/2002 señala en el art. 13.1 que "a los efectos de iniciar el procedimiento de inscripción de ficheros, los responsables de los mismos, una vez haya sido publicada en el Boletín Oficial de la Comunidad de Madrid o en el diario oficial que corresponda, la disposición de carácter general por la que se crean, modifican o suprimen los ficheros, vendrán obligados a comunicarla al Registro de Ficheros de Datos Personales, disponiendo para ello de un plazo de quince días"⁹³.

Por tanto, los ficheros públicos mencionados en las leyes de protección de datos de las Comunidades Autónomas sí tienen una doble obligación de inscripción registral: la obligación de inscribir sus ficheros en el Registro General de Protección de Datos de la Agencia Española y la obligación de inscribir sus ficheros en el Registro de Ficheros de las Autoridades Autonómicas de control. Esta doble obligación se da en la Comunidad de Madrid, en Cataluña, en el País Vasco, que también han previsto Registros autonómicos de ficheros y, presumiblemente se dará también en el resto de Comunidades Autónomas que opten por crear autoridades autonómicas de control.

No tiene sentido contraponer el Registro General de Protección de Datos y los Registros autonómicos. Al contrario, en función del principio de cooperación administrativa lo adecuado es utilizar el Registro autonómico como un medio para facilitar la inscripción de los ficheros públicos en el Registro general. La Ley Catalana establece en el art. 15.2 que "el Registro de Protección de Datos de Cataluña ha de establecer los acuerdos de cooperación necesarios con el Registro General de Protección de Datos del Estado a efectos de integrar la información

registral y de mantenerla actualizada”⁹⁴. Este es el motivo por el que la APDCM ha notificado directamente a la Agencia Española los ficheros públicos creados, modificados o suprimidos del territorio de la Comunidad de Madrid, que han sido inscritos directamente a instancia de la APDCM y no del responsable del fichero. La APDCM ha velado así por la calidad y por la efectividad no sólo de su registro autonómico sino del Registro General. La APDCM ha notificado los cambios producidos en los ficheros públicos al Registro General una vez aprobada la disposición de carácter general y publicada ésta en el diario oficial. Como señalaremos más adelante, la solicitud de inscripción de un fichero público al Registro General es esencialmente una comunicación a este Registro de la aprobación y de la publicación de la disposición de carácter general para su inscripción de oficio en el Registro General.

Por tanto, los responsables de los ficheros públicos del territorio de las Comunidades Autónomas con Autoridades de control pueden directamente trasladar a la Agencia Española una copia de la aprobación y publicación de la disposición de carácter general que permita la inscripción, modificación o supresión de sus ficheros en el Registro General. En todo caso, hay que resaltar dos principios: uno, que las competencias de control sobre la adecuación de los tratamientos de datos personales de los ficheros públicos a los que se refiere la legislación autonómica le corresponde en exclusiva y únicamente a las autoridades autonómicas de control; dos, que los Registros de Ficheros Autonómicos sirven para el ejercicio de las competencias que se les reconoce sobre los mismos, entre ellas la función de control y supervisión sobre los ficheros públicos –art. 41.2 LOPD–⁹⁵.

Es imprescindible aplicar en el ámbito registral los principios de coordinación entre Administraciones Públicas y de simplificación administrativa, que están previstos en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Así, como señala su Exposición de Motivos –apdo. IV–, “la

múltiple y compleja realidad que supone la coexistencia de la Administración del Estado, las Administraciones de las Comunidades Autónomas y las de las Entidades Locales, proyectando su actividad sobre un mismo espacio subjetivo y geográfico, hace necesario propiciar un acercamiento eficaz de los servicios administrativos a los ciudadanos. [...]. La eficacia en el resultado de la actuación de esa realidad plural y compleja que son las Administraciones Públicas hace que la cooperación entre ellas resulte un principio activo, no sólo deseable, sino indispensable de funcionamiento. La cooperación es un deber general, la esencia del modelo de organización territorial del Estado autonómico, que se configura como un deber recíproco de apoyo y mutual lealtad [...]. Esta necesaria cooperación institucional entre Administraciones Públicas permitirá, en el marco de la modernización de las estructuras, la simplificación de todas ellas [...]”. Las Agencias Autonómicas que desarrollan competencias en el mismo espacio físico que la Agencia Española de Protección de Datos deben desarrollar en el ámbito de los registros de ficheros un conjunto de actuaciones tendentes a facilitar la inscripción de los ficheros públicos en el Registro General. De esta forma, se materializa el esfuerzo de toda la Administración Pública por la simplificación administrativa, que se ha desarrollado también en distintas experiencias de ventanilla única y de interconexión de registros administrativos. De esta forma, se simplifica la doble obligación de inscripción registral, evitando que una garantía para los ciudadanos suponga una duplicación de trámites para las Administraciones públicas⁹⁶.

5.3. LA PUBLICIDAD COMO COMPETENCIA DEL REGISTRO GENERAL DE PROTECCIÓN DE DATOS Y LAS COMPETENCIAS PLENAS DE CONTROL DE LA AGENCIA AUTÓNOMICAS DE PROTECCIÓN DE DATOS SOBRE LOS FICHEROS PÚBLICOS DE SU ÁMBITO TERRITORIAL

Es de reseñar aquí que la LOPD atribuye en su art. 41 a la Agencia Española de Protección de Datos y a su Registro General la competencia de “velar por la publicidad de la existencia de los ficheros de datos de carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine”. Por tanto, el legislador ha atribuido la función de publicidad de los ficheros principalmente a la Agencia Española de Protección de Datos cuya competencia deriva directamente del cumplimiento de la previsión contenida en el art. 21 de la Directiva 95/46/CE. El Registro General tiene la competencia de garantizar la publicidad de los ficheros en todo el territorio nacional. No se puede discutir la facultad de dar publicidad del Registro General de Protección de Datos, ya que su propio carácter general, que abarca los ficheros públicos y privados de todo el territorio nacional, es lo que justifica que sea éste el instrumento más adecuado para velar por la publicidad de los tratamientos. De esta forma, el derecho de consulta al Registro General –art. 14 LOPD– queda garantizado con la existencia de una única fuente que incorpora todos los tratamientos de datos personales que se producen en el territorio español.

Al mismo tiempo, la LOPD autoriza expresamente a las Comunidades Autónomas a crear registros autonómicos de ficheros para el desarrollo de sus competencias. Como hemos señalado, el art. 41.2 LOPD establece que “las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros para el ejercicio de las competencias que se les reconoce sobre los mismos”. La función de publicidad del Registro General de Protección de Datos no es incompatible con la función de los

registros autonómicos de coadyuvar al principio de publicidad en registros donde se puede ejercer presencialmente el derecho de consulta de manera más cercana al ciudadano. En todo caso, los Registros autonómicos de Ficheros tienen que contribuir a garantizar la calidad del Registro General y en ningún caso puede constituirse en un impedimento o en una dificultad para el principio de publicidad del Registro General⁹⁷.

La Agencia Española de Protección de Datos no puede transformar la obligación de inscripción de los ficheros públicos en el Registro General a los efectos de publicidad en un instrumento para controlar aquellos ficheros públicos que están fuera de su ámbito competencial. Tanto la LOPD como la legislación autonómica de protección de datos han atribuido las funciones de control de los ficheros públicos a las Agencias de la Comunidad de Madrid, Catalana y Vasca, a las que ha constituido como autoridades de control.

Hay que señalar que la LOPD diferencia claramente en cuanto al procedimiento de inscripción de ficheros entre los ficheros privados y los públicos. Así, los ficheros de titularidad privada que contengan datos de carácter personal pueden ser creados cuando resulte necesario para el logro de la actividad u objeto legítimo de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas –art. 25 LOPD–. No obstante, como señala el art. 26 LOPD, “toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará *previamente* a la Agencia de Protección de Datos”. Además, “deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación”. El Registro General de Protección de Datos solo inscribirá este fichero “si la notificación se ajusta a los requisitos exigibles. En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación”. La obligación de notificar previamente a la Agencia de

Protección de Datos la creación del fichero queda resaltada por la previsión de que “transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado”. En cambio, “la creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición de carácter general publicada en el Boletín Oficial del Estado o Diario Oficial correspondiente” –art. 20 LOPD–. No es necesaria la inscripción registral a los efectos de entender creado el fichero.

Esta misma distinción esencial entre ficheros públicos y ficheros privados se encuentra en el Real Decreto 1332/1994, de 20 de junio, antes citado, que ha llevado a cabo el desarrollo reglamentario del procedimiento de inscripción de ficheros. Así, el art. 7 de este Real Decreto señala que “los ficheros de titularidad pública serán inscritos de oficio por la Agencia de Protección de Datos, una vez haya recibido la copia de la disposición de creación de fichero”. Igualmente, el art. 8 del mismo Real Decreto señala que “la modificación o, en su caso, cancelación de la inscripción de los ficheros de titularidad pública se producirá *de oficio* por la Agencia de Protección de Datos, previo traslado por el órgano de la Administración responsable del fichero de una copia de la disposición general que modifique o suprima aquél”. Ni siquiera, en virtud de la normativa estatal que desarrolla reglamentariamente el procedimiento de inscripción de ficheros, es necesario en el caso de los ficheros públicos una solicitud de inscripción, sino *el envío o traslado de una copia de la disposición de creación del fichero*. En cambio, los ficheros privados se encuentran en una situación radicalmente distinta. Así, “la persona o entidad que pretenda crear un fichero de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos mediante escrito o soporte informático en modelo normalizado al efecto [...]” –art. 6–. “El Director de la Agencia de Protección de Datos, a propuesta del

Registro General de Protección de Datos, acordará la inscripción de ficheros de titularidad privada si la notificación contuviera la información preceptiva y se cumplen las restantes exigencias legales, requiriendo, en caso contrario, al responsable del fichero para que la complete o subsane en el plazo de diez días, con indicación de que, si así no lo hiciera, se le tendrá por desistido de su petición, archivándose sin más trámite” –art. 7–⁹⁸.

La diferencia esencial en el procedimiento de inscripción de ficheros entre los ficheros públicos y los ficheros privados proviene de que mientras los ficheros privados se crean después de la solicitud de inscripción a la Agencia Española de Protección de Datos –siendo, por tanto, este trámite esencial–, en cambio, los ficheros públicos se crean a partir de la aprobación de la disposición de carácter general y publicación en el diario oficial correspondiente. La inscripción de los ficheros públicos en el Registro General de Protección de Datos se hace de oficio después de la notificación y no tiene efectos constitutivos sino de publicidad de los tratamientos. La misión de velar por la publicidad de los tratamientos que la LOPD atribuye al Registro General de Protección de Datos no se puede confundir con una actividad de control, que no corresponde a la Agencia Española de Protección de Datos sobre los ficheros públicos de los que son competentes las autoridades autonómicas de control.

Esta posición es la única acorde con LOPD, que diferencia nítidamente los ficheros públicos y los ficheros privados, con la legislación de la Comunidad de Madrid, catalana y vasca, que atribuyen a las Agencias Autonómicas el control de los ficheros públicos de sus territorios y que establecen el Registro de Ficheros de Datos Personales de la APDCM, el Registro de Protección de Datos de Cataluña y el Registro de Protección de Datos integrado en la Agencia Vasca, y con el Real Decreto 1332/1994, de 20 de junio, que regula el procedimiento de inscripción de ficheros en el Registro General de Protección de Datos⁹⁹. En el caso

de la Comunidad de Madrid, la APDCM, dentro de sus competencias de supervisión y control sobre los ficheros públicos, sí valora, con carácter previo a la aprobación de la disposición de carácter general que crea el fichero, la adecuación de los tratamientos de datos personales a la normativa de protección de datos. Esto es lo previsto en el Decreto 99/2002, de 13 de junio y es consecuencia de que la Agencia Autonómica es la única Autoridad de control sobre los tratamientos de datos personales desarrollados dentro del ámbito de aplicación de la Ley 8/2001, de 13 de julio.

Debe recordarse, en todo caso, que la Sentencia del Tribunal Constitucional 290/2000, de 30 de noviembre, señala en su Fundamento Jurídico 15 que “es la garantía de los derechos fundamentales exigida por la Constitución así como la de la igualdad de todos los españoles en su disfrute la que en el presente caso justifica que la Agencia de Protección de Datos pueda ejercer las funciones y potestades a las que antes se ha hecho referencia respecto a los ficheros informatizados que contengan datos personales y sean de titularidad privada”. En este sentido, la Sentencia señala que “la exigencia constitucional de protección de los derechos fundamentales en todo el territorio nacional requiere que éstos, en correspondencia con la función que poseen en nuestro ordenamiento (art. 10.1 CE), tengan una proyección directa sobre el reparto competencial entre el Estado y las Comunidades Autónomas ex art. 149.1.1 CE [...]” ■

Notas

1 Cfr. más ampliamente A. TRONCOSO REIGADA, “La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional”, *Cuadernos de Derecho Público*, núms.. 19-20, 2003

2 Cfr. L. LÓPEZ GUERRA, “El reparto de competencias Estado-Autonomías en la Jurisprudencia del Tribunal Constitucional”, *Comunidades Autónomas y Comunidad Europea*, Valladolid, 1991; M. CARRILLO, “La noción de materia y el reparto competencial en la jurisprudencia del Tribunal Constitucional”, en *RVAP* núm. 36, II, 1993.

3 Es comprensible la falta de interés del estatuyente en la protección de datos personales ya que ésta no es una materia vinculada a la voluntad de proteger las “culturas y tradiciones, lenguas e instituciones” de los distintos pueblos de España que afirma el Preámbulo de nuestra Constitución. Tampoco está relacionada con “características históricas, culturales y económicas comunes” o con la existencia de una “entidad regional histórica” que reconoce el art. 143 CE.

4 Posiblemente, la LORTAD permitía también el control por parte de las Agencias Autonómicas de los ficheros de las Universidades Públicas y de los ficheros de los Colegios Profesionales creados para el ejercicio de potestades administrativas ya que, como después veremos, ambas Administraciones Públicas desarrollaban competencias que estaban transferidas a las Comunidades Autónomas. Sin embargo, la única legislación autonómica aprobada en el marco de la LORTAD –la de la Comunidad de Madrid– limitaba la competencia de la Agencia de Protección de Datos de la Comunidad de Madrid al control de los ficheros de la Administración Regional.

5 Así, la Ley 13/1995, de 21 de abril, amplió el contenido de la información del carácter facultativo o no de la cesión de datos a la Comunidad; estableció la exposición en las oficinas públicas de modo claro y visible de los aspectos sobre los que los ciudadanos deben ser informados; facilitó la defensa de los ciudadanos ante la imposibilidad de negarse a dar determinados datos, mediante la formulación de alegaciones acerca de la adecuación de los datos solicitados a los principios de pertinencia o racionalidad que permita la cancelación de oficio de los datos;

reconoció el derecho del ciudadano a solicitar la certificación de seguridad y la subsiguiente acción en demanda del bloqueo cautelar de los ficheros. Igualmente, la Ley 13/1995, de 21 de abril, estableció el rango normativo que deben tener las disposiciones de regulación de los ficheros –en ese momento, Decreto del Consejo de Gobierno–, reforzando la participación de los ciudadanos en su elaboración al recoger una fase de alegaciones relativas a la adecuación, pertinencia o proporcionalidad de los datos en función de la finalidad del fichero. En lo relativo a la seguridad de los datos, la Ley 13/1995, de 21 de abril, estableció un plazo específico para la adopción de las medidas precisas para garantizar la confidencialidad, integridad y disponibilidad de la información y extendió la responsabilidad no solo al responsable de fichero sino también a los administradores de sistemas de tratamiento automatizado y a los usuarios de los mismos. Esta Ley reguló también de manera más precisa y clara el procedimiento de ejercicio de los derechos de acceso, rectificación y cancelación; creó un registro de interesados y estableció una tasa disuasoria del ejercicio abusivo e injustificado del derecho de acceso. En lo relativo a la aplicación de la LORTAD, desde el punto de vista material, la Ley 13/1995, de 21 de abril incluyó todas las actividades de tratamiento automatizado de datos de carácter personal, incluidas las accesorias o preparatorias, extendiendo las garantías de la Ley a los trabajos de desarrollo de aplicaciones informáticas que vayan a contener ficheros de datos personales. Como se puede comprobar, la Ley 13/1995, de 21 de abril, supuso un desarrollo legislativo de la LORTAD sin entrar en contradicción con ella, salvaguardando las condiciones básicas de ejercicio del derecho fundamental a la protección de datos que corresponde al Estado a través de su legislación básica. La Ley 13/1995, de 21 de abril, optó por no reproducir normas o mandatos de la LORTAD “ni tan siquiera para precisar aquellas definiciones, procedimientos o, instituciones que han sido duramente criticados por la doctrina con posterioridad a la entrada en vigor de la Ley Orgánica y de su normativa de desarrollo, manteniéndose así la unicidad de los conceptos de los textos” –Exposición de Motivos de esta Ley, Apdo. II–, salvo en aquellos supuestos donde el valor didáctico de la reproducción supera el de la nitidez de la remisión al texto orgánico, lo que se aplica en la referencia al deber de secreto de los empleados públicos.

6 Preámbulo de la Ley 8/2001, de 13 de julio.

7 Realmente, la LOPD no contiene esa habilitación a la que hace referencia la Ley 8/2001, de 13 de julio. Esta última Ley se limita a la creación de la Agencia de Protección de Datos de la Comunidad de Madrid, salvo lo relativo al procedimiento de creación, modificación y supresión de ficheros, donde se hacen menciones a materias más propias de un reglamento –como a una memoria económica o a los informes preceptivos–.

8 STC 208/1999, de 15 de noviembre, F. 6.

9 En esta dirección, el Abogado del Estado en la STC 290/2000, de 30 de noviembre afirmó, a partir de la jurisprudencia constitucional, que a los efectos del art. 149.3 CE, la expresión “materias” no asumidas en los Estatutos de Autonomía debe ser entendida como el “conjunto de actividades, funciones e institutos jurídicos relativos a un sector de la vida social”, y que entraría en juego esta cláusula residual que beneficia al Estado cuando la identificación de la concreta “materia” a la que pertenezca determinada actividad “no pueda quedar resuelta con los criterios interpretativos ordinarios” que permitan subsumirla en alguna de las ya asumidas por las Comunidades Autónomas (STC 123/1984, F. 2). Para el Abogado del Estado, en este supuesto, la protección de los datos personales objeto de tratamiento automatizado ni constituye una actividad materialmente típica a los efectos del reparto competencial, ni resulta reducible hermenéuticamente a otras materias expresamente enunciadas en la Constitución o en los Estatutos de Autonomía, por lo que, al no haber sido asumida por los Estatutos de Autonomía, correspondería al Estado en virtud de la cláusula residual del art. 149.3 CE.

10 Estos argumentos pueden verse expuestos en la Exposición de Motivos de la LORTAD y en la argumentación del Abogado del Estado en la Sentencia del Tribunal Constitucional 290/2000, de 30 de noviembre.

11 Cfr. los Antecedentes de la STC 290/2000, de 30 de noviembre.

12 Así, aunque el Tribunal Constitucional ha admitido el carácter instrumental de una determinada actividad respecto a una materia objeto de un título competencial en virtud de la conexión existente entre aquella y ésta –por ejemplo, de la actividad cartográfica respecto a las competencias de ordenación del territorio y urbanismo–, en este caso no se entiende probada tal conexión. Así, sí

existe una conexión entre ficheros informáticos y materias competenciales pero no entre éstas últimas y la protección de datos personales.

13 F. J. 11º de la STC 290/2000, de 30 de noviembre.

14 Cfr. A. TRONCOSO REIGADA, "Introducción y Presentación" en la *Guía de Protección de Datos Personales para Colegios Profesionales*, Civitas, Madrid, 2004, págs. 11-14. Esta situación se produce, por ejemplo, en la actualidad con las competencias de la Agencia Catalana de Protección de Datos que, como después veremos, abarca los ficheros de las empresas privadas que presten servicios públicos, por lo que existe una dualidad de régimen jurídico y de autoridad de control en el caso de los ficheros que sirven para prestar el servicio público y el resto de los ficheros de la empresa.

15 Así, el criterio que mantiene la Agencia Española de Protección de Datos en relación a la interpretación de qué es Administración Pública a los efectos del art. 41 LOPD –nos referimos, por ejemplo, a la problemática de las Fundaciones Sanitarias, de las Federaciones Deportivas o del carácter público o privado de los ficheros de los Colegios Profesionales– o en relación al funcionamiento del Registro General –como veremos más adelante– tiende a ser restrictiva acerca de las competencias de las Agencias Autonómicas.

16 La labor preventiva de la Agencia Española de Protección de Datos se circunscribe básicamente a los planes sectoriales de inspección y a la resolución de algunas consultas de responsables de ficheros, que no tienen carácter vinculante.

17 Exposición de Motivos de la LORTAD.

18 Cfr. A. TRONCOSO REIGADA, "La contribución de las Agencias Autonómicas al derecho fundamental a la protección de datos personales", *XVII Encuentro sobre Informática y Derecho*, Universidad de Comillas 2002-2003, págs. 40-45; id., "Contribution of the Substate Data Protection Authorities to the effective protection of Data Protection Principles", *Challenges and Problems facing the newly-established Data Protection Supervisory Authorities*, Council of Europe, 2003. Más actualizada es la reflexión realizada con ocasión del *Primer Encuentro entre Agencias Autonómicas de Protección de Datos Personales*, Civitas, Madrid, 2005.

19 El Tribunal Constitucional pone como ejemplo la Sentencia 154/1988, de 21 de julio -F. 3-, relativa a las

funciones de la Oficina del Censo Electoral en relación con la regulación del censo electoral, al señalar que mediante esta regulación institucional el Estado había pretendido ejercer la competencia que en esta materia se deriva del art. 149.1.1 CE en relación con el art. 23 CE.

20 La existencia de regímenes sancionadores autonómicos en las materias en las que la Comunidad Autónoma haya asumido competencias no quiebra la igualdad básica –SSTC 87/1985; 37/1987; y 227/1988–.

21 Véase la modificación de los arts. 31, 39 y disposición final tercera LORTAD por los arts. 32 y 40 LOPD.

22 La diferenciación entre el juicio de oportunidad y el juicio de constitucionalidad –sin mezclar ambos planos– ha sido desarrollado por el autor de estas páginas en distintos trabajos. Cfr. *Privatización, Empresa Pública y Constitución*, Marcial Pons, Madrid, 1997, págs. 113-116; o "Método jurídico, interpretación constitucional y principio democrático" en *La justicia constitucional en el Estado democrático*, Tirant lo Blanch, Valencia, 2000, págs. 399-454.

23 Hay que tener en cuenta que en futuro se va a tratamientos globalizados. No tendría mucho sentido que la Agencia de la Comunidad de Madrid inspeccione a El Corte Inglés de Barcelona por el hecho de que esta empresa tenga el domicilio social en Madrid. La experiencia alemana, donde la Agencia Federal sólo controla los Ministerios y las Agencias de los Länder controlan los ficheros públicos y privados no parece que dé un resultado positivo.

24 Este problema se da en la actualidad cuando el responsable del fichero público acude a un encargado de tratamiento privado ya que sobre éste último no es posible una actividad inspectora directa de la Agencia Autonómica sino que tiene que desarrollarse por la Agencia Española en el marco de las relaciones de cooperación.

25 Una exposición inicial anterior a la creación de nuevas Agencias Autonómicas se puede ver en A. TRONCOSO REIGADA, "La contribución de las Agencias autonómicas al derecho fundamental a la protección de datos personales", cit. págs. 23-47; cfr también M. FERNÁNDEZ SALMERÓN, *La protección de los datos personales en las Administraciones Públicas*, Civitas-APDCM, Madrid, 2003, págs. 395-443; uno de los primeros estudios es el de E. DEL PESO NAVARRO y M. A. RAMOS, *Lortad. Análisis de la Ley*, Díaz de Santos,

1994, págs. 169-180.

26 Un análisis expositivo de las Agencias Autonómicas en A. I. HERRÁN ORTIZ, *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*, Dykinson 2002, págs. 341-347; E. DEL PESO, *Ley de Protección de Datos*, Diaz de Santos, 2000 págs. 97-104.

27 La actividad de la Agencia de Protección de Datos de la Comunidad de Madrid puede analizarse a partir de las distintas Memorias, siendo la primera Memoria 1997-1998 aprobada en la etapa de R. GARCÍA ONTOSO. Cfr. A. TRONCOSO REIGADA, "Presentación", en *Memoria de la Agencia de Protección de Datos de la Comunidad de Madrid 2001* págs. 7-10.

28 El primer Estatuto de la Agencia de Protección de Datos de la Comunidad de Madrid fue aprobado por el Decreto 22/1998, de 12 de febrero. El Estatuto actual ha sido aprobado por el Decreto 40/2004, de 18 de marzo.

29 La impugnación del modelo de distribución de competencias en este ámbito realizado por la LORTAD –resuelto por la STC 290/2000, de 30 de noviembre– es el argumento aducido para el retraso en la constitución de la Agencia Catalana de Protección de Datos.

30 El Estatuto de la Agencia Catalana de Protección de Datos se aprobó por el Decreto 48/2003, de 20 de febrero. Cfr. más ampliamente X. HERNÁNDEZ I MORENO, "Presentació", *Legislació sobre protecció de dades*, Generalitat de Catalunya, 2003, pág. 12. Algunos de los textos normativos citados se encuentran en el *Repertorio de Legislación y Jurisprudencia sobre Protección de Datos*, Civitas-Thomson, Madrid, 2004.

31 Para un análisis de la Ley vasca y de sus antecedentes, cfr. J. M. ENDEMAÑO AROSTEGUI, "La Agencia Vasca de Protección de Datos: competencias y perspectivas", *Ponencia presentada en el Colegio de Abogados de Barcelona*, noviembre, 2003, *pro manuscrito*. Una crítica a este anteproyecto de ley se puede ver en *Informe del Consejo Económico y Social del País Vasco*.

32 Este es el motivo por el que la Agencia de Protección de Datos de la Comunidad de Madrid organizó el *Encuentro entre Agencias Autonómicas de Protección de Datos*. En este texto se recogen las ponencias referidas a la creación de nuevas Agencias Autonómicas.

33 Se prevé la aprobación de la Ley de creación de la

Agencia Valenciana para el año 2005. Sobre el Anteproyecto de Ley Valenciano, cfr. J. M. GARCÍA I BÀRRIO, "Agència Valenciana de Protecció de dades", Teulada, mayo, 2004. *I Encuentro entre Agencias Autonómicas de Protección de Datos* Cfr. J. BENEDITO AGRAMUNT, "Anteproyecto de Ley de creación de la Agencia Valenciana de Protección de Datos", en el *I Encuentro entre Agencias Autonómicas de Protección de Datos*, Civitas, Madrid, 2005. Con anterioridad, el Gobierno Valenciano, a través del Decreto 96/1998, de 6 de julio, por el que se regula la organización de la función informática, la utilización de los sistemas de información y el Registro de Ficheros informatizados de la Administración de la Generalitat, había puesto en marcha la UARFI –*unitat administrativa de registre de fitxers informatitzats*– con la finalidad de facilitar la declaración de los ficheros de la Administración autonómica. Igualmente, la Generalitat Valenciana ha aprobado una normativa específica en materia de seguridad: la Orden, de 3 de diciembre de 1999, de la Conselleria de Justicia y Administraciones Públicas, por la que se aprueba el Reglamento Técnico de Medidas de Seguridad para la aprobación y homologación de Aplicaciones y Medios de Tratamiento Automatizado de la Información, y el Decreto 37/2004, de 5 de marzo, del Gobierno Valenciano, por el que se crea la Comisión Interdepartamental para la coordinación de la política de seguridad de los sistemas de información de la Generalitat Valenciana –COIPSE–.

34 A la elaboración de este anteproyecto está contribuyendo la profesora M. Serrano, de la Universidad de Castilla la Mancha. Cfr. R. ARIZA FERNÁNDEZ, "Anteproyecto de Ley de Creación de la Agencia de Castilla la Mancha de Protección de Datos", en *I Encuentro*, cit. En la actualidad, Castilla la Mancha dispone de alguna normativa reglamentaria. Cfr. el Decreto 53/2002, de 23 de abril, sobre normas reguladoras de la protección de datos de carácter personal y la Orden de 3 de mayo 2002 de la Consejería de Ciencia y Tecnología de modelos de solicitud para ejercer los derechos de acceso, oposición, rectificación y cancelación de datos de carácter personal.

35 Cfr. A. RODRÍGUEZ CARVALLO, "La Autoridade Galega de Protección de Datos", en *I Encuentro*, cit. En relación con esta última, y gracias a la amabilidad del Director General de Organización y Sistemas Informáticos de la Xunta de Galicia, he podido participar en algunos aspectos como la denominación –he defendido la expresión *Autoridade Galega*–, las competencias y la posibilidad de firmar Convenios con la

Agencia Española en el ámbito de los ficheros privados –esto último estuvo en los primeros borradores pero se suprimió en el Proyecto de Ley–.

36 La proposición de Ley 6- 03/PPL- 000008, de creación de la Agencia Andaluza de Protección de Datos, fue presentada por la Asociación Andaluza de Comercio Electrónico (ANDCE) y fue admitida a trámite por el Parlamento de Andalucía el 14 de octubre de 2003. Cfr. *Repertorio de Legislación y Jurisprudencia sobre Protección de Datos*, cit. págs. 357-368. Otras Comunidades Autónomas han comenzado al menos a regular sus ficheros. Cfr. en Navarra, el Decreto Foral 143/1994, de 26 julio, sobre ficheros informatizados con datos de carácter personal dependientes de los órganos de la Administración de la Comunidad Foral y de sus Organismos Autónomos; en las Islas Baleares, el Decreto 92/1994, de 27 julio, de ficheros automatizados con datos de carácter personal gestionados por el Servicio de Informática; en Cantabria, el Decreto 48/1994, de 18 octubre, de ficheros informatizados con datos de carácter personal y de sus organismos autónomos; en Castilla y León, el Decreto 40/1999, de 8 marzo, de la Junta de Castilla y León, sobre ficheros automatizados con datos de carácter personal; por último, en Aragón, el Decreto 98/2003, de 29 de abril, que Regula los ficheros de datos de carácter personal gestionados por la Administración de la Comunidad Autónoma de Aragón.

37 Cfr. M. HEREDERO HIGUERAS, *La Directiva Comunitaria de Protección de los Datos de Carácter Personal*, Aranzadi, Pamplona, 1997, págs. 201-218

38 Semejantes referencias se encuentran en los Anteproyectos de creación de Autoridades de Control en Valencia, Castilla la Mancha y Galicia.

39 Desde esta posición, y con todo el respeto que merece el Gobierno de Cataluña, y sin perjuicio de la lealtad institucional entre las Administraciones Públicas y entre las Autoridades de Control, no podemos compartir y debemos criticar –en términos académicos– el cese del Director de la Agencia Catalana de Protección de Datos Sr. D. Xavier Hernández i Moreno, por Acuerdo del Gobierno de la Generalitat, de 31 de mayo de 2005, que alegaba incumplimiento de sus funciones. Con anterioridad, el 30 de marzo de 2005, el Consejo Asesor de Protección de Datos de Cataluña acordó demandar al Gobierno la instrucción del correspondiente expediente al Director de la Agencia Catalana por el mismo motivo,

expediente para el que fue nombrado un instructor.

La Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos establece en su art. 13.3 que el director cesa únicamente por expiración del mandato, a petición propia o por separación acordada por el Gobierno, previa instrucción del correspondiente expediente, a propuesta de las tres cuartas partes de los miembros del Consejo Asesor, por incumplimiento de sus obligaciones, incompatibilidad sobrevenida para el ejercicio de sus funciones o condena por delito doloso. Consideramos que la inclusión de un correo electrónico dirigido a un trabajador de la Agencia que se grapó y se fotocopió dentro de la documentación de la Jornada sobre “Protección de Datos de Carácter Personal. Balance y retos de futuro”, celebrada el día 15 de marzo de 2005 –hecho desgraciado inmediatamente subsanado– debe ser considerado un error grave e involuntario del personal administrativo de la Agencia Catalana, no imputable al Director. Este hecho no puede ser interpretado para afirmar una falta de objetividad e independencia del Director de la Agencia, que conoció los hechos con posterioridad a haberse producido. No es un supuesto jurídico de incumplimiento de sus obligaciones ya que no se trata de un hecho reiterado sino de un suceso aislado, por lo que no existe una responsabilidad *in vigilando* del Director. Por tanto, el supuesto de hecho objeto de análisis no puede ser subsumido en absoluto en ninguno de los supuestos de cese previstos en la Ley 5/2002, de 19 de abril.

El cese del Director de la Agencia Catalana supondría una vulneración del derecho fundamental a ejercer un cargo público con los requisitos establecidos en las leyes –art. 23.2 CE–. Como señala la Sentencia del Tribunal Constitucional 24/1984, “el derecho a acceder a los cargos públicos comprende también el de permanecer en los mismos en condiciones de igualdad “con los requisitos que señalan las leyes” –cfr. también las SSTC 5/1983 y 60/1982–. Igualmente puede suponer una lesión del derecho fundamental a la protección de datos personales –art. 18.4 CE– ya que la independencia de las Agencias de Protección de Datos es una exigencia de este derecho fundamental. Siendo la principal garantía de independencia de la Agencia la inamovilidad del director durante el periodo de mandato, salvo supuestos tasados, el cese del Director de la Agencia Catalana fuera de estos supuestos tasados previstos en la Ley significa una arrogación por parte del Gobierno de Cataluña de un poder de remoción que no le corresponde, tratando a la Agencia Catalana como una

Administración dependiente del Poder Ejecutivo y sometiéndola a una relación de tutela. La quiebra de la independencia de la Agencia Catalana de Protección de Datos representa una vulneración del derecho fundamental de todos los ciudadanos de Cataluña a la protección de datos personales, que lleva dentro de su contenido esencial la tutela de este derecho por autoridades independientes. Existe, en este sentido, una preocupación de las Autoridades de Protección de Datos de que el cese pueda afectar la credibilidad futura de la Agencia Catalana de Protección de Datos como autoridad administrativa independiente y dañar gravemente una institución de defensa de los derechos fundamentales que todavía se encuentra en fase de implantación.

Al tratarse de la lesión de derechos fundamentales, existe la posibilidad de obtener una tutela a través de las garantías jurisdiccionales e instar el procedimiento preferente y sumario previsto en el art. 53.2 CE, denominado amparo judicial o amparo ordinario, y ulteriormente el recurso de amparo ante el Tribunal Constitucional. En este caso, al provenir la vulneración del derecho fundamental a la protección de datos personales de una Administración Pública, el procedimiento preferente y sumario –el amparo contencioso– se encontraría entre los previstos en la Ley de la Jurisdicción Contencioso-Administrativa.

40 Cfr. los Anteproyectos de creación de Autoridades de Control en Valencia, Castilla la Mancha y Galicia

41 Cfr. Anteproyectos mencionados en la nota anterior.

42 Permítaseme remitirme a los planteamientos expuestos más ampliamente en A. TRONCOSO REIGADA, *Administraciones Independientes y Constitución*, Universidad de Cádiz, 1997 –segundo ejercicio de titularidad de Universidad–. Cfr. también A. BETANCOR, *Las Administraciones Independientes*, Tecnos, Madrid, 1994.

43 Cfr. también el art. 28 de la Directiva 95/46/CE.

44 Cfr. art. 45 de la LOPD.

45 Cfr. arts. 28 y 29 de la Directiva 95/46/CE y arts. 9 y 12.2 d) del Real Decreto 428/1993, de 26 de marzo.

46 Cfr. J. APARICIO, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, cit. págs. 213-222.

47 Esta cuestión ha sido abordada más ampliamente por P. PÉREZ TREMP, *Comunidades Autónomas, Estado y Comunidad Europea*, Ministerio de Justicia, Madrid, 1987

48 Así, la Agencia de Protección de Datos de la Comunidad de Madrid, la Agencia Catalana de Protección de Datos y la Agencia Vasca de Protección de Datos han sido acreditadas y forman parte de la Conferencia Internacional de Autoridades y Comisionados de Protección de Datos, pero no participan en el Grupo del art. 29 de la Unión Europea, en el que sí toman parte, sin embargo, otras Agencias subnacionales de Protección de Datos como las de los länder alemanes. Esta problemática que, obviamente, no es original del ámbito de la protección de datos, va a ser replanteada en nuestro país.

49 Cfr. *infra* apdo. 5.b). Cfr. art. 15.k) de la LPD de la Comunidad de Madrid y art. 6 de la Ley 5/2002, de 19 de abril, de la Generalitat de Cataluña

50 En éste último supuesto no hay que olvidar el régimen específico de las infracciones de las Administraciones públicas previsto en el art. 46 LOPD.

51 Cfr. art. 15 de la LPD de la Comunidad de Madrid, art. 17 de la Ley 2/2004, de 25 de febrero, del País Vasco; art. 5 de la Ley 5/2002, de 19 de abril, de la Generalitat de Cataluña

52 El Anteproyecto de creación de la Agencia Valenciana extiende su control a los ficheros de datos de carácter personal directamente vinculados con el ejercicio de potestades de derecho público o de funciones públicas que hayan sido creados por la Administración Pública Valenciana, en la que se encuentran la Administración Autonómica –Instituciones de la Generalitat, Administración Pública de la Generalitat y Administración Institucional o Entes instrumentales públicos dependientes de la Generalitat Valenciana–, la Administración Local –también la Administración institucional o entes instrumentales dependientes de las entidades locales valencianas siempre que actúen sujetos al Derecho Público–, la Administración independiente –en la que incluyen a las Universidades Públicas de la Comunidad Valenciana–, la Administración Corporativa y la Administración Consorcial –cualesquiera entes dotados de personalidad jurídica propia que actúen sometidos al Derecho Público, en los que participen distintas Administraciones Públicas de la Comunidad Valenciana–. No se incluyen las sociedades

civiles o mercantiles públicas –en las que haya participación mayoritaria de las Administraciones Públicas de la Comunidad Valenciana–, ni las Fundaciones Públicas, ni las Asociaciones Públicas –reguladas en el art. 2.6 de la Ley Orgánica 1/2002, de 22 de marzo, reguladora del derecho de asociación–, ni las entidades concesionarias de servicios públicos. Tampoco entran dentro de su ámbito de aplicación las entidades públicas radicadas en la Comunidad Valenciana con domicilio social fuera de ésta. Cfr. los Anteproyectos de Galicia y de Castilla la Mancha.

53. El apartado B del Acuerdo de traspaso de funciones y servicios de la Administración del Estado a la Comunidad de Madrid en materia de Universidades, aprobado por Real Decreto 942/1995, de 9 de junio, prevé en su número primero que “se traspasan a la Comunidad de Madrid las Universidades Complutense, Politécnica, Autónoma, Alcalá de Henares y Carlos III”, habiendo sido creada por la Ley 7/1996, de 8 de julio, de la Asamblea de Madrid, la Universidad Rey Juan Carlos. Esta transferencia se efectúa en desarrollo de lo establecido en el artículo 29.1 del Estatuto de Autonomía de la Comunidad de Madrid, según el cual “[c]orresponde a dicha Comunidad Autónoma la competencia de desarrollo legislativo y ejecución de la enseñanza en toda su extensión, niveles y grados, modalidades y especialidades, de acuerdo con lo dispuesto en el artículo 27 de la Constitución y leyes orgánicas que conforme al apartado 1 del artículo 81 de la misma lo desarrollen, y sin perjuicio de las facultades que atribuye al Estado el número 30 del apartado 1 del artículo 149 y de la Alta Inspección para su cumplimiento y garantía”

54 La Ley Orgánica 11/1983, de 25 de agosto, de Reforma Universitaria estableció en su momento los supuestos en los que la actuación de las Universidades quedaría sujeta al control de las Comunidades Autónomas. Así, el art. 3.3 atribuía a cada Comunidad Autónoma la tarea de coordinación de las Universidades de su competencia. De esta forma, la Universidades públicas y privadas se creaban modificaban o suprimían por normas de las propias Comunidades Autónomas. Este criterio ha sido mantenido por la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades que atribuye a las Comunidades Autónomas la coordinación de las Universidades de su competencia, sin perjuicio de las funciones del Consejo de Coordinación Universitaria –art. 2.5 LOU–. Así, la LOU ha incrementado las facultades autonómicas de coordinación y gestión, al

añadir a las competencias originarias otras facultades como la regulación del régimen jurídico y retributivo del profesorado contratado, la capacidad para establecer retribuciones adicionales para el profesorado, la aprobación de programas de financiación plurianual conducentes a contratos programa y la evaluación de la calidad de las Universidades en el ámbito de su responsabilidad. Cfr. más ampliamente A. TRONCOSO REIGADA, “Introducción” en *Guía de Protección de Datos para Universidades Públicas*, Civitas-APDCM, 1994, págs. 9-33.

55 En relación con este aspecto, el Acuerdo de Traspaso a la Comunidad de Madrid de funciones y servicios de la Administración del Estado en materia de Colegios Oficiales o Profesionales, aprobado por Real Decreto 2368/1994, de 9 de diciembre, señala, en su apartado B) que “se traspasan a la Comunidad de Madrid las funciones y servicios que realiza la Administración del Estado en relación con los Colegios Oficiales o Profesionales, cuyo ámbito territorial esté exclusivamente comprendido dentro del territorio propio de la Comunidad. Todo ello sin perjuicio de que los citados Colegios mantengan su vinculación con los respectivos Consejos Generales, como órganos de relación de los Colegios Oficiales o Profesionales en el ámbito estatal o internacional”. Cfr. más ampliamente G. FERNÁNDEZ FARRERES, “La distribución de competencias sobre Colegios Profesionales entre el Estado y las Comunidades Autónomas” en L. MARTÍN-RETORTILLO (coord.), *Los Colegios Profesionales a la luz de la Constitución*, cit.; J. M. BAÑO LEÓN, “Las competencias del Estado y de las Comunidades Autónomas sobre Colegios Profesionales”, *Derecho Privado y Constitución*, núm. 5, 1997, págs. 39-68.

56 Cfr. más ampliamente L. CALVO SÁNCHEZ, *Régimen Jurídico de los Colegios Profesionales*, Civitas, Madrid, 1998.

57 Así, como ejemplos de ficheros públicos tenemos el fichero de colegiados, el fichero de expedientes deontológicos, el fichero de peritos o el de justicia gratuita. Como ejemplos de ficheros privados tendríamos el fichero de nóminas del personal del Colegio, el fichero de la mutualidad –que es voluntaria–, los ficheros de alumnos de los cursos que imparte el Colegio o el fichero de asociados –prelicenciados–. A esta cuestión nos hemos referido más ampliamente en A. TRONCOSO REIGADA, “Introducción y Presentación”, *Guía de Protección de Datos Personales para Colegios*

Profesionales, Civitas-APDCM, Madrid, 2004, págs. 11-18. Como hemos comentado en la citada Guía, en la actualidad, la mayoría de los ficheros de los Colegios Profesionales para el desarrollo de funciones administrativas están declarados en el Registro General de Protección de Datos como ficheros privados. Esta situación representa una inadecuación de los Colegios Profesionales a la legislación de protección de datos, que exige que los ficheros públicos sean creados por una disposición de carácter general y publicados en un diario oficial. A los efectos de creación del fichero, es incorrecto que un fichero materialmente público esté registrado como privado y no haya sido aprobado por una disposición de carácter general y publicado en un diario oficial. La declaración de un fichero público a través de una disposición de carácter general no es un simple trámite burocrático; es la garantía de que el órgano más importante de una Administración, y, en el caso de los Colegios Profesionales la Junta de Gobierno, asume que los datos personales que están en un fichero no son de la Administración sino de los ciudadanos y que para utilizarlos tiene que aprobar una norma jurídica y publicarla en un diario oficial. No obstante, es también incorrecto que un fichero privado pretenda ser declarado como público y beneficiarse de ese modo de las excepciones a la regulación general de la que disfrutaban los ficheros públicos.

58 Es especialmente importante que la determinación de la naturaleza pública o privada de los tratamientos de datos personales sea homogénea en todo el territorio español. No tendría sentido que la naturaleza pública o privada de un fichero de un Colegio Profesional dependiera del ámbito territorial, de forma que un fichero esté inscrito como público en el Registro autonómico y como privado en el Registro General. Es necesario en este aspecto ajustarse a los criterios que se establezcan en el futuro de común acuerdo entre la Agencia Española de Protección de Datos, las Autoridades Autonómicas y la Unión Interprofesional en relación con los ficheros de los Colegios Profesionales. Es especialmente importante el punto de vista de la Unión Interprofesional, que agrupa a los Colegios Profesionales, ya que el carácter público o privado de los ficheros de los Colegios es consecuencia del carácter público o privado de la actividad de los Colegios Profesionales –del hecho de que existan actos sometidos al derecho administrativo y al derecho privado, controlados por la jurisdicción contencioso-administrativa y por la jurisdicción civil- por lo que la opinión de los Colegios –familiarizados con el carácter

mixto o bifronte que se da en todos los ámbitos de su actividad y no sólo en protección de datos- hace que su criterio sea muy definitorio.

59 A esta cuestión nos hemos referido en la “Introducción y Presentación” a la *Guía de Protección de Datos Personales para Universidades*, cit.

60 Se omite una referencia expresa a las Universidades Públicas, pero que debe incluirse por las razones ya expuestas en la Administración Autonómica. Sería interesante una reflexión –que la dejaremos para un trabajo posterior– sobre el control por parte de la Agencia Vasca sobre sus propios ficheros y el principio de *iudex super partes*, así como sobre el control de las autoridades autonómicas sobre los ficheros del Parlamento. Así, en este último caso, hay que tener en cuenta que se produce el supuesto insólito de que el control no sería del poder legislativo al poder ejecutivo, sino de este último sobre el primero, aunque estemos hablando, en todo caso, de un control jurídico –y no político– practicado por una Administración independiente –y no dependiente del Gobierno Regional-

61 Cfr. los Anteproyectos de Valencia, Galicia y Castilla la Mancha.

62 Una de las principales razones para esta delimitación competencial es atribuir a la Agencia Catalana de Protección de Datos el control sobre la Universidad Abierta de Cataluña, una Fundación privada de iniciativa pública. Otras Universidades Privadas de Cataluña que controlarían la Agencia Catalana son la Universidad de Vic, la Universidad Ramón LLull, la Universidad Abad Oliva y la Universidad Internacional de Cataluña.

63 Para el ámbito de la Comunidad de Madrid, hay que señalar las leyes 23 y 24/1995, de 17 de julio, de reconocimiento de la Universidad Antonio de Lebrija y la Universidad Europea de Madrid, la Ley 18/1998, de 20 de noviembre, de reconocimiento de la Universidad Camilo José Cela y la Ley 7/2001, de 3 de julio, de reconocimiento de la Universidad Francisco de Vitoria.

64 El Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal –en vigor– establece que la persona o entidad que pretenda crear un fichero de datos de carácter personal lo notificará previamente a la Agencia Española de Protección de Datos. El Director de la Agencia

Española, a propuesta del Registro General de Protección de Datos, acordará la inscripción de los ficheros de titularidad privada “si la notificación contuviera la información preceptiva y se cumplen las restantes exigencias legales, requiriendo, en caso contrario, al responsable del fichero para que la complete o subsane en el plazo de diez días, con indicación de que, si así no lo hiciera, se le tendrá por desistido de su petición, archivándose sin más trámite” –arts. 6 y 7–.

65 Una posible solución sería la creación del fichero de la universidad privada través de una disposición de carácter general de la Consejería que tuviera las competencias sobre universidades.

66 Cfr. A. TRONCOSO REIGADA, *Privatización, Empresa Pública y Constitución*, Marcial Pons, Madrid, 1997, págs. 37-42.

67 La LPD de la Comunidad de Madrid exceptúa expresamente “las sociedades mercantiles a que se refiere el art. 2.2.)1 de la Ley 1/1984, de 19 de enero, reguladora de la Administración Institucional de la Comunidad de Madrid.

68 Cfr. los Anteproyectos de Valencia, Galicia y Castilla la Mancha.

69 La regulación catalana puede encontrar justificación para facilitar el control de la Agencia Autonómica de Protección de Datos sobre los centros sanitarios privados que se encuadran en el Servicio Catalán de Salud. El modelo catalán de salud se caracteriza por su gestión a través de una red privada concertada. Así, un posible fichero centralizado de historias clínicas –que sería un fichero público de titularidad de la Conselleria– puede prever un encargado de tratamiento o la cesión a los centros sanitarios privados, que estarían en todo caso sometidos al control de la Agencia Autonómica.

70 De hecho, el Gobierno no recurrió al Tribunal Constitucional el art. 3.2 de la Ley Catalana, aunque la razón de fondo de la ausencia de impugnación no fue la consideración de la constitucionalidad de la Ley sino la falta de oportunidad política de la presentación de un recurso de inconstitucionalidad por parte del Gobierno.

71 Cfr. L. LÓPEZ GUERRA, “El reparto de competencias Estado-autonomías en la jurisprudencia del Tribunal Constitucional”, en AA.VV *Comunidades Autónomas y Comunidad Europea. Relaciones jurídico-institucionales*,

Cortes de Castilla y León, Valladolid 1991, págs. 231-249; C. VIVER I PI-SUNYER, *Materias competenciales y Tribunal Constitucional*, Ariel, Barcelona, 1989.

72 Esto no obsta para que puedan existir diferencias de criterio. Así, la Agencia Española de Protección de Datos mantiene que el Reglamento de Medidas de Seguridad para ficheros automatizados puede aplicarse también a los ficheros manual-estructurados –en soporte papel– para fundamentar una resolución de infracción administrativa, mientras que la Agencia de Protección de Datos de la Comunidad de Madrid mantiene que puede recomendarse la implantación de algunas medidas previstas en el Reglamento de Seguridad para ficheros informatizados, aunque no puede fundamentar una resolución de infracción administrativa en virtud de la aplicación del principio *nulla crimen sine legge* y *nulla pena sine legge* y de la prohibición de extender *in malam partem* las infracciones administrativas. Cfr. A. TRONCOSO REIGADA, “Introducción” a la Guía de Protección de Datos Personales para Ayuntamientos, Civitas, Madrid, 2004, págs. Cfr. también la Recomendación 2/2004, de 30 de junio, de la Agencia de Protección de Datos de la Comunidad de Madrid sobre custodia, archivo y seguridad de los datos de carácter personal de las historias clínicas no informatizadas.

73 Un estudio del Reglamento de Seguridad se puede ver en E. DEL PESO, *Ley de Protección de Datos*, Díaz de Santos, 2000 págs. 29-41. Una visión más amplia desde la auditoría de sistemas de información en M. G. PIATTINI y E. DEL PESO, *Auditoría informática*, Ra-ma, Madrid, 2000.

74 Igualmente, por Resolución de 14 de junio del Director de la Agencia de Protección de Datos de la Comunidad de Madrid se aprobaron los modelos de impresos y los medios por los que debe procederse a la notificación de inscripciones de creación, modificación o supresión de ficheros en el Registro de Ficheros de Datos Personales.

75 Cfr. A. TRONCOSO REIGADA, “Dogmática administrativa y Derecho Constitucional: el caso del servicio público”, *Revista Española de Derecho Constitucional* núm. 57, 1999, págs. 87-164.

76 Cfr. más ampliamente A TRONCOSO REIGADA, “Contribución de las Agencias Autonómicas al derecho fundamental a la protección de datos personales”, cit., págs. 41-45.

77 Cfr. AA.VV, “Administración y Constitución: el principio

de coordinación”, *Documentación Administrativa*, n.º 230-231, 1992; ;M. ALVAREZ RICO, “El principio de coordinación en el Estado de las Autonomías”, *Documentación Administrativa*, n.º 196,1982, págs. 5-48.

78 Cfr. F. BALAGUER CALLEJÓN, “Igualdad de los ciudadanos y proceso de descentralización” en J. ASENSI SABATER, *Ciudadanos e instituciones en el constitucionalismo actual*, Tirant Lo Blanch/UNIVERSIDAD de Alicante, Valencia, 1997.

79 Cfr. E. BARRACHINA JUAN, “Problemas de ejecución del principio de coordinación”, *Revista de Administración Pública*, n.º 128, 1992, págs. 225-234.

80 Cfr. A. GUILLO SÁNCHEZ-GALIANO y D. CORDOBA CASTROVERDE, “Principio de coordinación en la jurisprudencia del Tribunal Constitucional”, *Documentación Administrativa*, n.º 230-231, 1992, págs. 337-387.

81 Cfr. P. SANTOLAYA MACHETTI, “En torno al principio de cooperación”, *Revista de Derecho Político*, núm. 21, 1984, págs. 83-109; A. HERNÁNDEZ LAFUENTE, “Coordinación, colaboración y cooperación. El desarrollo del principio de cooperación” y “Técnicas y fórmulas de cooperación en el Estado autonómico”, en AA.VV *El funcionamiento del Estado Autonómico*, MAP, Madrid, 1996, págs. 419-447 y 479-501.

82 Cfr. A. DE MARCOS, “Jurisprudencia constitucional sobre el principio de cooperación”, *Documentación Administrativa*, n.º 240, 1994, págs. 265-353, 1994; J. TAJADURA TEJADA, “El principio de cooperación en el Estado autonómico”, *Revista Vasca de Administración Pública*, núm. 46 1996, págs. 177-238.

83 Este apartado recoge sustancialmente el informe que elaboré como Director de la Agencia de Protección de Datos de la Comunidad de Madrid como respuesta a un informe de la Agencia Española de Protección de Datos, de 13 de noviembre de 2003 que apareció publicado en la Memoria de dicha Agencia de 2002.

84 Acerca del Registro General de Protección de Datos, cfr. más ampliamente M. VIZCAINO op. cit. .

85 Hay que hacer constar que este Real Decreto continua vigente, en virtud de lo previsto en la Disposición Transitoria Tercera LOPD que establece expresamente la subsistencia de este Real Decreto en cuanto no se oponga a la Ley.

86 Como hemos señalado anteriormente, se encuentran en fase de elaboración los anteproyectos de ley de creación de la Agencia Valenciana de Protección de Datos, de creación de la *Autoridade Galega* de Protección de Datos y de la Agencia de Protección de Datos de Castilla la Mancha.

87 Exposición de Motivos. Apdo. III.

88 Cfr. los Anteproyectos de Valencia, Galicia y Castilla la Mancha.

89 Esta consideración se encuentra en el Informe de la Agencia Española de Protección de Datos ya mencionado.

90 Cfr. los Anteproyectos antes mencionados.

91 La Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid fue informada favorablemente por la Agencia Española de Protección de Datos –Informe de 5 de marzo y de 21 de mayo de 2001.

92 Cfr. los Anteproyectos Autonómicos antes mencionados.

93 El Decreto 99/2002, de 13 de junio fue informado favorablemente por la Agencia Española de Protección de Datos, con fecha 14 de junio de 2002. En este Informe se señalaba: “Examinada la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, así como la normativa de desarrollo de la misma, y considerando igualmente la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal de la Comunidad Autónoma de Madrid *debe indicarse que el texto de proyecto de disposición normativo se ajusta plenamente a las mismas, sin que se aprecie, desde el punto de vista jurídico, incorrección o deficiencia que deba ser puesta de relieve*”.

94 Esta posibilidad ha sido aceptada expresamente por la Agencia Española de Protección de Datos, en el informe emitido con fecha 6 de marzo de 2001, al informar favorablemente el proyecto de ley 8/2001, de 13 de julio. En dicho informe se señalaba que: “No obstante, debe recordarse lo que ya se indicó en nuestro anterior informe, en el sentido de que es necesario que de lo dispuesto en el artículo 20 se derive con claridad y precisión que la inscripción en el Registro de la Comunidad de Madrid no es óbice para que el responsable haya de inscribir el fichero en el Registro

General de Protección de Datos, *sin perjuicio de que el trámite para obtener dicha inscripción pueda ser, vía convenio de cooperación, la remisión de la solicitud del fichero inscrito en el Registro Autonómico por la Agencia de la Comunidad de Madrid*" Por ello, la Agencia de Protección de Datos de la Comunidad de Madrid ha comunicado al Registro General de Protección de Datos 5.523 ficheros públicos automatizados inscritos en el Registro de Ficheros de Datos Personales de la Comunidad de Madrid, que forman parte de los más de 9.500 ficheros inscritos en el Registro autonómico (conjuntamente con los más de 3.700 ficheros manuales y con los preexistentes a su creación).

95 La inscripción en el Registro autonómico de Ficheros de Datos Personales se hace habitualmente de oficio –sin comunicación del responsable del fichero–, pues ésta es una posibilidad que en aras de la simplificación administrativa permite el Decreto 99/2002, de 13 de junio. La comunicación de la creación, modificación o supresión del fichero público al Registro General también está fundamentada en los diferentes Convenios de Colaboración que la APDCM tiene suscritos con las Universidades Públicas, con la Federación de Municipios de Madrid y con la Unión Interprofesional de la Comunidad de Madrid.

La APDCM ha notificado a la Agencia Española los cambios en los ficheros públicos de la Comunidad de Madrid, pero no debate la competencia de inscripción en el Registro General de Protección de Datos, que ha sido realizada por Resolución del Director de la Agencia Española de Protección de Datos, resolución que era notificada tanto a la APDCM como al responsable del fichero. La APDCM ha solicitado la inscripción de los ficheros en el Registro General utilizando los modelos de comunicación normalizados por la Agencia Española. Este es el procedimiento por el que se han inscrito los ficheros públicos del territorio de la Comunidad de Madrid los últimos ocho años. Así, la APDCM ha ido notificando a la Agencia Española de Protección de Datos la creación, modificación y supresión de los ficheros públicos para su inscripción en su Registro General, y colaborando de esta manera con la calidad del Registro General.

96 La Agencia de Protección de Datos de la Comunidad de Madrid propuso, con fecha 22 de septiembre de 2003, un Protocolo elaborado por el Subdirector General de Consultoría y Registro de Ficheros Francisco José López Carmona para mejorar el procedimiento de

notificación al Registro General de Protección de Datos de la Agencia Española de los ficheros inscritos y de las modificaciones del Registro de Ficheros de Datos Personales de la APDCM, todo ello encaminado a facilitar la inscripción en dicho Registro General. A tal efecto, se proponía el estudio conjunto de vías que pueden contemplar, entre otras: la descarga directa por la Agencia Española de las inscripciones y modificaciones del Registro de Ficheros de Datos Personales de la APDCM a través de un procedimiento telemático; el envío automático de las modificaciones registrales con la periodicidad que se acuerde (por tanto sin necesidad de intervención ad-hoc de la Agencia de Protección de Datos de la Comunidad de Madrid para cada envío); la utilización de certificación y firma electrónicas en los envíos; la notificación también telemática de modificaciones en el Registro General de Protección de Datos que afecten a las competencias de esta Agencia; la interconexión de los sitios web de ambas Agencias en lo relativo al registro de ficheros (sindicación/exportación de contenidos u otras vías), y finalmente; cualesquiera otros mecanismos de naturaleza técnica que se acuerden. En este mismo sentido, la APDCM mostró su voluntad de colaboración en la definición general de los formatos de intercambio de datos que la Agencia Española de Protección de Datos pueda tener la intención de desarrollar en relación con las Agencias de Protección de Datos de las Comunidades Autónomas. Estas iniciativas podrían materializarse del siguiente modo: la elaboración, por los respectivos responsables de registro de ficheros, de un plan de trabajo conjunto, incluyendo objetivos de entre los reseñados u otros nuevos que pudieran plantearse, así como plazos de realización; el análisis y aprobación del plan de trabajo por los Directores de ambas Agencias; el establecimiento de un mecanismo periódico de seguimiento técnico (por ejemplo, una reunión trimestral entre los responsables de registro de ficheros); la definición de una comisión de dirección del proyecto con frecuencia semestral.

Este Protocolo de Actuación contaba con un Anexo, que recogía el Planteamiento Técnico. La interconexión entre el Registro General de Protección de Datos y el Registro de Ficheros de Datos de Carácter Personal de la APDCM se podría realizar a partir de los siguientes componentes y tareas: definición de los formatos de intercambio de datos. Se propone la utilización del protocolo XML para la especificación técnica de los mismos, dado que garantiza el intercambio de datos y a la vez la

independencia entre los estándares técnicos de las distintas Agencias (una agencia podría tener el registro de ficheros basado en Oracle, otra en SQLServer/Visual Basic, una tercera en DB2/Java, y todas ellas podrían intercambiar datos sin necesidad de modificar sus arquitecturas técnicas básicas); determinación de las reglas de intercambio y validación de la información a la entrada en cada registro, e implantación de las mismas atendiendo a las peculiaridades técnicas de los mismos. En este particular, se incluyen consideraciones tales como: periodicidad de los mensajes automáticos de intercambio de datos (o bien descarga bajo demanda); categorías de mensajes (notificación de inscripción, informativo, solicitud de información, error, etc...); reglas de validación y comunicación de errores en tratamientos automáticos; determinación de los mecanismos técnicos de intercambio (se proponía la utilización de los protocolos SOAP y UDDI); definición de los mecanismos de seguridad y autenticación. En particular, se proponía la utilización de firma electrónica clase 2CA o compatible, que es la utilizada por la Fábrica Nacional de la Moneda y Timbre – Real Casa de la Moneda para las aplicaciones públicas más extendidas (por ejemplo, la declaración de IRPF a través de Internet). De igual modo, se incluirían en este apartado los elementos de transmisión cifrada de la información, que pueden incorporar componentes de alto nivel y coste moderado (por ejemplo, protocolo https), o bien otros de mayores garantías aunque también coste y complejidad técnica (protocolo IPSEC, etc...); mecanismos para la notificación automática a terceros (por ejemplo, notificación al responsable de fichero mediante correo electrónico cifrado y firmado electrónicamente por la APDCM de modificaciones realizadas en el registro de la misma o incluso en el Registro General de Protección de Datos en ámbitos de su competencia), así como para el acceso telemático a los datos personales del registro de ficheros correspondiente previa autenticación mediante certificado electrónico; definición de tipos de contenido, estructuras de datos, formatos de intercambio (XML) y reglas de publicación para el intercambio de contenidos entre los sitios web de la Agencia de Protección de Datos y de la Agencia de Protección de Datos de la Comunidad de Madrid.

97 En esta dirección, la Agencia de Protección de Datos de la Comunidad de Madrid siempre ha resaltado en su actividad formativa la función de publicidad que corresponde al Registro General de Protección de Datos y la comunicación que hace la Agencia Autónoma a la

Agencia Española para la inscripción de los ficheros públicos a los que se refiere la Ley 8/2001, de 13 de julio, en el Registro General de Protección de Datos Personales.

98 Llama la atención que el Informe de la Agencia Española de Protección de Datos, de 18 de noviembre, que analiza la inscripción de los ficheros públicos en el Registro General de Protección de Datos no haga mención al contenido de los preceptos ahora señalados del Real Decreto 1332/1994 que es el que desarrolla reglamentariamente en su Capítulo III el procedimiento de notificación y de inscripción de ficheros en el Registro General.

99 Esta posición es también la más coherente con el Decreto 99/2002, de 13 de junio, que regula el procedimiento de declaración e inscripción de ficheros públicos en la Comunidad de Madrid –informado favorablemente por la Agencia Española de Protección de Datos–, con las Resoluciones de los Directores de la Agencia Española de Protección de Datos de los últimos años que han inscrito los ficheros públicos de oficio después de la notificación de la Agencia de la Comunidad de Madrid y con los informes de todos los abogados del Estado destinados en el Servicio Jurídico del Estado adscrito a la Agencia Española de Protección de Datos, a excepción del mencionado de fecha de 13 de noviembre de 2003.