

INTEGRACIÓN EUROPEA Y PROTECCIÓN DE DATOS
PERSONALES. LAS GARANTÍAS ESPECÍFICAS DEL DERECHO
A LA PROTECCIÓN DE DATOS PERSONALES

Mónica Arenas Ramiro.
Profesora Asociada de Derecho Constitucional.
Universidad de Alcalá.

SUMARIO: I. La exigencia de crear Autoridades nacionales independientes de protección de datos. II. La necesidad de crear Autoridades independientes para garantizar el derecho a la protección de datos personales III. Las Autoridades nacionales independientes de protección de datos de los Estados miembros de la Unión Europea: 1. Organización; 2. Funciones y competencias: 2.1. Competencias; 2.2. Ámbito competencial.

El reconocimiento del derecho a la protección de datos personales va de la mano de los avances científicos y tecnológicos experimentados, especialmente, en el terreno de la informática. Las nuevas tecnologías permiten almacenar datos personales en cantidades y por periodos de tiempo hasta ahora inimaginables y permiten su transmisión no sólo dentro de las fronteras de un mismo Estado, sino fuera de éste, al otro lado del mundo. Se puede decir que el derecho a la protección de datos personales tiene una dimensión internacional que no poseen otros derechos fundamentales. Así pues, si las amenazas a este derecho pueden tener carácter transnacional, entonces también el reconocimiento y la garantía del mismo deben tener ese carácter. Con este artículo se pretende poner de manifiesto la relación existente entre el proceso de integración europea y los sistemas de garantías específicos del derecho a la protección de datos personales, en concreto, las conocidas Autoridades independientes de protección de datos personales, que surgen para proteger y garantizar este nuevo derecho fundamental y cuya creación se ha producido a través del proceso típicamente europeo de influencias recíprocas entre los ordenamientos jurídicos nacionales y los ordenamientos jurídicos europeos supranacionales más relevantes en materia de

derechos fundamentales, esto es, el del Consejo de Europa con el Convenio Europeo de Derechos Humanos, y el de la Unión Europea.

I. La exigencia de crear Autoridades nacionales independientes de protección de datos

La exigencia de crear “Autoridades” encargadas de controlar los tratamientos de datos personales se manifestó por primera vez en el ámbito del Consejo de Europa, en el Convenio 108 sobre Protección de Datos,¹ y a través de la jurisprudencia del TEDH, de acuerdo con la cual la falta de este tipo de garantía supone una injerencia injustificada en el derecho garantizado por el artículo 8 del CEDH.² Dicha obligación se concretó definitivamente en el 2001 en el Protocolo Adicional al Convenio 108 en el que se exige expresamente la creación, por parte de los Estados firmantes del mismo, de una o más Autoridades que ejerzan sus funciones con total independencia y que sean responsables de asegurar la conformidad de las medidas que den cumplimiento, en el Derecho interno, a los principios básicos de la protección de datos y al flujo transfronterizo de los mismos recogidos en el Convenio 108.³

Posteriormente, en la Unión Europea, la normativa comunitaria, en especial, la Directiva 95/46/CE, de 24 de octubre de 1995, sobre Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante Directiva 95/46/CE sobre Protección de Datos Personales),⁴ y las normas reguladoras de los sistemas de información del tercer pilar de la Unión Europea en materia de cooperación policial y judicial en materia penal (Sistema de Información Schengen (SIS), Sistema de Información Aduanera (SIA), Europol y Eurojust), han exigido a los Estados miembros la creación de este tipo de Autoridades independientes

¹ Convenio 108, de 28 de enero de 1981, para la Protección de las Personas respecto al Tratamiento Automatizado de Datos de Carácter Personal. España lo ratificó por Instrumento de 27 de enero de 1984 (BOE de 15 de noviembre de 1985). Vid. Art. 13.1 y 2.a) Convenio 108, relativo a la cooperación entre las Partes firmantes del mismo, que dispone: “1. Las Partes se obligan a concederse mutuamente asistencia para el cumplimiento del presente Convenio. 2. A tal fin, a) cada Parte designará a una o más autoridades cuya denominación y dirección comunicará al Secretario general del Consejo de Europa (...)”.

² Vid., en concreto, STEDH de 7 de julio de 1989, caso *Gaskin*.

³ Art. 1.1 y 3 Protocolo Adicional al Convenio 108.

⁴ El art. 28.1 Directiva 95/46/CE sobre Protección de Datos Personales establece: “1. 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. Estas autoridades ejercerán las funciones que les son atribuidas con total independencia”.

para garantizar el derecho fundamental a la protección de datos personales. Esta exigencia se ha visto completada con lo previsto en los artículos I-51 y II-68 del Tratado que establece la Constitución Europea, que exigen de la misma manera la existencia de “Autoridades” independientes encargadas de garantizar el derecho fundamental a la protección de datos personales en el ámbito de la Unión Europea.⁵

Brevemente, señalar aquí que en el ámbito de la Unión Europea, además de la exigencia de estas Autoridades nacionales de control destaca la existencia de un Supervisor Europeo de Protección de Datos (SEPD) y de unas Autoridades de Control Común dentro del marco del tercer pilar. El primero, creado por el Reglamento CE nº 45/2001 sobre Protección de Datos Personales por parte de las instituciones y órganos comunitarios, en cumplimiento del mandato contenido en el artículo 286 TCE, que establece la creación de un organismo de vigilancia independiente, responsable de controlar que las instituciones y organismos de Unión cumplan con la normativa comunitaria sobre protección de datos personales.⁶ Y, las segundas, debido a la falta de competencia directa del SEPD para actuar en el ámbito del tercer pilar, encargadas de garantizar la protección de datos personales en los tratamientos de datos que se realicen en los sistemas de información desarrollados a nivel europeo para la cooperación en materia policial y judicial.⁷

⁵ Según el art. I-51 (cuya redacción coincide con la del art. 286 TCE): “1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. La Ley o Ley marco europea establecerá las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes”. Y conforme el art. II-68 (que reproduce el art. 8 de la Carta de Derechos Fundamentales de la Unión Europea): “1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente”. Sobre esta cuestión, entre otros, vid. DONATI, F. “Art. 8. Protezione dei dati di carattere personale”, en BIFULCO R. / CARTABIA M. / CELOTTO, A. *L’Europa dei Diritti. Commento alla Carta dei Diritti Fondamentali dell’Unione Europea*, Società Editrice il Mulino, Bologna, 2001, p. 87; BERNSDORFF, N. “Kapitel II, Freiheiten: Artikel 6 bis 19”, en MEYER, J. (coord.), *Kommentar zur Charta der Grundrechte der Europäischen Union*, Nomos Verlagsgesellschaft, Baden-Baden, 2003, p. 164; y KÜBLER, J. *Die Säulen der Europäischen Union: einheitliche Grundrechte?*, Nomos Verlag, Baden-Baden, 2002, pp. 197-198 y 201.

⁶ Reglamento CE nº 45/2001, de 18 de diciembre de 2000, del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

⁷ Aunque el Reglamento Eurodac también creó este tipo de Autoridad, cuando se creó el SEPD todas las funciones de la misma pasaron a ser asumidas por éste. Sobre la creación de estas ACC, vid. art. 115

Finalmente, fruto de esta obligación a nivel europeo, los Estados miembros han creado en sus respectivos ordenamientos jurídicos nacionales “Autoridades independientes” encargadas de controlar los tratamientos de datos personales y garantizar de esta forma el derecho a la protección de datos.⁸ Los Estados se han encargado de introducir en sus respectivos ordenamientos jurídicos los elementos de garantía que, del derecho a la protección de datos personales, han extraído los anteriores ámbitos supranacionales ya mencionados, es decir, el del Consejo de Europa y el de la Unión Europea. Y es en este punto donde más evidente se hace el proceso de integración europeo, a la hora de crear estas Autoridades independientes. Así por ejemplo, en España, a la hora de crear este tipo de “Autoridad” se tuvo en cuenta lo establecido en la normativa internacional sobre la materia que vincula a nuestro Estado: el Convenio 108, aprobado en el seno del Consejo de Europa, aunque no definía los criterios ni las pautas que debían inspirar la actuación y las funciones del citado órgano en el ámbito nacional; el Acuerdo de Schengen que exigía que cada Parte contratante designara a una autoridad de control independiente encargada de controlar el fichero de la parte nacional del sistema de Schengen;⁹ y, por último, la Directiva 95/46/CE sobre Protección de Datos Personales que estableció los criterios que debían regir la creación y organización de estas autoridades en los países miembros.¹⁰

II. La necesidad de crear Autoridades independientes para garantizar el derecho a la protección de datos personales

En Europa se ha considerado que la garantía del derecho a la protección de datos personales exigía mecanismos específicos adicionales a los mecanismos establecidos

Convenio Schengen; art. 18 Convenio SIA; art. 20 Reglamento Eurodac (y art. 20.11 sobre su disolución); art. 24 Convenio Europol; y art. 23 Decisión Eurojust.

⁸ Vid. TÉLLEZ AGUILERA, A. *Nuevas tecnologías. Intimidad y protección de datos con estudio sistemático de la LO 15/1999*, Edisofer, Madrid, 2001, p. 206; HERRÁN ORTÍZ, A.I., *El derecho a la intimidad en la nueva Ley Orgánica de protección de datos personales*, Dykinson, Madrid, 2002, pp. 323-324; y, SERRANO PÉREZ, M.M., *El derecho fundamental a la protección de datos. Derecho español y comparado*, Thomson/Civitas, Madrid, 2003, pp. 461-465.

⁹ Arts. 114.1 y 128.1 Acuerdo Schengen, ratificado por Instrumento de 23 de julio de 1993.

¹⁰ Art. 13.2 Convenio 108, que impone a los Estados partes la designación de una o varias autoridades de control, cuya ubicación y denominación debían comunicarse al Secretario General del Consejo de Europa. Y, posteriormente, art. 28 Directiva sobre Protección de Datos, que también menciona la posibilidad de la existencia de más de una autoridad de control en un Estado miembro. Vid. TÉLLEZ AGUILERA, A. *Nuevas tecnologías. Intimidad...*, op. cit., p. 206; HERRÁN ORTÍZ, A.I., *El derecho a la protección de datos personales en la sociedad de la información*, Cuadernos Deusto de Derechos Humanos, nº 26, Universidad de Deusto, Bilbao, 2003, pp. 85-86.

con carácter general para proteger los derechos fundamentales. Por este motivo, a diferencia de lo que ha ocurrido en Estados Unidos, donde la garantía del derecho a la protección de datos personales se ha encomendado a los Tribunales ordinarios,¹¹ en Europa se ha considerado necesario crear un determinado tipo de organismos, las Autoridades nacionales de protección de datos, encargadas de controlar el cumplimiento de la normativa sobre protección de datos personales y que sirven así de garantía específica al derecho a la protección de datos personales.

Los argumentos esgrimidos para justificar la creación de estas Autoridades han sido principalmente tres: En primer lugar, la necesidad de establecer un mecanismo preventivo, ya que en el campo de la protección de los datos personales, frente a las amplias posibilidades que ofrecen las técnicas informáticas, la vía jurisdiccional posterior a la lesión del derecho resulta insuficiente y poco adecuada;¹² En segundo lugar, la especialización técnica de las mismas, pues se trata de un campo en el que es necesaria una cualificación y especialización técnica específica en la materia de las personas que las componen;¹³ Y, por último, y lo más importante, la independencia en el ejercicio de la tarea que tienen atribuida, que actúen libres de órdenes e instrucciones, en su labor de garantía del derecho a la protección de datos personales, sin estar movidas por ningún tipo de interés político o económico.¹⁴ Las Directivas sobre Protección de Datos establecen las características generales que deben cumplir este tipo de Autoridades, exigiéndolas ese carácter “independiente”, pero son finalmente los

¹¹ No es esta la única diferencia entre el sistema europeo y el norteamericano, ya que mientras el europeo tiene un carácter preventivo, el norteamericano exige que se haya producido el daño. Vid. GARRIGA DOMÍNGUEZ, A., *La protección de los datos personales en el derecho español*, Dykinson, Madrid, 1999, p. 249; de la misma autora, *Tratamiento de datos personales y derechos fundamentales*, Dykinson, Madrid, 2004, pp. 183-184; MARTÍNEZ MARTÍNEZ, R. “El control de la Agencia de Protección de Datos sobre los ficheros automatizados de carácter personal de las Fuerzas y Cuerpos de Seguridad del Estado”, en *Cuadernos constitucionales de la Cátedra Fadrique Furió Ceriol*, nº 30-31, 2000, pp. 80-81; HEREDERO HIGUERAS, M. “La Agencia de Protección de Datos”, en *Informática y Derecho*, nº 6/7, 1994, p. 323; y SÁNCHEZ BRAVO, A.A., *La protección del derecho a la libertad informática en la Unión Europea*, Ed. Universidad de Sevilla, Sevilla, 1998, pp. 115-116. Para otras clasificaciones, vid. TÉLLEZ AGUILERA, A., *Nuevas tecnologías. Intimidación...*, op. cit., p. 208; y DAVARA RODRÍGUEZ, M.A., *La protección de datos en Europa. Principios, derechos y procedimiento*, ASNEF, Madrid, p. 59.

¹² Sobre esta cuestión, vid. Considerando 54 y art. 20 Directiva 95/46/CE sobre Protección de Datos Personales. Aunque es una exigencia, sólo exigen ese control preventivo Italia, el Reino Unido, Hungría, Lituania y Eslovaquia.

¹³ Sobre este argumento, vid. SALVADOR MARTÍNEZ, M. *Autoridades independientes*, Ariel, Barcelona, 2002, p. 348.

¹⁴ En este sentido destaca el objetivo de la “neutralidad política”, mediante el que se explica la necesidad de que ciertas actividades se ejerzan al margen de las “luchas de partidos”, y, más concretamente, de los órganos del Estado en los que tiene lugar la lucha política. Se ha afirmado así que la protección de ciertos derechos no puede dejarse en manos de órganos políticos del Estado, pues es frente a ellos, aunque no

Estados miembros los que deciden cómo crear y qué organización dar a su Autoridad nacional de control.¹⁵

Así, por ejemplo, en nuestro ordenamiento jurídico, el Tribunal Constitucional se ha pronunciado sobre la necesidad de crear este tipo de Autoridades de protección de datos, en concreto de la Agencia Española de Protección de Datos (AEPD). De acuerdo con el Tribunal Constitucional la creación de esta “Autoridad independiente” se deduce, por un lado, de la necesidad de una respuesta rápida, especializada técnicamente y que actúe de forma preventiva, pues, frente a las amplias posibilidades informáticas, la vía jurisdiccional resulta insuficiente e inadecuada para proteger los datos personales; y, por otro lado, de la necesidad de crear un órgano de control independiente del Gobierno, pues la Administración también debe cumplir las normas de protección de datos y queda sometida a control.¹⁶

III. Las Autoridades nacionales independientes de protección de datos de los Estados miembros de la Unión Europea

Ya hemos visto como tanto el Consejo de Europa en su Convenio 108 sobre Protección de Datos, y el Protocolo Adicional al mismo, como las Directivas sobre Protección de Datos Personales y las normas reguladoras de los sistemas de información creados en el marco del tercer pilar (en especial, SIS, SIA, Europol y Eurojust) exigen que cada Estado miembro nombre a una Autoridad Independiente de Control que se encargue de vigilar, de forma independiente, el cumplimiento a nivel nacional de las disposiciones adoptadas en aplicación de la normativa europea sobre protección de datos personales.

sólo, frente a quienes se quieren garantizar. Vid. SALVADOR MARTÍNEZ, M. *Autoridades independientes*, op. cit., pp. 344-348.

¹⁵ *Primer Informe de la Comisión relativo a la aplicación de la Directiva sobre Protección de Datos 95/46/CE*, de 15 de mayo de 2003 (COM (2003) 265 final), p. 38; y KORFF, D., *EC study on implementation of data protection Directive*, Human Rights Centre, University of Essex, Colchester (UK), Cambridge (UK), September, 2002, pp. 200 y 203.

¹⁶ Vid. STC 290/2000, FJ 9º que mantiene que: “...el legislador, sin excluir en modo alguno el recurso último a los órganos jurisdiccionales para la tutela de los derechos individuales (...) no ha querido, sin embargo que la protección de datos personales frente al uso de la informática se lleve a cabo exclusivamente en la vía judicial, esto es, cuando ya se ha producido una lesión del derecho fundamental. Por el contrario, ha querido que dicha protección se lleve a cabo mediante el ejercicio por la Agencia de protección de Datos, con carácter básicamente preventivo...”. Vid. SALVADOR MARTÍNEZ, M. *Autoridades independientes*, op. cit., pp. 270-271; MARTÍNEZ MARTÍNEZ, R. “El control de...”, op. cit., pp. 80-81; y LUCAS MURILLO DE LA CUEVA, P. *El derecho a la autodeterminación informativa*, Tecnos, Madrid, 1990, p. 140.

De esta forma, en todos los Estados miembros de la Unión Europea, incluso en los nuevos Estados que se adhirieron en mayo de 2004, se han creado Autoridades nacionales de protección de datos personales.¹⁷ Las Autoridades nacionales de protección de datos existentes en los Estados miembros de la Unión Europea son las siguientes:

- En Alemania, el Comisionado Federal para la Protección de Datos (*Bundesbeauftragter für den Datenschutz*), creado por la Ley de protección de datos alemana con la función de velar por el cumplimiento de la Ley en el sector público es nombrado por el Presidente de la Federación tras haber sido elegido por el Bundestag. Junto al Comisionado se han creado otras dos figuras, el Oficial para la protección de datos (*Beauftragter für den Datenschutz*) y la Autoridad de supervisión (*Aufsichtsbehörde*). El primero debe ser nombrado por cada organismo, público o privado, que desee realizar un tratamiento de datos personales y su tarea es la de “vigilar” los tratamientos de datos que el mencionado organismo realice; la segunda, la Autoridad de Supervisión, que puede ser designada por los Gobiernos de los *Länder*, se encarga de comprobar todos los tratamientos de datos personales que se realicen, llevando un registro de los mismos y pudiendo notificar las infracciones que se cometan a los órganos competentes en función de la infracción cometida. Hay que señalar finalmente que en Alemania, al ser un Estado federal, además del Comisionado Federal, se han creado Autoridades de protección de datos en los diferentes *Länder* (*Landesdatenschutzbeauftragten*), que son designadas por los Gobiernos de los *Länder* o por los órganos que éstos designen para controlar los tratamientos de datos personales en el ámbito que los mismos determinen.¹⁸

- En Austria, la Comisión Austriaca de Protección de Datos (*Österreichische Datenschutzkommission*). La Ley de protección de datos austriaca

¹⁷ Las direcciones de todas estas Autoridades, así como sus páginas web se pueden encontrar en http://europa.eu.int/comm/internal_market/privacy/links_en.htm. Las referencias a las Leyes de los distintos países son hechas a las Leyes de protección de datos de los mismos que se pueden encontrar en la misma página web. Sobre estas Autoridades, vid. también, *Primer Informe de la Comisión relativo a la aplicación de la Directiva sobre Protección de Datos 95/46/CE*, de 15 de mayo de 2003 (COM (2003) 265 final), pp. 38-41; KORFF, D. *EC study on...*, op. cit., pp. 200-209; y TÉLLEZ AGUILERA, A., *La protección de datos en la Unión Europea. Divergencias normativas y anhelos unificadores*, Edisofer, Madrid, 2002, a lo largo de las pp. 77-163.

¹⁸ Sobre el Comisionado alemán, vid. arts. 22-26 Ley alemana; y sobre las otras figuras, arts. 4f y 4g, y art. 38 de la misma Ley. Sobre esta cuestión, vid. VOGELGESANG, K. “Verfassungsregelungen zum Datenschutz”, en *CR*, 11 (1995) 9, p. 560; y *Primer Informe de la Comisión relativo a la aplicación de la Directiva sobre Protección de Datos 95/46/CE*, de 15 de mayo de 2003 (COM (2003) 265 final), p. 38.

establece que para garantizar la protección de datos personales, además de las garantías genéricas, se deben crear una Comisión de Protección de Datos (*Datenschutzkommission*), compuesta por miembros nombrados a propuesta del Gobierno federal por el Presidente de la Federación; y un Consejo de Protección de datos (*Datenschutzrat*), para el asesoramiento del Gobierno Federal y de los Gobiernos de los *Länder* en cuestiones jurídico-políticas de protección de datos, compuesto por representantes de los partidos políticos, un representante de los Tribunales laborales y del Tribunal de Cuentas, dos representantes de los *Länder*, un representante de los municipios y de las ciudades, y un representante del Canciller alemán.¹⁹

- En Bélgica, la Comisión para la protección de la vida privada (*Commission de la protection de la vie privée*), compuesta por miembros elegidos por la Cámara de Representantes y por el Senado.²⁰ En el seno de la Comisión se crean una serie de Comités sectoriales (*Comités sectoriels*) competentes para instruir las demandas relativas al tratamiento o a la comunicación de datos personales.²¹ Además, la Ley ha creado la figura del “oficial encargado para la protección de datos” (“*préposé à la protection des données*”), designado por el responsable del tratamiento para aquellos tratamientos de datos más “peligrosos”, encargado de asegurar, de forma independiente, la aplicación de la Ley.²²

- En Chipre, el Comisionado para la Protección de Datos (*Commissioner for Personal Data Protection*). Este Comisionado tiene como función la garantía del cumplimiento de la legislación sobre protección de datos personales. Esta figura destaca por su estrecha relación con el Consejo de Ministros de quien también recibe su remuneración.²³

- En Dinamarca, la Agencia de Protección de Datos Danesa (*Datatilsynet*). Esta Agencia, que consta de un Consejo y una Secretaría, está encargada de la

¹⁹ Esta Comisión se regula en los arts. 35-44 Ley austriaca.

²⁰ Esta Comisión se regula en los arts. 23-36 Ley belga.

²¹ Vid. art. 36.bis y 31.bis Ley belga sobre protección de datos personales. Vid., también, *Séptimo Informe Anual sobre la situación de la protección de las personas en lo que respecta al tratamiento de los datos personales y a la protección de la vida privada en la Unión Europea y en terceros países, relativo a los años 2002 y 2003*, adoptado el 21 de junio de 2004, p. 10.

²² El art. 17 bis Ley belga, se refiere, en relación con los tratamientos de datos personales que pueden causar más problemas, al “*préposé à la protection des données*”, que según dicho artículo puede ser designado por el responsable del tratamiento “*chargé d’assurer, d’une manière indépendante, l’application de la présente loi ainsi que de ses mesures d’exécution*”.

supervisión de todos los tratamientos de datos personales que entren en el campo de aplicación de la normativa danesa. Se trata de un órgano independiente, que ejerce sus funciones libre de órdenes e instrucciones.²⁴

- En Eslovaquia, la Oficina para la protección de Datos Personales (*Personal Data Protection Office*). Esta Oficina es un órgano de la Administración pública encargada de vigilar de forma independiente la protección de datos personales. La preside un Presidente elegido por el Consejo Nacional de la República de Eslovaquia a propuesta del Gobierno y está asistido de un conjunto de inspectores que son nombrados por el Gobierno a propuesta suya. Las sanciones las puedan imponer tanto el Presidente de la Oficina como sus inspectores, y si las infracciones cometidas son muy graves, el Presidente puede hacer públicos los datos del responsable del tratamiento.²⁵

- En Eslovenia, el Inspectorado para la Protección de Datos Personales (*Inspectorate for Personal Data Protection*). A mediados de 2001, dando cumplimiento al mandato constitucional y a la Ley eslovena de protección de datos, se creó un organismo dependiente del Ministerio de Justicia, con un carácter básicamente preventivo, encargado de informar a los ciudadanos de sus derechos y de recibir las quejas de los mismos.²⁶ A pesar de la existencia de esta Autoridad, debido al “escaso” carácter independiente de la misma, hay que destacar el importante papel que juega el Defensor de los Derechos Humanos de Eslovenia (*Human Rights Ombudsman*), que entre sus funciones tiene encomendada la protección de los derechos constitucionales, entre los que se encuentra la protección de datos personales. Así, las quejas que tengan que ver con la protección de datos personales las resuelve, también, un grupo de especialistas en la materia que forman parte de este organismo.²⁷

- En España, la Agencia Española de Protección de Datos (en adelante, AEPD). En cumplimiento del mandato del artículo 18.4 de la Constitución Española el legislador elaboró, para limitar el uso de la informática, la LORTAD y, posteriormente,

²³ Se regula en los arts. 18-24 Ley chipriota, en la que se establece la forma de elección del mismo, su estatuto y sus funciones.

²⁴ Vid. arts. 55-66 Ley danesa.

²⁵ Arts. 33-48 Ley eslovaca.

²⁶ Antes del 2001 este Inspectorado estaba a cargo de un “experto independiente” del Ministerio de Justicia. En busca de ese carácter independiente, entre los objetivos del Ministerio de Justicia esloveno para el 2005, se encuentra el establecimiento de las condiciones necesarias para la creación y funcionamiento de una autoridad independiente de protección de datos.

²⁷ El art. 38 de la Constitución eslovena reconoce el derecho a la protección de datos personales.

para transponer al ordenamiento interno los cambios introducidos en esta materia por la Directiva 95/46/CE sobre Protección de Datos Personales, aprobó la LOPD, con la finalidad de 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.²⁸ Estas Leyes de protección de datos personales, a través de las cuales se ha desarrollado el derecho fundamental a la protección de datos personales crearon la AEPD para controlar los tratamientos de datos y garantizar dicho derecho fundamental.²⁹ La AEPD está sujeta al régimen jurídico establecido en el Estatuto de la Agencia Española de Protección de Datos (en adelante, EAEPD), aprobado por Real Decreto 428/1993. Tanto la LOPD como el EAEPD la definen como un ente de Derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones.³⁰ Una de las características definitorias de la AEPD es su “independencia”, que deriva, esencialmente, del estatuto de sus miembros. La Agencia se compone de los siguientes órganos: el Consejo Consultivo, el Director y, como órganos jerárquicamente dependientes del Director, el Registro General de Protección de Datos, la Inspección de Datos y la Secretaría General.

A nivel autonómico, y debido a la habilitación contenida tanto en la LORTAD como en la LOPD para que las Comunidades Autónomas crearan y regularan sus propios registros de ficheros y controlaran los ficheros creados y gestionados por ellas mismas, algunas Comunidades Autónomas han aprobado normas autonómicas sobre la

²⁸ Art. 1 LOPD. Recordemos también que en desarrollo de la LORTAD el Gobierno aprobó el Estatuto de la Agencia Española de Protección de Datos (EAEPD) mediante RD 428/1993; el RD 1332/1994, de 20 de junio, que desarrolla determinados aspectos de la LO 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal; el RD 994/1999, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados de datos personales; y el RD 195/2000, por el que se establece el plazo para implantar las medidas de seguridad de los ficheros automatizados previstas por el Reglamento aprobado por el RD 994/1999. Toda esta normativa de desarrollo continúa en vigor tras la aprobación de la LOPD, mientras no la contradiga, tal y como dispone la Disposición Adicional 3ª LOPD.
²⁹ Título VI LOPD.

³⁰ Art. 35.1 LOPD y art. 1 EAEPD. Por este motivo un amplio sector doctrinal ha considerado que la AEPD es una “autoridad administrativa independiente”. En este sentido, COLLADO GARCÍA-LAJARA, E., *Protección de datos de carácter personal*, Comares, Granada, 2000, p. 85; y TÉLLEZ AGUILERA, A., *La protección de...*, op. cit., pp. 299-301; GARCÍA-BERRIO HERNÁNDEZ, T., *Informática y libertades. La protección de datos personales en Francia y España*, Colección Estudios de Derecho, Universidad de Murcia, Murcia, 2003, pp. 355-357; HERRÁN ORTIZ, A.I., *El derecho a la protección...*, op. cit., p. 86; BETANCOR RODRÍGUEZ, A. *Las Administraciones independientes: un reto para el Estado social y democrático de derecho*, Tecnos, Madrid, 1994, pp. 187 y ss.; y SALVADOR MARTÍNEZ, M., *Autoridades independientes*, op. cit..

materia y han creado un “órgano de control” de sus ficheros.³¹ Así, las Comunidades Autónomas que han aprobado normas sobre protección de datos personales son: Madrid, Cataluña, País Vasco, Comunidad Valenciana, Castilla-La Mancha, Navarra, y Castilla y León;³² y de todas éstas, sólo Madrid, Cataluña y el País Vasco cuentan actualmente con Autoridades de protección de datos personales. De la misma forma que a nivel central se ha creado una autoridad independiente encargada de garantizar el derecho a la protección de datos personales, la AEPD, a nivel autonómico las Comunidades Autónomas también han creado “autoridades independientes”, Agencias de Protección de Datos autonómicas, siguiendo el modelo de la AEPD.³³

- En Estonia, la Inspección de la Protección de Datos (*Estonian Data Protection Inspectorate*). La Ley de protección de datos estona califica al Inspector encargado de monitorizar todos los tratamientos de datos que se realicen como órgano “extrajudicial” de carácter independiente. En Estonia esta figura no se regula sólo en la Ley de protección de datos personales, sino también en otras normas relativas a los tratamientos de datos personales. En cualquier caso, la función principal de este Inspector es controlar el cumplimiento de la normativa sobre protección de datos, para lo que se le atribuyen diferentes competencias, entre ellas la potestad sancionadora.³⁴

- En Finlandia, el Defensor de la Protección de Datos (*Data Protection Ombudsman*). Este “Defensor” se encarga de dirigir y supervisar los tratamientos de datos personales. Junto al Defensor se ha creado la Junta de Protección de Datos (*Data*

³¹ Hay que señalar que ningún Estatuto de Autonomía atribuye a su Comunidad Autónoma competencias en materia de protección de datos personales; aunque en alguna Comunidad, como es el caso de Cataluña, el Preámbulo de la Ley de protección de datos hace también referencia a la competencia de los poderes públicos de la Comunidad, recogida en el Estatuto de Autonomía, para promover la igualdad de sus ciudadanos y remover cualquier obstáculo que dificulte el ejercicio de los derechos de los mismos. En este sentido, vid., por ejemplo, de las tres Comunidades que tienen Agencias, el art. 7 Estatuto de Autonomía de la Comunidad de Madrid, el art. 8 Estatuto de Autonomía de Cataluña, y el art. 9 Estatuto de Autonomía del País Vasco. En este sentido, vid. TRONCOSO REIGADA, A., “Las Comunidades Autónomas y la protección de datos personales: marco constitucional y posibilidades para el futuro”, en *Revista parlamentaria de la Asamblea de Madrid*, nº 12, junio 2005, pp. 116 y 127-128, quien señala que en los proyectos de Estatutos de las Comunidades Autónomas de Cataluña y Canarias se reconoce la protección de datos personales como competencia de la Comunidad, extendiéndose el ámbito de control a los ficheros privados.

³² Art. 41.1, 2 y 3 LOPD. Una de las materias para las cuales las Comunidades Autónomas han encontrado una habilitación concreta en la LORTAD o en la LOPD es la delimitación de las funciones, organización y régimen jurídico básico de la Agencia de Protección de Datos de la Comunidad.

³³ Es sabido que las Comunidades Autónomas disponen de una Administración propia, organizada de manera semejante a la Administración General del Estado y en la que también existe un considerable número de entes instrumentales, por lo que los problemas que se planteen a nivel autonómico serán semejantes a los que se planteen a nivel central. Vid. SALVADOR MARTÍNEZ, M., *Autoridades independientes*, op. cit., p. 262.

Protection Board), encargada de las cuestiones relativas a los principios del tratamiento de datos personales, como, por ejemplo, la concesión de la autorización para el tratamiento de determinados datos sensibles. El Defensor proporciona la dirección y el asesoramiento sobre el tratamiento de los datos personales, supervisa el tratamiento y toma decisiones.³⁵

- En Francia, la Comisión Nacional de la Informática y de las Libertades (*Commission Nationale de L'informatique et des Libertés, CNIL*). Esta Comisión es una de las primeras Autoridades de control de protección de datos personales y una de las primeras “autoridades administrativas independientes”, calificativo que le otorga la Ley de protección de datos francesa.³⁶ Por ello, la CNIL ha servido como modelo para muchos otros países. Esta Autoridad se caracteriza por lo que la doctrina francesa ha denominado el “gobierno de los expertos” (“*gouvernement des sages*”), es decir, una composición caracterizada por la independencia del Gobierno (no está sujeta a instrucción u orden alguna) y la neutralidad de sus técnicos y miembros directivos.³⁷ Además, la Ley de protección de datos francesa prevé que un “Comisionado del Gobierno” (*commissaire du gouvernement*), designado por el Primer Ministro, pueda estar presente en la CNIL y pueda acudir a todas las sesiones de la misma en las mismas condiciones que el resto de miembros, asumiendo un papel de “coordinador” de los tratamientos de datos que se realizan en las diferentes administraciones. Junto a este “Comisionado” la Ley francesa, como se prevé en las Leyes alemana, holandesa y sueca, prevé la existencia de un “corresponsal para la protección de datos personales” (“*correspondant à la protection des données à caractère personnel*”), que es un empleado del responsable del tratamiento de datos o de una empresa, que se encarga de controlar los tratamientos de datos que se realicen en el sector o empresa que lo haya

³⁴ Arts. 34-42 Ley estona.

³⁵ Sobre estas figuras, vid. arts. 38-46 Ley finesa.

³⁶ Sobre la CNIL, vid. arts. 11-21 Ley francesa. Vid. también, FENOLL-TROUSSEAU M.P. / HAAS, G., *Internet et protection des données personnelles*, Éditions Litec, Paris, 2000, pp. 17 y 22-23; y GARCÍA-BERRIO, T., *Informática y libertades*..., op. cit., pp. 358-359.

³⁷ GARCÍA-BERRIO, T., *Informática y libertades*..., op. cit., pp. 355-357; BETANCOR RODRÍGUEZ, A., *Las Administraciones independientes*..., op. cit., p. 28; y FLAHERTY, D.H., *Protecting privacy in surveillance societies*, Chapel Hill, University of North Carolina Press, 1989, pp. 182-186. Hay que señalar que el que ningún miembro del Gobierno pueda formar parte de la CNIL refuerza su carácter independiente, pero el que el Gobierno tenga un cierto poder de control directo a la hora de elegir tres miembros hace pensar todo lo contrario. En este sentido, vid. FLAHERTY, D.H., *Protecting privacy in*..., op. cit., pp. 165 y 172-173. Sobre su composición, vid. del mismo autor, pp. 192-200; y BRAIBANT, G., *Données personnelles et société de l'information*, La Documentation Française, París, 1998, pp. 130-132.

designado.³⁸ Se considera que la tarea de la CNIL no es sólo el control del tratamiento de datos personales sino la búsqueda del equilibrio entre la informática y las libertades.³⁹

- En Grecia, la Autoridad de Protección de Datos Helénica (*Hellenic Personal Data Protection Authority*). Esta Autoridad se crea, conforme a la Ley de protección de datos griega, con el objeto de vigilar la aplicación de la misma y que los tratamientos de datos personales no lesionan los derechos de las personas. Destaca la precisión y la amplitud con la que se han desarrollado las funciones y obligaciones de esta Autoridad, a la que se reconocen entre otros poderes, potestad normativa, inspectora y sancionadora. Cuenta con el apoyo de una Secretaría formada por un número no superior de treinta funcionarios.⁴⁰

- En Hungría, el Comisionado para la Protección de Datos (*Data Protection Commissioner*). La Ley de protección de datos húngara, con la finalidad de garantizar el derecho constitucional a la protección de datos personales y el acceso a los datos personales de interés público, crea un Comisionado para la Protección de Datos. De la labor de este Comisionado destaca la forma de imponer las sanciones, ya que si el Comisionado observa un tratamiento de datos ilegal, requerirá al “director” del mismo que ponga fin al mismo, y si éste no atendiera a tal petición, en un plazo de treinta días, el Comisionado anunciará públicamente la ilegalidad, la identidad del director del tratamiento y la categoría de los datos tratados. En este sistema, como en Irlanda y el Reino Unido, se le da una gran importancia al Registro y así todos los tratamientos de datos personales deben ser inscritos en el Registro de Protección de Datos (*Data Protection Register*) tras haber pasado por un previo control del Comisionado.⁴¹

- En Irlanda, el Comisionado de Protección de Datos (*Data Protection Commissioner*). Este Comisionado es nombrado por el Gobierno para un periodo de cinco años, es un órgano independiente y dotado de personalidad jurídica propia que

³⁸ La figura del corresponsal se regula en el art. 22 Ley francesa.

³⁹ Sobre el objeto de la CNIL, vid. FLAHERTY, D.H., *Protecting privacy in...*, op. cit., pp. 177-178, quien considera que la verdadera misión de la CNIL es complementar el desarrollo tecnológico con la evolución de la sociedad. En este sentido, se la ha tomado como referente en muchos Estados miembros, incluida España. Así, por ejemplo, en Portugal, el Tribunal Constitucional ha reconocido tomarla como ejemplo para “*rodear de mecanismos de garantía el tratamiento de datos personales*”. Vid. Acuerdo nº 355/97, de 7 de mayo. Vid., también, GOMES CANOTILHO J.J. / VITAL MOREIRA, *Constituição da República Portuguesa*. Anotada, 3ª ed., Coimbra Editora, Coimbra, 1993, p. 218.

⁴⁰ Sobre esta Autoridad, vid. arts. 15-23 Ley griega.

tiene como principal función velar por la aplicación de la Ley de protección de datos. El sistema de protección de datos irlandés es eminentemente registral, la inscripción de los registros tiene un valor constitutivo y es obligatoria para los ficheros del sector público y determinados ficheros del sector privado, como los de las instituciones financieras, de compañías de seguros, de empresas de venta por correo, de agencias de información sobre solvencia patrimonial y crediticias o los que traten datos especialmente protegidos.⁴²

- En Italia, el Garante para la protección de los datos personales (*Garante per la protezione dei dati personali*). Se trata de un órgano colegiado autónomo e independiente. Tiene un amplio número de competencias, entre las que destacan la de recibir las quejas y reclamaciones de los afectados, la de denunciar ante los Tribunales los hechos que tengan carácter delictivo, proponer al Gobierno las normas sobre protección de datos y elaborar un informe anual que eleva al Parlamento y al Gobierno. En su organización cuenta con el apoyo de una Oficina (*Ufficio del Garante*) que no puede superar los cuarenta y cinco funcionarios. Sus recursos dependen de una partida de los presupuestos del Estado, en función de las previsiones del Ministerio de Economía, y está, en este sentido, sujeto al control del Tribunal de Cuentas.⁴³

- En Letonia, la Inspección Estatal de Datos (*State Data Inspection*). La Ley sobre protección de datos personales de Letonia establece la posibilidad de que los ciudadanos que consideren que se ha lesionado su derecho a la protección de datos puedan acudir a la Inspección Estatal de Datos, encargada, entre otras cosas, del registro obligatorio de los tratamientos de datos personales. Esta Inspección, bajo el mando de un Director, se define como una institución de la Administración del Estado bajo la jurisdicción del Ministerio de Justicia que actúa de forma independiente.⁴⁴

- En Lituania, la Autoridad Estatal de Supervisión de Datos (*State Data Protection Inspectorate*). Conforme a la Ley de protección de datos lituana, el control de la aplicación corresponde a la Autoridad de Supervisión, institución estatal financiada con los Presupuestos del Estado y cuya regulación se deja también en manos del Gobierno. Entre sus funciones destaca la función de asesoramiento, la de examinar

⁴¹ Arts. 23-31A Ley húngara.

⁴² Sobre este Comisionado, vid. arts. 9-26 Ley irlandesa; y sobre el Registro, vid. arts. 16-20 de la misma Ley.

⁴³ Arts. 153-160 Decreto italiano.

las demandas y quejas impuestas ante las violaciones de la Ley de protección de datos y la de conceder las autorizaciones para transmitir datos a terceros países, pero no tiene atribuida potestad sancionadora al respecto.⁴⁵

- En Luxemburgo, la Comisión nacional para la protección de datos (*Commission nationale pour la protection des données*). Esta Comisión es la encargada de controlar y verificar si los datos sometidos a tratamientos son conformes con los principios y disposiciones de la normativa sobre protección de datos. Junto a la *Commission nationale pour la protection des données* se ha creado una autoridad específica vinculada al Ministerio Fiscal, encargada de controlar la aplicación de la protección de datos personales en el ámbito de las operaciones relativas a la seguridad pública, defensa, seguridad del Estado y prevención, detección y persecución de delitos criminales.⁴⁶ Y también, junto a esta Comisión, se crea la figura del “encargado de la protección de datos” (“*chargé de la protection de données*”). Hay que señalar, que este “encargado de la protección de datos” nada tiene que ver con la figura del “encargado” prevista en las Directivas comunitarias y en la propia Ley luxemburguesa (“*sous-traitant*”), que se encarga de tratar los datos personales por orden del responsable del tratamiento.⁴⁷

- En Malta, el Comisionado para la Protección de Datos (*Data Protection Commissioner*). La Ley de protección de datos personales de Malta exige que exista un Comisionado encargado de la protección de los datos personales, designado por el Primer Ministro tras consulta con el líder de la oposición. Junto al Comisionado se ha creado, del mismo modo que en el Reino Unido, un Tribunal (*Data Protection Appeals Tribunal*) encargado de conocer de aquellos asuntos que se le presenten en relación con

⁴⁴ Arts. 20 y 29-31 Ley letona.

⁴⁵ Sobre esta Autoridad, vid. arts. 29-32 Ley lituana.

⁴⁶ *Séptimo Informe Anual sobre la situación de la protección de las personas en lo que respecta al tratamiento de los datos personales y a la protección de la vida privada en la Unión Europea y en terceros países, relativo a los años 2002 y 2003*, adoptado el 21 de junio de 2004, p. 13.

⁴⁷ La Comisión se regula en los arts. 32-38 Ley luxemburguesa, y la figura del “encargado de la protección de datos” en el art. 12.3 de la misma Ley, al excluir de la obligación de notificar el tratamiento de datos a la Autoridad de control en aquellos casos en los que se nombre a dicho “encargado”: “*Est exempté de l’obligation de notification: a) le responsable du traitement qui désigne un chargé de la protection des données tenu notamment d’assurer, de manière indépendante, l’application des dispositions légales en la matière et d’établir et de continuer à la Commission nationale un registre des traitements effectués par le responsable du traitement conformément aux dispositions relatives à la publicité des traitements telles que prévues à l’article 15; (...)*”. En cambio, el “encargado” (“*sous-traitant*”) se define en el art. 2.p) Ley luxemburguesa como: “*la personne physique ou morale, l’autorité publique, le service ou tout autre organisme qui traite des données pour le compte du responsable du traitement*”.

las decisiones que hubiera tomado el Comisionado.⁴⁸ Además del Comisionado y del Tribunal, encontramos un “representante de los datos personales” (“*personal data representative*”), que no debemos confundir con el “encargado” que actúa por orden del responsable del tratamiento de datos personales, y que se encarga de controlar de forma independiente la legitimidad de los tratamientos de datos personales y de llevar un registro de los mismos.⁴⁹

- En los Países Bajos, la Comisión para la Protección de datos Personales (*College bescherming persoonsgegevens, CBP, o Data Protection Commission*). En el Capítulo dedicado a la supervisión, la Ley de protección de datos holandesa exige la creación de una Comisión independiente con el fin de controlar el procesamiento de datos personales en los Países Bajos. Esta Autoridad de control se ha creado con el fin de vigilar que los tratamientos de datos personales se realicen conforme a la Ley de protección de datos holandesa. La Comisión cuenta con el apoyo de una Secretaría compuesta por funcionarios públicos. Es de destacar que junto a la Comisión, existe la posibilidad de crear una asociación de responsables de los tratamientos de datos personales, y que, sin perjuicio de las competencias de la Comisión, tanto el “responsable del tratamiento” como la mencionada organización a la que estén afiliados los responsables pueden designar un “Oficial de protección de datos” (*Data protection officer*), que posee un conocimiento adecuado a la materia y actúa de forma independiente, encargándose de fiscalizar los tratamientos de datos que se realicen, incluso los que realicen el responsable del tratamiento o los responsables afiliados a la organización que lo han designado.⁵⁰

- En Polonia, el Inspector General para la Protección de Datos Personales (*Inspector General for Personal Data Protection*). El Inspector es nombrado por la Asamblea de Polonia, con el consentimiento del Senado, exigiéndose que la persona en cuestión sea un ciudadano polaco con residencia permanente en Polonia, conocido por “tener unos principios morales excelentes”, sin antecedentes penales y licenciado en

⁴⁸ Sobre los mismos, vid. arts. 36-53 Ley maltesa.

⁴⁹ El art. 2 Ley maltesa define al represante, diferenciándolo del “encargado” (“*processor*”), como: “*a person, appointed by the controller of personal data, who shall independently ensure that the personal is processed in a correct and lawful manner*”. Sobre el mismo, vid. también, arts. 30-35.

⁵⁰ Vid., arts. 51-64 ley holandesa; y, en concreto, sobre el Oficial de protección de datos (“*Data protection officer*”), arts. 62-64, del que se establece que “*A responsible party or an organisation to which responsible parties are affiliated may appoint its own data protection officer, without prejudice to responsibilities of the Commission under Chapter 9 and 10 of this Act*”.

Derecho con una experiencia profesional adecuada. Cuenta con el apoyo de una Oficina integrada por Inspectores (*Bureau of the Inspector General for Personal Data Protection*).⁵¹

- En Portugal, la Comisión Nacional de Protección de Datos (*Comissão Nacional de Protecção de Dados, CNPD*). Es una entidad administrativa independiente cuya misión principal es controlar y fiscalizar el cumplimiento de la legislación en materia de protección de datos, para lo cual dispone de potestades de investigación, asesoramiento, procesal y de sanción. Sólo se encuentra sometida al imperio de la Ley, y se somete a sus miembros a un estricto régimen de incompatibilidades.⁵²

- En el Reino Unido, el Comisionado de Información (*Information Commissioner*) y el Tribunal de Información (*Information Tribunal*). La antigua Ley de protección de datos inglesa de 1984 establecía la existencia de un Registrador de la Protección de Datos (*Data Protection Registrar*) y un Tribunal de Protección de Datos (*Data Protection Tribunal*). Con la aprobación de la nueva Ley de protección de datos de 1998, así como con la aprobación de la Ley de Libertad de Información del 2000 (*Freedom of Information Act, FOIA*),⁵³ el Registrador y el Tribunal de Datos pasaron a ser, respectivamente, el Comisionado y el Tribunal de Información.⁵⁴ El Comisionado es un oficial independiente nombrado por la Reina y encargado de controlar, por un lado, la aplicación de la legislación sobre protección de datos personales y, por otro lado, la relativa a la libertad de información prevista en la FOIA, en la que se regula el acceso a los datos personales que obran en manos de los poderes públicos. Su obligación principal es promover las buenas prácticas entre los responsables de los tratamientos de datos personales y controlar el cumplimiento de la legislación sobre protección de datos.⁵⁵ Junto al Comisionado, existe un Tribunal “especial”, el Tribunal

⁵¹ Vid., arts. 8 a 22 Ley polaca.

⁵² Sobre la CNPD, vid. arts. 21-31 Ley portuguesa.

⁵³ Esta Ley ofrece el derecho general de acceso a todo tipo de información “grabada” por las autoridades públicas.

⁵⁴ Vid., art. 6 y Schedules 5 y 6 Ley inglesa. Vid. también sobre el procedimiento seguido por el mismo, arts. 40-54. Vid. JAY, R. / HAMILTON, A., *Data protection. Law and practice*, 2ª ed., Sweet & Maxwell, London, 2003, p. 518. Y sobre la figura y funciones del “Registrar”, vid. SAVAGE, N. / EDWARDS, CH., *A guide to the data protection Act*, 2ª ed., Blackstone, London, 1985, pp. 47-105.

⁵⁵ Art. 51.(1) y Schedule 5 Ley inglesa. Vid. JAY, R. / HAMILTON, A., *Data protection. Law...*, op. cit., p. 530.

de Información, compuesto por un número indeterminado de miembros.⁵⁶ Las reglas por las que se rige el funcionamiento de este Tribunal, que estaban previstas en la Ley de protección de datos inglesa, se han modificado para introducir los cambios técnicos necesarios para que este Tribunal pueda ocuparse también de los recursos presentados contra la FOIA, que entró en vigor en enero de 2005.⁵⁷

- En la República Checa, la Oficina de Protección de Datos (*Office for Personal Data Protection*). La Ley de protección de datos checa crea la Oficina de protección de Datos con la finalidad de controlar el cumplimiento de la legislación sobre protección de datos. Es una autoridad independiente sometida tan solo al imperio de la Ley. Entre sus funciones destaca la de atender las peticiones y quejas hechas por los ciudadanos y la de conceder las autorizaciones previstas en la Ley. Está compuesta por un Presidente, los inspectores y los empleados de la misma.⁵⁸

- En Suecia, la Inspección de Datos Sueca (*Datainspektionen*, o *SwData Inspection Board*). La regulación de la Autoridad nacional de protección de datos en la Ley sueca es un tanto ambigua y confusa, pues ésta se refiere indistintamente a la “Autoridad designada por el Gobierno”, encargada de autorizar ciertos tratamientos de datos y de informar sobre los mismos o sobre las excepciones a los mismos, y a la “Autoridad de supervisión”, encargada de decidir sobre las medidas de seguridad que debe implantar el responsable del tratamiento, de recibir las notificaciones de los tratamientos que se vayan a realizar y de tomar las decisiones procedentes sobre los tratamientos de datos que se le planteen.⁵⁹ No obstante, a pesar la diferente terminología empleada en la Ley, existe una única Autoridad de protección de datos, la Inspección de Datos (*Data Inspection Board*) compuesta por unos cuarenta empleados, abogados en su mayoría, distribuidos en diferentes unidades administrativas bajo el mando de un Comité ejecutivo formado por un Director General y por ocho miembros designados por

⁵⁶ Entre este número indeterminado de miembros tienen que existir: un Presidente, designado por el Ministro de Justicia; tantos Vicepresidentes como determine el mismo Ministro de Justicia; y tantos miembros como designe el Gobierno. Vid. Schedule 5, art. 12 Ley inglesa.

⁵⁷ JAY, R. / HAMILTON, A., *Data protection. Law...*, op. cit., p. 534.

⁵⁸ Sobre esta Oficina, vid. arts. 28-43 Ley checa.

⁵⁹ Así, por ejemplo, podemos ver como en un mismo art. se hace referencia a lo que parecen dos tipos de “autoridades”. El art. 35 relativo a las excepciones a la prohibición de transferir datos a terceros países mantiene: “(...) Furthermore, the Government or the authority appointed by the Government issue regulations about exemptions from the prohibition in Section 33, if this is necessary having regard to an important public interest or if there are adequate safeguards to protect the rights of the registered person. The Government may, subject to the preconditions mentioned in the second paragraph, decide in

el Gobierno, de ahí que se la considere una “agencia central del Gobierno” (“*central government agency*”). Junto a la Inspección de Datos, la Ley sueca de protección de datos personales crea también un “representante de los datos personales” (“*personal data representative*”), nombrado por el responsable del tratamiento de datos y encargado de asegurar de forma independiente que el responsable del tratamiento de datos realiza un tratamiento de datos personales conforme a los principios establecidos en la legislación sobre la materia.⁶⁰

1. Organización

En la mayoría de las Leyes de creación de las Autoridades nacionales de protección de datos se las ha calificado de organismos o entes “independientes”, como exige la Directiva 95/46/CE sobre Protección de Datos Personales. En unos casos estas Autoridades se crean con personalidad jurídica propia y separada de la Administración, con las características que definen en cada ordenamiento jurídico a las “autoridades independientes”; en otros casos, se crean sin personalidad jurídica propia, es decir, integradas en la Administración Pública, pero con un régimen jurídico especial que asegura que pueden actuar con independencia.⁶¹ La autonomía funcional de estas autoridades se garantiza asegurándolas que actuarán libres de las órdenes e instrucciones y del sistema de controles que caracteriza a la Administración jerarquizada.⁶²

individual cases on an exemption from the prohibition in Section 33. The Government may delegate power to the supervisory authority to make such decisions”.

⁶⁰ El art. 3 define esta figura del “representante” junto a la del responsable (“*controller of personal data*”) y a la del “encargado” (“*personal data assitant*”) y lo define como: “*a natural person, appointed by the controler of personal data, who shall independently assure that the personal data is processed in a correct and lawful manner*”. Sobre dicha figura, vid. también, arts. 37-40 Ley sueca.

⁶¹ Sobre estas autoridades, vid., por ejemplo, BETANCOR RODRÍGUEZ, A., *Las Administraciones independientes*:...op. cit.; y SALVADOR MARTÍNEZ, M., *Autoridades independientes*, op. cit.. Así, por ejemplo, en Eslovaquia y Letonia, se las ha calificado como órganos de la Administración estatal. Vid. art. 28 Directiva 95/46/CE sobre Protección de Datos Personales. El art. 33 de la Ley eslovaca dispone: “*The Personal Data Protection Office, which is a body or state administration with a state-wide competence and its seat in Bratislava, shall be established*”; y de la misma forma, el art. 29.(1) Ley letona establece: “*...The State Data Inspection shall be an institution of state administration, functions, rights and duties of which shall be established by the law...*”.

⁶² SALVADOR MARTÍNEZ, M., *Autoridades independientes*, op. cit., p. 360. Por ejemplo, en Alemania, aunque la Ley de protección de datos establezca que el Comisionado Federal es un órgano independiente en el ejercicio de sus funciones, sometido tan sólo al imperio de la Ley, éste se encuadra en la organización del Ministerio del Interior y está sujeto a la supervisión jerárquica del mismo; y si el Comisionado alemán no pudiera temporalmente desempeñar sus funciones, es el Ministro del Interior el

En cuanto a la composición, la mayoría de las Autoridades nacionales de protección de datos se componen de órganos colegiados frente a las que se han creado como órganos unipersonales, en Alemania, Irlanda, Reino Unido y España.⁶³ Entre las que se componen de un órgano colegiado, existen diferencias en relación con el número de miembros que lo integran, que van desde los 17 de la CNIL a los 3 miembros de la Autoridad de protección de datos de los Países Bajos, pasando por 4 en Italia, 5 en Luxemburgo, y 6 en Austria y en Grecia.⁶⁴

La forma de elección de los miembros que componen estas Autoridades es lo que determina, en muy buena medida, el grado de independencia real del órgano. En la mayoría de los casos los miembros de las Autoridades nacionales de protección de datos personales son designadas a través de un procedimiento especial en el que interviene el Parlamento, aunque en algunos casos son designadas por el Gobierno, como en España,⁶⁵ Irlanda, Luxemburgo y el Reino Unido, o por un miembro del Gobierno, el Ministro de Justicia, como ocurre en Dinamarca y en los Países Bajos. En Francia, la CNIL se compone de miembros designados por las dos cámaras del Parlamento y por miembros que son elegidos por otras autoridades, incluso por el Gobierno; y en Portugal la mayoría de los miembros son designados por el Parlamento, aunque dos de sus

encargado de designar a su sustituto, por lo que en la práctica la “independencia” es cuestionable (art. 22.(4) a (6) Ley alemana).

⁶³ Sobre la estructura de la AEPD varios autores han lamentado que ésta no adoptara la forma colegiada ofreciendo mayor peso al Consejo Consultivo como órgano de decisión (y de control, en última instancia) frente al Director, con lo que se hubiera evitado que una sola persona acumulara todo el poder y se hubiera garantizado la independencia y el pluralismo de esta institución. Vid. entre estos autores, FERNÁNDEZ-SAMANIEGO, J. “La nueva Ley de protección de datos de carácter personal española”, en *REDI*, nº 24, 2000, p. 4; VIZCAÍNO CALDERÓN, M., *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Madrid, 2001, p. 397; y HERRÁN ORTÍZ, A.I., *El derecho a la intimidad...*, op. cit., pp. 334-335; y de la misma autora, *La violación de...*, op. cit., p. 349-350.

⁶⁴ TÉLLEZ AGUILERA, A., *La protección de...*, op. cit., pp. 339-340.

⁶⁵ Entre las numerosas críticas recibidas por este motivo, vid. GARRIGA DOMÍNGUEZ, A., *Tratamiento de datos...*, op. cit., pp. 186-187 y 192-194; FREIXAS GUTIÉRREZ, G. *La protección de los datos de carácter personal en el derecho español. Aspectos teóricos y prácticos*, Bosch, Barcelona, 2001, pp. 288-289; HERRÁN ORTÍZ, A.I., *La violación de la intimidad en la protección de datos personales*, Dykinson, Madrid, 1999, pp. 344 y 346; SÁNCHEZ BRAVO, A.A., *La protección del...*, op. cit., p. 116; DAVARA RODRÍGUEZ, M.A., “La Ley española de protección de datos (LORTAD): ¿una limitación del uso de la informática para garantizar la intimidad?”, en *AJA*, nº 76/77, 1992, p. 3; MARTÍNEZ MARTÍNEZ, R. “El control de...” op. cit., pp. 82-83; y PÉREZ LUÑO, A.E., “Comentario legislativo: la LORTAD y los derechos fundamentales”, en *DL*, nº 1, 1993, pp. 413-414, que califica a la AEPD de “mero delegado gubernativo para la informática”. Por el contrario, opina HEREDERO HIGUERAS, a nuestro entender de una forma desafortunada, que el hecho de que la designación del Director se haga por el Gobierno es irrelevante desde el punto de vista de su independencia, pues la designación parlamentaria, en sí misma, también “puede acarrear un riesgo de politización, en la medida en que la elección de su titular o titulares pueda estar mediatizada por la correlación de las fuerzas políticas”. Vid. HEREDERO HIGUERAS, M., “La Agencia de...” op. cit., p. 326; y DE LA SERNA BILBAO, M.N., “La Agencia de Protección de Datos española: con especial referencia a su característica de independiente”, en *AIA*, nº 22, 1997, p. 14.

miembros son designados por el Gobierno.⁶⁶ Destaca el caso de Alemania, donde el Comisionado federal y las Autoridades nombradas por los *Länder* para controlar los tratamientos de datos efectuados en el sector público son designados por los respectivos Parlamentos, mientras que las Autoridades encargadas de controlar los ficheros privados son, en muchos de los *Länder*, parte del Gobierno local o del Ministerio.⁶⁷

Los miembros de estas Autoridades son elegidos por un periodo de tiempo que no en todos los Estados miembros es el mismo: 4 años en Dinamarca, Grecia, Italia y España; 5 años en Alemania, Austria, Francia, Irlanda Portugal y Reino Unido; y 6 años en Bélgica, Holanda y Luxemburgo. Por regla general se intenta que el mandato de los miembros de estas Autoridades nacionales de protección de datos personales no coincida con el periodo de legislatura o con el mandato del Presidente. Además, en algunos casos se prohíbe la reelección, como en Portugal, y, en otros sólo se permite una vez, como en Alemania, Grecia e Italia, o por un máximo de 15 años, como en el Reino Unido.⁶⁸

Una de las razones que justifican la creación de las Autoridades de protección de datos es la especialización técnica de las mismas, lo cual se debe reflejar en la “preparación técnica” de sus miembros. Pues bien, existen muchas diferencias entre los Estados en lo que al grado de cualificación de los miembros de dichas Autoridades se refiere. Así, en algunos países no se exige ninguna cualificación profesional para ser elegido miembro de la Autoridad de Control, como es el caso del Comisionado alemán, del finlandés, del irlandés, del británico, de los miembros de la CNIL o del Director de la AEPD; por el contrario, en otros países sí se exige que al menos el Presidente pertenezca a la carrera judicial, como es el caso por ejemplo de la Agencia danesa, la griega o la holandesa; y, por último, en otros países se exige una alta cualificación, como, por ejemplo, en Bélgica, donde se exige la presencia de al menos un jurista, un informático y dos profesionales de protección de datos; en Grecia, donde los miembros de la Autoridad (además del Presidente) deben ser un Magistrado, un profesor universitario de Derecho, otro de Informática y tres profesionales con experiencia en la

⁶⁶ KORFF, D., *EC study on...*, op. cit., p. 203.

⁶⁷ Hay que señalar que muchos de los *Länder* han modificado sus Leyes para que sea la Autoridad de control del *Land* la que se encargue también del sector privado. Vid., sobre esta cuestión, KORFF, D., *EC study on...*, op. cit., pp. 203-204.

⁶⁸ TÉLLEZ AGUILERA, A., *La protección de...*, op. cit., p. 340; y KORFF, D., *EC study on...*, op. cit., p. 204.

materia; o, en Portugal, donde de los cinco miembros, dos han de ser magistrados y dos especialistas en protección de datos.⁶⁹

La independencia de estas Autoridades no sólo deriva de su organización, sino también de su forma de financiación. En la mayoría de los casos, los recursos de estas Autoridades nacionales de protección de datos proceden de una determinada partida de los Presupuestos Generales, pero en algunos casos su presupuesto depende del Ministerio al que estén adscritas, que suele ser el de Justicia o Interior. Además, en muchos casos, tienen también recursos propios derivados de los ingresos por los pagos de las tasas por el desempeño de sus actividades, como es el caso de la CNIL.⁷⁰ Y la mayoría de ellas están obligadas a informar al Tribunal de Cuentas y al Parlamento de esa gestión económica. En cualquier caso, independientemente del modelo de Autoridad elegido, la mayoría de ellas consideran que los recursos de los que disponen son insuficientes para llevar a cabo sus funciones, que son muchas más que las previstas en la Directiva 95/46/CE sobre Protección de Datos Personales, lo cual afecta directamente a su independencia.⁷¹

Hay que señalar finalmente que muchas de estas Autoridades conviven con otros órganos encargados también de garantizar el cumplimiento de la legislación sobre protección de datos y cuyos nombramientos siempre se basan en su especialización técnica. Así, por ejemplo, encontramos el “Oficial de la protección de datos” (“*Beauftragter für den Datenschutz*”) en Alemania; el “Encargado de la protección de datos” (“*chargé de la protection de données*”) en Luxemburgo; el “Oficial de protección de datos” (“*data protection officer*”) holandés; el “representante de datos personales” (“*personal data representative*”) en Suecia; y el “representante de datos personales” (“*personal data representative*”) en Malta.⁷²

⁶⁹ TÉLLEZ AGUILERA, A., *La protección de...*, op. cit., p. 340.

⁷⁰ Sobre la financiación de la CNIL, vid. FLAHERTY, D.H., *Protecting privacy in...*, op. cit., p. 183; y GARCÍA-BERRIO, T., *Informática y libertades...*, op. cit., p. 362.

⁷¹ *Primer Informe de la Comisión relativo a la aplicación de la Directiva sobre Protección de Datos 95/46/CE*, de 15 de mayo de 2003 (COM (2003) 265 final), pp. 38-39. Así, en Alemania, aunque sus recursos cuentan con una “partida” independiente en el Presupuesto del Ministerio del Interior, es este último el que decide sobre la admisión o no de cualquier ingreso que reciba el Comisionado. Vid. Arts. 22.(5) y 23.(3) Ley alemana.

2. *Funciones y competencias*

Todas las Autoridades nacionales de protección de datos tienen atribuidas la labor de supervisar la actividad de aquellos sujetos públicos y/o privados que realizan tratamientos de datos y controlar el cumplimiento de las normas de protección de datos personales, garantizando así los derechos de los titulares de los datos.⁷³ Para cumplir con su función a las Autoridades nacionales se les han atribuido las competencias necesarias.⁷⁴

2.1. Competencias

Las competencias que los Estados miembros han atribuido a las Autoridades de protección de datos son un reflejo de las establecidas en las Directivas de Protección de Datos, es decir, poderes de investigación, poderes de intervención y capacidad procesal, entre otras.⁷⁵

a) Competencias de control, supervisión e inspección. Respecto de los poderes de investigación sobre los ficheros y los tratamientos de datos realizados, la mayoría de las Leyes de protección de datos reconocen amplias facultades a sus Autoridades de protección de datos, aunque en la práctica muy pocas la ejercen efectivamente. Así, por ejemplo, en la mayoría de los países las “auditorías de datos” son poco frecuentes. En los Países Bajos, la Autoridad de control está comenzando a practicar “auditorías privadas” a un determinado grupo de usuarios; y en el Reino Unido, la Autoridad de control no puede realizar tal tipo de auditorías sin el acuerdo del responsable del tratamiento y tiene condicionado el acceso a los datos de las empresas al

⁷² TÉLLEZ AGUILERA, A., *La protección de...*, op. cit., p. 341.

⁷³ Se considera que estas Autoridades deben llevar a cabo ciertas funciones, entre las que destacan: la vigilancia de la aplicación de la normativa comunitaria; la contestación de demandas y solicitudes que se le presenten con motivo de cualquier actuación relacionada con un tratamiento de datos personales, como, por ejemplo, la solicitud de verificación de la licitud de un tratamiento de datos personales; la presentación de un Informe sobre sus actividades; el recibimiento de las notificaciones de los tratamientos de datos que se vayan a efectuar y, en relación con esta función, un control previo de dichos tratamientos en el caso de que pudieran suponer algún riesgo específico para los derechos y libertades de los interesados. Vid. Considerando 53 y arts. 18, 20.2 y 21.2 Directiva 95/46/CE sobre Protección de Datos Personales.

⁷⁴ Vid. Art. 28.3 Directiva 95/46/CE sobre Protección de Datos Personales. Sobre estos poderes, vid. WEICHERT, TH., “Teil 13: Datenschutz. Vor 134. Grundrechtsschutz durch Verfahren”, en W. KILLIAN / B. HEUSSEN, *Computerrechts Handbuch*, Verlag C.H. Beck, München, März, 2002, p. 2; ROSSNAGEL, A. (ed.), *Handbuch Datenschutzrecht*, Verlag C.H. Beck, München, 2003, pp. 144-145; HERRÁN ORTÍZ, A.I., *El derecho a la intimidad...*, op. cit., p. 188.

⁷⁵ Vid. art. 28 Directiva 95/46/CE sobre Protección de Datos Personales.

expreso permiso de las mismas o bajo la constitución de una garantía.⁷⁶ Las facultades de inspección muchas veces se ejercen a instancia de los ciudadanos que presentan quejas o reclamaciones ante las Autoridades. En este sentido, mientras que algunas Autoridades consideran que el recibimiento de la queja no supone abrir un expediente administrativo sino que se puede resolver mediante una resolución de la Autoridad de control; para otras Autoridades ese es el camino más frecuente para iniciar las inspecciones.

b) Competencias en relación con la adopción de decisiones. La mayoría de las Autoridades pueden “intervenir” los tratamientos de datos efectuados, ordenar el bloqueo y la cancelación de los datos, y prohibir de forma definitiva o temporal dicho tratamiento; las Autoridades nacionales de Alemania, Bélgica, Francia, Italia o Suecia, sin embargo, no tienen tal capacidad. Además, la mayoría de las Autoridades nacionales otorgan “autorizaciones” a los responsables de los tratamientos para que puedan realizar el tratamiento de datos personales. Así, por ejemplo, en Francia, antes del tratamiento de datos se debe producir una declaración previa y conforme de la CNIL, y para el tratamiento de datos relativos a la salud o a datos genéticos y biométricos, así como para los tratamientos en los que conste el número de identificación personal, se requerirá la autorización de la misma; en Suecia, los tratamientos de datos relacionados con operaciones de crédito requieren un previo permiso de su Inspección; y en Malta, la investigación de los tratamientos de datos que se realicen por motivos de seguridad nacional, defensa, seguridad pública, prevención de delitos o materias económicas y financieras requieren la autorización por escrito de su Comisionado.⁷⁷

c) Competencias normativas. Muchas de las Autoridades de protección de datos de los Estados miembros tienen potestad normativa y pueden dictar Instrucciones o Circulares que ayuden a una aplicación uniforme de la Ley de protección de datos de

⁷⁶ En este sentido, vid. también, KORFF, D., *EC study on...*, op. cit., p. 206; y ROSSNAGEL, A., *Handbuch Datenschutzrecht*, op. cit., p. 145.

⁷⁷ Vid., por ejemplo, de entre los casos mencionados, el art. 25 de la Ley francesa dispone: “1. *Sont mis en oeuvre après autorisation de la Commission nationale de l’informatique et des libertés, à l’exclusion de ceux qui sont mentionnés aux articles 26 et 27: (...) 2°. Les traitements automatiques portant sur des données génétiques, à l’exception de ceux d’entre eux qui sont mis en oeuvre par des médecins ou des biologistes et qui sont nécessaires aux fins de la médecine préventive, des diagnostics médicaux ou de l’administration de soins ou de traitements. (...)*”; y el art. 41.3 de la Ley maltesa: “*The investigations on the data processing described in article 23 are subject to the written authorisation of the Commissioner*”.

que se trate, como es el caso de la Autoridad española, de la griega, de la chipriota, de la polaca o de la eslovaca.⁷⁸

d) Competencias de asesoramiento. Puesto que se trata de Autoridades especializadas en la materia tienen también competencias asesoras que ejercen informando a los titulares de sus derechos, informando a los poderes públicos cuando lo necesitan y publicando una Memoria o Informe sobre sus actividades. En este último supuesto puede señalarse que mientras la mayoría de las Autoridades deben elaborar un Informe sobre sus actividades de forma anual, en el caso de Alemania o de Austria dicho Informe se elabora de forma bianual, cada dos años. Destaca en este punto la Autoridad de protección de datos del Reino Unido, que a través de un sistema de “notificaciones” o avisos ha desarrollado un sistema de asesoramiento al ciudadano que se diferencia del resto de sistemas de los demás Estados miembros.⁷⁹

e) Potestad sancionadora. Hay que decir que estas Autoridades, tal y como se ha reconocido en el caso de la CNIL francesa, más que funciones de “policía” desarrollan funciones “conciliadoras”, ofreciendo soluciones ante las posibles lesiones de los derechos de los ciudadanos.⁸⁰ La regla general es que las Autoridades de control buscan una solución “amistosa” de la lesión producida y ante la imposibilidad de llegar a esa solución es cuando se produce la sanción administrativa y, cuando proceda, en última instancia o en caso extremo, la penal. Destaca aquí el caso de Alemania, por ser el único país en que, a pesar de que las medidas no son excesivamente severas, los “avisos” ante los incumplimientos en los tratamientos de datos personales se tienen en cuenta por los infractores.⁸¹

⁷⁸ Vid. art. 37.1.c) LOPD; y, también, por ejemplo, entre las competencias de la Autoridad polaca, el art. 12 de la Ley polaca se refiere a “*issuing administrative decisions*”.

⁷⁹ Sobre los tipos de notificaciones efectuadas y la posibilidad de acudir también a un Tribunal especializado, vid. arts. 40-54 Ley inglesa.

⁸⁰ Sobre esta cuestión, vid. BRAIBANT, G. *Données personnelles et...*, op. cit., pp. 132-134; y FLAHERTY, D.H., *Protecting privacy in...*, op. cit., pp. 186-191 y 200-205.

⁸¹ En este sentido, vid., KORFF, D., *EC study on...*, op. cit., pp. 206-209; BRAIBANT, G., *Données personnelles et...*, op. cit., p. 129; y TRONCOSO REIGADA, A., “La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional”, en *Cuadernos de Derecho Público*, nº 19-20, 2003, pp. 314-315 (nota 192), que sostiene: “La Autoridad alemana, además de estar encuadrada en el Ministerio del Interior, no desarrolla una labor real de inspección. La Autoridad italiana elige los temas que investiga y sólo lleva a cabo inspecciones puntuales. La Autoridad francesa hace básicamente deliberaciones, pero tampoco lleva a cabo inspecciones realmente. La Agencia de Gran Bretaña tiene que pedir permiso para hacer una inspección al responsable del fichero. La Agencia irlandesa ha hecho una sola inspección en los últimos cinco años. Sólo Portugal y Grecia atribuyen poderes reales de inspección en materia de protección de datos”.

En relación con el ejercicio de esta potestad sancionadora existen relevantes diferencias entre las Autoridades nacionales de protección de datos de unos países y otros. En primer lugar, existen Autoridades nacionales de protección de datos, la mayoría de ellas, que persiguen y castigan la infracción que se produzca en relación con el tratamiento de datos personales sin necesidad de acudir a los Tribunales (a excepción, claro está, de los delitos penales, sometidos a la jurisdicción penal), es decir, que aplican directamente las sanciones legalmente previstas, como las la AEPD y las Autoridades de Grecia, Países Bajos, Italia, Luxemburgo, Portugal, y la República Checa. En segundo lugar, existen Autoridades de control que tienen capacidad para investigar, pero no tienen capacidad para imponer sanciones, debiendo denunciar la infracción producida ante las autoridades judiciales competentes, pudiendo incluso ser parte en el proceso, como ocurre con las Autoridades de Alemania, Austria, Bélgica, Dinamarca, Suecia, Polonia y Lituania.⁸² Destaca el caso de Finlandia, donde el Comisionado sólo tiene potestad para imponer amenazas de multa; y el caso de Hungría donde existen las “penas infamantes” consistentes en la publicación de la ilegalidad cometida una vez verificada.⁸³

f) Otras competencias. Entre otras competencias destacan las relativas a la cooperación que desarrollan las Autoridades de protección de datos nacionales entre sí, y la función de llevanza de los Registros de ficheros y tratamientos de datos personales. En relación con la función de cooperación hay que señalar que se prevé la posibilidad de que dichas Autoridades cooperen entre sí o con otros organismos cuando sea necesario para el cumplimiento de sus funciones mediante el intercambio de información que estimen útil. Esta cooperación se desarrolla a través de Conferencias o Encuentros de los que surgen Informes o Declaraciones que contribuyen a mejorar el nivel de protección de los datos personales. Así, por ejemplo, a nivel europeo, estas Autoridades se reúnen anualmente en las conocidas “Conferencias de Primavera de las Autoridades europeas de protección de datos”;⁸⁴ y a nivel internacional, las Autoridades

⁸² En este sentido, la potestad sancionadora se reconoce a las Autoridades de control o se residencia en los Tribunales administrativos o penales. Vid. TÉLLEZ AGUILERA, A., *La protección de...*, op. cit., pp. 341-342.

⁸³ Art. 25 Ley húngara.

⁸⁴ Vid., por ejemplo, Conferencia de 10-11 de mayo de 2001 en Atenas, en la que se elaboró la Declaración sobre el art. 8 de la Carta, señalando la satisfacción de las Autoridades de Control por el reconocimiento definitivo del carácter de derecho fundamental del derecho a la protección de datos personales; Conferencia de 25-26 de abril de 2002 en Bonn; Conferencia de 3-4 de abril de 2003 en Sevilla; y de 21-24 abril de 2004 en Rotterdam bajo el lema “La navegación de la intimidad”, en la que participó por primera vez el Supervisor Europeo de Protección de Datos y que se centró en las novedades

europas se reúnen con Autoridades Independientes de Control de todo el mundo, como, por ejemplo, con las de Australia, Canadá o Japón, una vez al año en las conocidas “Conferencias Internacionales de Autoridades de Protección de Datos”.⁸⁵ No podemos olvidar aquí el encuentro anual que se celebra entre la Agencia Española de Protección de Datos (AEPD) y el Comissão Nacional de Protecção de Dados (CNPD) de Portugal en el conocido “Encuentro Ibérico de Protección de Datos”.⁸⁶

2.2. Ámbito competencial

La mayoría de las Leyes de protección de datos de los Estados miembros se aplican a todos los ficheros de datos, independientemente de su titularidad pública o privada, aunque en los casos de Alemania y España las Leyes de protección de datos prevén un régimen jurídico diferente para los tratamientos de datos efectuados en el sector público y en el privado.

En relación con la distribución competencial en el caso de los Estados con una organización territorial descentralizada, la tarea de asegurar el cumplimiento de las normas de protección de datos personales se ha repartido entre una Autoridad nacional y Autoridades regionales. En Alemania los *Länder* han creado una Autoridad de protección de datos (*Landesdatenschutzbeauftragten*) con las mismas competencias que las del Comisionado Federal, pero sólo respecto de los tratamientos de datos que efectúen los poderes públicos del *Land* correspondiente.⁸⁷ Recordemos aquí que el Comisionado Federal para la Protección de datos se encarga sólo de los ficheros de los poderes públicos federales, y que del control del sector privado se ocupan los “Oficiales

surgidas en el marco del tercer pilar; y la de 24-26 de abril de 2005 en Krakovia sobre las perspectivas de la Directiva 95/46/CE sobre Protección de Datos Personales. Sobre estas Conferencias, vid. ROSSNAGEL (ed.), A., *Handbuch Datenschutzrecht*, op. cit., p. 781.

⁸⁵ Así, por ejemplo, la 20ª Conferencia Internacional que tuvo lugar el 16-18 de septiembre 1998 en España (Santiago de Compostela); la 22ª el 28-30 de septiembre de 2000 en Venecia (Italia), de la que surgió la Declaración de Venecia; la 26ª el 14-16 septiembre de 2004 en Wroclaw a la que asistió el Supervisor Europeo de Protección de Datos y cuyo tema fue “Derecho a la intimidad: derecho a la dignidad”; y la 27ª, que tendrá lugar el 14-16 de septiembre de 2005 en Montreux sobre “La protección de los datos personales y de la intimidad en un mundo globalizado: un derecho universal que respeta las diversidades”.

⁸⁶ De estos encuentros ha surgido, por ejemplo, en el IV Encuentro Ibérico, los días 6 y 7 de noviembre de 2003, la Declaración de Jarandilla de la Vera, en la que aborda la cuestión de la armonización en las normas a seguir para la notificación de los tratamientos de datos personales.

⁸⁷ Todos los *Länder* han aprobado sus Leyes de protección de datos. Sobre la distribución de competencias en esta materia entre la Federación (*Bund*) y los *Länder*, vid. arts. 70 y 80 GG, y ROSSNAGEL, A., *Handbuch Datenschutzrecht*, op. cit., pp.191-193.

para la protección de datos” (*Beauftragter für den Datenschutz*) que, de acuerdo con la Ley, deben designar las empresas u organismos que realicen tratamientos de datos personales, y las “Autoridades de Supervisión” (*Aufsichtsbehörde*), nombradas por los Gobiernos de los respectivos *Länder*.⁸⁸ En el Reino Unido, con el fin de mejorar su labor, el Comisionado de Información (*Information Commissioner*) está propiciando la creación de oficinas regionales en Irlanda del Norte, en Escocia y en Gales, y se ha designado un Asistente para cada Área. Las oficinas se ocupan, como el Comisionado, de las materias relacionadas tanto con la protección de datos como con la libertad de información.⁸⁹

Respecto del ámbito de actuación de la AEPD, de acuerdo con la LORTAD y con la LOPD, ésta ejerce las competencias que las mismas le otorgan, en primer lugar, en relación con los ficheros de datos creados o gestionados directamente por la Administración central del Estado y, en segundo lugar, en relación con todos los ficheros de titularidad privada. La diferencia fundamental entre la AEPD y las Agencias de protección de datos autonómicas reside en el diferente ámbito de actuación de una y otras. El ámbito de actuación de estos organismos autonómicos se encuentra restringido al territorio de la propia Comunidad Autónoma y a los ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local situada en el territorio de la Comunidad.⁹⁰ La LORTAD, y actualmente la LOPD, excluyen, en todo caso, la competencia de las Agencias autonómicas sobre los ficheros de titularidad privada, y es aquí, donde surgió el conflicto sobre la distribución de competencias entre la Agencia estatal y las autonómicas, llegándose a interponer por parte del Consejo Ejecutivo de la Generalidad y el Parlamento de Cataluña sendos recursos de inconstitucionalidad contra la

⁸⁸ Vid. art. 24.(6) Ley alemana. Sobre esta cuestión, vid., al detalle, ROSSNAGEL, A., *Handbuch Datenschutzrecht*, op. cit., pp. 745-801; y FREIXAS GUTIÉRREZ, G., *La protección de...*, op. cit., p. 286.

⁸⁹ La Schedule 5, art. 4 establece: “1. *The Commissioner: (a) shall appoint a deputy commissioner, and (b) may appoint such number of others officers and staff as he may determine. (...)*” y el art. 5: “1. *The deputy commissioner shall perform the functions conferred by this Act on the Commissioner during any vacancy in that office or at any time when the Commissioner is for any reason unable to act. 2 Without prejudice to sub-paragraph (1), any functions of the Commissioner under this Act may, to the extent authorised by him, be performed by any of his officers or staff*”.

⁹⁰ HERRÁN ORTÍZ, A.I., *El derecho a la intimidad...*, op. cit., p. 342. Crítico con la aplicación del ámbito territorial para la distribución de competencias entre la AEPD y las Agencias autonómicas, vid. CASTELLS ARTECHE, J.M., “Derecho a la privacidad y a procesos informáticos”, en *RVAP*, nº 39, 1994, p. 277, que considera que la “ruptura del ámbito territorial (...) revela una voluntad de control y supervisión central desprovista de suficiente cobertura normativa”. Sobre la distribución competencial en

LORTAD⁹¹ denunciando que esa distribución de competencias entre la AEPD y las Agencias Autonómicas de Protección de Datos, que otorgaba a la AEPD la ejecución en exclusiva de la LORTAD respecto de los ficheros de titularidad privada, lesionaba el reparto constitucional de competencias entre el Estado y las Comunidades Autónomas. El Tribunal Constitucional en la Sentencia 290/2000, que resuelve dichos recursos, entendió que debía ser la AEPD quien controle todos los ficheros privados, incluso los que radiquen en las Comunidades Autónomas, porque la creación de la AEPD responde no sólo al mandato constitucional del artículo 18.4 CE, sino a la garantía de un derecho fundamental, el derecho a la protección de datos personales y, porque es competencia del Estado, en base al artículo 149.1.1º CE, asegurar el respeto de los derechos fundamentales en todo el territorio nacional mediante el establecimiento de las condiciones básicas que hagan posible que el disfrute de tales derechos sea igual para todos los ciudadanos.⁹²

materia de protección de datos y sobre la STC 290/2000, vid. TRONCOSO REIGADA, A., “Las Comunidades Autónomas...”, op. cit., pp. 115-134 (pp. 122-131).

⁹¹ Aunque la LORTAD fue derogada durante el transcurso del recurso de inconstitucionalidad, el TC consideró que “*la regla general en este supuesto es que cuando la controversia competencial se ha planteado (...) y tal controversia pervive tras la derogación de la ley que ha suscitado el conflicto, es procedente que nos pronunciemos sobre el mismo*”. Vid. STC 290/2000.

⁹² Voces a favor y en contra de la decisión del Tribunal, vid. a favor, por ejemplo, HERRÁN ORTÍZ, A.I., *El derecho a la intimidad...*, op. cit., pp. 345-346 y LUCAS MURILLO DE LA CUEVA, P., *Informática y protección de datos personales*, CEC, Madrid, 1993, p. 159. Y, en contra, por ejemplo, RUÍZ CARRILLO, A., *Los datos de carácter personal. Concepto, requisitos de circulación, procedimientos y formularios*, Bosch, Barcelona, 1999, p. 58.