CELSO RODRÍGUEZ PADRÓN, SECRETARIO GENERAL DEL CONSEJO GENERAL DEL PODER JUDICIAL,

CERTIFICO: QUE EL PLENO DEL CONSEJO GENERAL DEL PODER JUDICIAL, EN SU REUNIÓN DEL DÍA DE LA FECHA, HA APROBADO EL INFORME A LA PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO RELATIVO A LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE SUS DATOS PERSONALES Y A LA LIBRE CIRCULACIÓN DE ESTOS DATOS.

I
ANTECEDENTES

Con fecha 14 de diciembre de 2012 ha tenido entrada mediante correo electrónico dirigido al Excmo. Sr. Secretario General del Consejo General del Poder Judicial (CGPJ), una carta fechada el 11 de diciembre de 2012, del Director General de Cooperación Jurídica Internacional y Relaciones con las Confesiones del Ministerio de Justicia, en la que se daba traslado a este Consejo General de la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos (en adelante la Propuesta), a los efectos de que se notifique por parte de aquél la normativa específica de su ámbito de actividad que pudiera verse afectada por la aprobación definitiva de ese Reglamento. Junto a la Propuesta, se remitía un documento en el que se expresa la Posición

oficial del Reino de España en relación con aquélla, fechado el 27 de noviembre de 2012.

La Comisión de Estudios e Informes, en su sesión de 18 de diciembre de 2012 y de conformidad con su Protocolo interno, acordó designar Ponente al Excmo. Sr. D. Carles Cruz Moratones, y en su reunión de fecha 21 de enero de 2013 aprobó el presente Informe, acordando su remisión al Pleno del Consejo General del Poder Judicial.

II
DESCRIPCIÓN DE LA PROPUESTA

La Propuesta se apoya tanto en el artículo 8 de la Carta de los Derechos Fundamentales de la UE, el cual consagra como derecho fundamental la protección de los datos de carácter personal, como en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea (TFUE), introducido por el Tratado de Lisboa, según el cual toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. Sobre estas bases pretende someter a revisión el actual marco normativo en materia de protección de datos, compuesto principalmente por la Directiva 95/46/CE, 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.

En 2010 el Consejo Europeo invitó a la Comisión a evaluar el funcionamiento de éste y otros instrumentos normativos complementarios y a presentar, en caso necesario, nuevas iniciativas. Ello sobre la base de constatar que la rápida evolución tecnológica ha supuesto nuevos retos para la protección de los datos personales,

incrementando la magnitud del intercambio y la recogida de datos. Las autoridades comunitarias han constatado la importancia de generar confianza en el entorno en línea para el desarrollo económico, pues en ausencia de esa confianza los consumidores vacilan a la hora de adquirir productos y servicios en línea, con el consiguiente riesgo de ralentización del uso de las nuevas tecnologías. La protección de datos personales desempeña, por tanto, una función esencial en la Agenda Digital para Europa y más concretamente en la Estrategia Europa 2020.

En su Comunicación «Un enfoque global de la protección de los datos personales en la Unión Europea» (2010), la Comisión señalaba que, si bien el marco jurídico actual sigue siendo adecuado por lo que respecta a sus objetivos y principios, no ha evitado la fragmentación en la aplicación en la UE de la protección de datos de carácter personal, la inseguridad jurídica y la percepción generalizada de que existen riesgos significativos, especialmente en el entorno en línea. Por ello, se considera llegado el momento de establecer un marco más sólido y coherente en materia de protección de datos en la UE, con una aplicación estricta que permita el desarrollo de la economía digital en el mercado interior, otorgue a los ciudadanos el control de sus propios datos y refuerce la seguridad jurídica y práctica de los operadores económicos y las autoridades públicas.

La Propuesta se estructura en once Capítulos cuyo contenido se resume a continuación de manera esquemática:

CAPÍTULO I.- DISPOSICIONES GENERALES (arts. 1-4).

En él se definen el objeto y objetivos del Reglamento, su ámbito material y territorial de aplicación y las definiciones de los términos

utilizados en el mismo. Debe destacarse que el Reglamento es aplicable aunque el responsable del tratamiento de los datos sea una autoridad, servicio u organismo público.

CAPÍTULO II.- PRINCIPIOS (arts. 5-10).

En este Capítulo se compendian los principios relativos al tratamiento de los datos personales; se establecen los criterios que ha de seguir el tratamiento lícito; se aclaran las condiciones para que un consentimiento sea válido como fundamento para el tratamiento lícito de los datos; se marcan nuevas condiciones para la licitud del tratamiento de los datos personales relativos a los niños; y se establece la prohibición general de tratamiento de categorías especiales de datos.

CAPÍTULO III.- DERECHOS DEL INTERESADO (arts. 11-21).

La Propuesta introduce la obligación para los responsables del tratamiento de ofrecer información transparente y de fácil acceso y comprensión, por lo que respecta al tratamiento de datos personales y al ejercicio de los derechos de los interesados. Se obliga al responsable del tratamiento a arbitrar procedimientos y mecanismos para que puedan ejercerse los derechos de los interesados, incluidos los medios para presentar solicitudes electrónicas, con la obligación de responder a la solicitud del interesado en un plazo determinado, y de motivar las denegaciones.

Información y acceso a los datos.-

La Propuesta profundiza en las obligaciones de información del responsable del tratamiento, sobre la base de lo dispuesto en la

Directiva 95/46/CE, y dispone el deber de suministrar información al interesado sobre aspectos como el periodo de conservación de los datos, el derecho a presentar una reclamación, las transferencias internacionales y la fuente de la que proceden los datos. Asimismo mantiene las posibles excepciones de la Directiva 95/46/CE, de modo que no habrá tal obligación de información, por ejemplo, si el registro o la comunicación de los datos están expresamente previstos por la ley.

Desde el punto de vista del derecho de acceso del interesado a sus datos personales, se dispone igualmente el derecho a obtener información sobre aspectos como el periodo de conservación, los derechos de rectificación y supresión y la facultad de interponer una reclamación.

Rectificación y supresión.-

La Propuesta reconoce el derecho del interesado a la rectificación de sus datos cuando resulten inexactos. Asimismo, se proclama el derecho del interesado al olvido y a la supresión de los datos que le conciernen, los cuales deberán ejercerse bajo determinadas condiciones. El responsable del tratamiento que haya difundido los datos personales quedará obligado a informar a los terceros sobre la solicitud del interesado de suprimir todos los enlaces a los datos personales, copias o réplicas de los mismos. El derecho de supresión también integra el derecho a que se restrinja el tratamiento en determinados casos, evitando la ambigüedad del término «bloqueo».

La Propuesta introduce el derecho del interesado a la portabilidad de los datos, es decir, a transferir datos de un sistema de tratamiento electrónico a otro, sin que se lo impida el responsable del tratamiento. A

modo de condición previa y con el fin de seguir mejorando el acceso de las personas físicas a sus datos personales, establece el derecho de obtener del responsable esos datos en un formato electrónico estructurado y de uso habitual.

Derecho de oposición y elaboración de perfiles.-

Se plasma el reconocimiento del derecho de oposición del interesado, basándose en la Directiva 95/46/CE, con algunas modificaciones, especialmente por lo que respecta a la carga de la prueba y su aplicación a la mercadotecnia directa. Junto a ello, se contempla el derecho del interesado a no ser objeto de una medida basada en la elaboración de perfiles.

CAPÍTULO IV.- RESPONSABLE Y ENCARGADO DEL TRATAMIENTO (arts. 22-39).

El responsable del tratamiento deberá adoptar políticas e implementar medidas apropiadas para asegurar y poder demostrar que el tratamiento de datos personales se lleva a cabo de conformidad con el Reglamento. Las medidas y procedimientos técnicos que sirvan para garantizar esa conformidad habrán de implementarse tanto en el momento de diseñar los medios de tratamiento como en el del tratamiento propiamente dicho. Asimismo, el responsable debe articular mecanismos con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales necesarios para cada fin específico del tratamiento.

La Propuesta aclara la posición y las obligaciones que pesan sobre los encargados del tratamiento. Yendo más allá de lo dispuesto en

el art. 17.2 de la Directiva 95/46/CE, se dispone que todo encargado que trate datos más allá de las instrucciones del responsable del tratamiento, ha de ser considerado corresponsable.

Tanto para responsables como para encargados del tratamiento, se introduce la obligación de cooperar con la autoridad de control, así como de conservar la documentación relativa a las operaciones de tratamiento que estén bajo su responsabilidad, en lugar de la notificación general a la autoridad de control exigida por la Directiva 95/46/CE.

En cuanto a la seguridad de los datos, la Propuesta obliga a responsables y a encargados del tratamiento a adoptar las medidas oportunas para garantizar la seguridad del mismo. La obligación del encargado a este respecto es independiente del contrato que haya suscrito con el responsable del tratamiento. De forma complementaria, se introduce una obligación de pronta notificación de las violaciones de los datos personales a la autoridad de control, así como al propio interesado.

En otro orden de cosas, se prevé la obligación de que los responsables y encargados del tratamiento lleven a cabo una evaluación de impacto de la protección de datos antes de efectuar operaciones de tratamiento arriesgadas. En algunos casos será obligatoria la autorización y consulta de la autoridad de control con anterioridad al tratamiento.

Una novedad importante es la figura del delegado de protección de datos, cuyas funciones y tareas esenciales se describen en la Propuesta. Se introduce la obligatoriedad de contar con un delegado de protección de datos en el sector público y en el sector privado, cuando

se trate de grandes empresas o en caso de que las actividades principales del responsable o del encargado del tratamiento consistan en operaciones de tratamiento que exijan un seguimiento periódico y sistemático.

CAPÍTULO V.- TRANSFERENCIA DE DATOS PERSONALES A TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES (arts. 40-45).

La Propuesta parte de que sólo podrán realizarse transferencias de datos personales que sean o vayan a ser objeto de tratamiento tras su transferencia a un tercer país o a una organización internacional, si el responsable y el encargado del tratamiento cumplen una serie de condiciones, en particular en lo tocante a las transferencias ulteriores de esos datos. Como requisito general, la transferencia sólo podrá realizarse cuando la Comisión haya decidido que el tercer país, o la organización internacional de que se trate, garantizan un nivel de protección adecuado. Entre los criterios que deberán tenerse en cuenta para que la Comisión evalúe si existe o no un nivel adecuado de protección se incluyen expresamente el Estado de Derecho, el recurso jurisdiccional y la supervisión independiente.

Para las transferencias a terceros países en relación con las cuales la Comisión no haya adoptado ninguna decisión de adecuación, se requiere que se aporten las garantías apropiadas, especialmente cláusulas tipo de protección de datos, normas corporativas vinculantes y cláusulas contractuales. No obstante, podrá procederse excepcionalmente a la transferencia en ausencia de una decisión de adecuación o de garantías apropiadas, en una serie de casos, como por

ejemplo cuando la transferencia sea necesaria para el reconocimiento, el ejercicio o la defensa de un derecho en un procedimiento judicial.

CAPÍTULO VI.- AUTORIDADES DE CONTROL INDEPENDIENTES (arts. 46-54).

La Propuesta obliga a los Estados miembros a crear autoridades de control, las cuales deberán cooperar entre sí y con la Comisión. Concretamente se prevé que cada Estado miembro dispondrá que una o varias autoridades públicas se encarguen de supervisar la aplicación del Reglamento y de contribuir a su aplicación coherente en toda la Unión, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento de sus datos personales y de facilitar la libre circulación de datos personales en la Unión. Asimismo, se fijan las condiciones para la independencia de esas autoridades, así como las condiciones generales aplicables a los miembros de las mismas.

El art. 51 de la Propuesta establece cuál es el alcance de la competencia de las autoridades de control. En su apartado tercero especifica que “la autoridad de control no será competente para controlar las operaciones de tratamiento efectuadas por los órganos jurisdiccionales en el ejercicio de su función jurisdiccional”.

Los artículos siguientes enumeran las funciones que desempeñará la autoridad de control, entre las que se incluye conocer e investigar las reclamaciones y fomentar el conocimiento de los ciudadanos en materia de riesgos, normas, garantías y derechos, y los poderes de que estará investida, incluido el de sancionar infracciones administrativas.

CAPÍTULO VII.- COOPERACIÓN Y COHERENCIA (arts. 55-72).

Este Capítulo prevé la asistencia mutua entre autoridades de control, incluidas las consecuencias del incumplimiento de la solicitud de asistencia girada por otra autoridad de control, así como las pautas a seguir en materia de operaciones conjuntas llevadas a cabo por varias autoridades de control. En segundo lugar, dispone un mecanismo de coherencia para garantizar la uniforme aplicación en las operaciones de tratamiento de datos que pueden afectar a interesados de varios Estados miembros.

CAPÍTULO VIII.- RECURSOS JUDICIALES, RESPONSABILIDAD Y SANCIONES (arts. 73-79).

Se establece el derecho de cualquier interesado a presentar una reclamación ante una autoridad de control. Ciertos organismos, organizaciones o asociaciones podrán presentar una reclamación en nombre del interesado o, en caso de violación de los datos personales, con independencia de la reclamación de un interesado.

Junto a ello, se contempla el derecho de toda persona a interponer un recurso judicial contra las decisiones de una autoridad de control que le conciernan, más en concreto se dispone que “todo interesado tendrá derecho a un recurso judicial que obligue a la autoridad de control a dar curso a una reclamación en ausencia de una decisión necesaria para proteger sus derechos, o en caso de que la autoridad de control no informe al interesado en el plazo de tres meses sobre el curso o el resultado de la reclamación”.

La competencia corresponderá a los órganos jurisdiccionales del Estado miembro en que esté establecida la autoridad de control, aunque se admite que la autoridad de control del Estado miembro en el que resida el interesado, ejercite, en nombre del interesado, una acción ante los órganos jurisdiccionales de otro Estado miembro en el que esté establecida la autoridad de control competente.

Se establecen normas comunes para los procedimientos judiciales, incluidos los derechos de los organismos, organizaciones o asociaciones de representar a los interesados ante los tribunales, el derecho de las autoridades de control a ejercitar acciones legales y de los órganos jurisdiccionales a ser informados sobre los procedimientos paralelos en otro Estado miembro.

Se establece igualmente que “toda persona que haya sufrido un perjuicio como consecuencia de una operación de tratamiento ilegal o de un acto incompatible con el presente Reglamento tendrá derecho a recibir del responsable o encargado del tratamiento una indemnización por el perjuicio sufrido”.

Finalmente, se obliga a los Estados miembros a establecer normas en materia de sanciones, a sancionar las infracciones del Reglamento, y a garantizar su aplicación; y a las autoridades de control a sancionar las infracciones administrativas enumeradas en esta disposición, imponiendo multas hasta un importe máximo, atendiendo a las circunstancias específicas de cada caso.

CAPÍTULO IX.- DISPOSICIONES RELATIVAS A SITUACIONES DE TRATAMIENTO DE DATOS ESPECÍFICAS (arts. 80-85).

La Propuesta, basándose en el art. 9 de la Directiva 95/46/CE, tal como ha sido interpretado por el Tribunal de Justicia de la UE, obliga a los Estados miembros a adoptar exenciones y excepciones a las disposiciones específicas del Reglamento cuando resulte necesario para conciliar el derecho a la protección de los datos de carácter personal con el derecho a la libertad de expresión.

Junto a ello, se disponen normas especiales para el tratamiento de datos personales relativos a la salud, en el ámbito laboral, para fines históricos, estadísticos y de investigación científica, o cuando se trate de datos de las iglesias y asociaciones religiosas.

CAPÍTULO X.- ACTOS DELEGADOS Y ACTOS DE EJECUCIÓN (arts. 86-87).

En este Capítulo se contienen las disposiciones tipo para el ejercicio de las funciones delegadas por parte de la Comisión, al tiempo que se indica la naturaleza del comité que asistirá a la Comisión.

CAPÍTULO XI.- DISPOSICIONES FINALES (arts. 88-91).

En este último Capítulo se prevé la derogación de la Directiva 95/46/CEE, se aclaran las relaciones con la Directiva 2002/58/CE, sobre la privacidad y las comunicaciones electrónicas, y se impone a la Comisión la obligación de evaluar el Reglamento y de presentar los oportunos informes. Finalmente, se establece la fecha de entrada en vigor del Reglamento y una fase transitoria.

III
REGULACIÓN Y SUPERVISIÓN DEL TRATAMIENTO DE DATOS PERSONALES OBRANTES EN FICHEROS DEPENDIENTES DE LOS ÓRGANOS JUDICIALES

A) El marco legal de referencia.

En el ámbito judicial, como en otras áreas de actividad tanto del sector público como privado, se produce el tratamiento de un gran volumen de datos de carácter personal. Dichos datos son objeto de inclusión en ficheros dependientes de los órganos judiciales, si bien ello no significa que el tratamiento de los datos en ellos incluidos obedezca al ejercicio de función jurisdiccional alguna.

En principio, debe partirse de que los ficheros judiciales, dado que no consta una exclusión expresa de los mismos en el artículo 2 de la Ley Orgánica 5/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), están sujetos, en cuanto al régimen de protección de los datos personales que consten en los mismos, a las disposiciones generales de la LOPD y de su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

De hecho, el artículo 230.5 de la Ley Orgánica del Poder Judicial (LOPJ), en la redacción dada al mismo por la L. O. 16/1994, si bien prevé que el CGPJ determine reglamentariamente “los requisitos y demás condiciones que afecten al establecimiento y gestión de los ficheros automatizados que se encuentren bajo la responsabilidad de los órganos judiciales”, añade que ello se deberá efectuar de forma “que se asegure el cumplimiento de las garantías y derechos establecidos en la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento

automatizado de los datos de carácter personal", referencia que actualmente debe entenderse hecha a la citada a la L. O. 15/1999.

Dicho de otro modo, en lo tocante a ficheros de origen judicial que contengan datos personales, la LOPJ efectúa un claro reenvío a los principios y garantías contempladas en la LOPD y su normativa de desarrollo. Ahora bien, la singularidad de la actividad jurisdiccional y los intereses generales que en ella subyacen determinan que, por otro lado, la LOPJ habilite al CGPJ para el desarrollo reglamentario de los requisitos y demás condiciones que afecten a los ficheros que se encuentren bajo la responsabilidad de los órganos judiciales, habilitación que es consecuencia directa de la consideración del Consejo como órgano de gobierno del Poder Judicial (artículo 122.2 CE) por lo que a él corresponde determinar los requisitos y demás condiciones que afecten al establecimiento y gestión de tales ficheros.

B) El Reglamento de los Aspectos Accesorios de las Actuaciones Judiciales.

La actual regulación de esos ficheros se contiene en el Reglamento del Consejo 1/2005, de 15 de septiembre, de los Aspectos Accesorios de las Actuaciones Judiciales (RAA), más en concreto en su Título V (artículos 86 a 97) dedicado al "establecimiento y gestión de los ficheros automatizados bajo la responsabilidad de los órganos judiciales", que se aplica a los ficheros de datos automatizados de carácter personal dependientes tanto de los Juzgados y Tribunales como del propio Consejo General del Poder Judicial (artículo 86).

El RAA diferencia conceptualmente, dentro de los ficheros dependientes de los órganos judiciales, entre los ficheros

"jurisdiccionales" y los "gubernativos" (art. 87.1). Los primeros son aquellos que contienen datos de carácter personal que figuren en los procesos de los que conozcan y que derivan por tanto de las actuaciones jurisdiccionales, en tanto que los segundos contienen datos personales que derivan de los procedimientos gubernativos y los definitorios de la relación funcionarial o laboral de las personas destinadas en los órganos jurisdiccionales, sus situaciones e incidencias. Más en concreto, el art. 87.2 RAA enumera los datos personales que podrán contener los ficheros de datos jurisdiccionales, a saber:

a) Los que en atención a lo dispuesto en las leyes procesales sean necesarios para el registro e identificación del procedimiento o asunto jurisdiccional con el que se relacionan;

b) Los que sean necesarios para la identificación y localización de quienes pudieran tener derecho a intervenir como parte;

c) Los necesarios para la identificación de quienes asuman las labores de defensa o representación procesal o intervengan en cualquier otra calidad en el procedimiento o asunto;

d) Los que exterioricen las resoluciones dictadas y las actuaciones en él realizadas;

e) Los derivados de la instrucción o tramitación de las diligencias judiciales.

El Reglamento (art. 88) dispone las fuentes de las que se podrán recoger los datos en uno y otro tipo de ficheros: en el caso de los

jurisdiccionales, se recogerán de los documentos o escritos que obren en el procedimiento o asunto o de las actuaciones que, con sujeción a las normas procedimentales, se realicen en ellos; en el caso de los no jurisdiccionales, los datos se obtendrán directamente de los afectados y, en los casos en los que la ley así lo permita y dentro de los límites por ella establecidos, de los órganos competentes sobre los cuerpos o carreras a los que los afectados pertenezcan.

En cuanto a la conservación y cancelación de los datos, el art. 89 establece que los datos se conservarán en tanto su supresión no sea ordenada por una decisión judicial o de los órganos de gobierno propios del Poder Judicial dictada en ejercicio de sus competencias gubernativas, no obstante lo cual se eliminarán también de forma periódica los datos reflejados en las actuaciones procedimentales que el propio sistema identifique como sujetas a un plazo de caducidad informática.

El Reglamento contempla que, por aplicación de las normas de cooperación jurisdiccional, o de competencia territorial, objetiva o funcional, o de organización de los servicios, que determinen la atribución del conocimiento del asunto o procedimiento, o de alguna de sus incidencias, o la realización de actuaciones determinadas, a un órgano jurisdiccional o gubernativo distinto, se produzca la cesión a éste de los datos de carácter personal recogidos en los ficheros propios de otro órgano (art. 90). Por su parte, las Administraciones Públicas sólo podrán hacer uso de los productos extraídos del fichero, no de éste, en virtud de decisión previa y escrita que sus órganos adopten en cumplimiento de las competencias que les sean atribuidas por el ordenamiento jurídico. La decisión habrá de ser motivada y expresará el

fin o los fines para los que se necesita hacer uso de los productos que pretenden extraerse del fichero (art. 92 RAA).

El art. 93 del RAA se refiere al ejercicio de los derechos de acceso, rectificación y cancelación [no se menciona el derecho de oposición porque éste no estaba contemplado en la LORTAD, pero debe entenderse igualmente comprendido por derivación del marco legal posteriormente vigente]: tales derechos podrán ejercerse por el afectado en la sede del órgano judicial o gubernativo titular del fichero y ante el responsable del mismo. Estos derechos se ejercerán de conformidad con las normas establecidas en la Ley Orgánica de Protección de Datos y en su reglamento de desarrollo, con las siguientes peculiaridades:

– Se denegará el acceso a los datos de carácter personal registrados en un fichero dependiente de un Juzgado o Tribunal cuando los datos afecten a unas diligencias judiciales penales que hayan sido declaradas secretas (art. 93.3).

– El derecho de acceso no podrá ejercerse en perjuicio del derecho a la intimidad de personas distintas del afectado (art. 93.4).

– Los datos que reflejen hechos constatados en un procedimiento jurisdiccional o en un expediente gubernativo no podrán ser modificados o cancelados mediante el ejercicio de los derechos de acceso, rectificación, cancelación u oposición (art. 93.5).

Por lo que se refiere al régimen de reclamaciones y recursos, el art. 94 RAA dispone que contra las resoluciones expresas o presuntas del responsable del fichero denegatorias del acceso, rectificación o cancelación [léase también oposición] que se haya solicitado, el

afectado podrá interponer los recursos previstos en el art. 4.3 de este Reglamento. El art. 4 RAA regula el régimen de acceso de los interesados a los documentos judiciales (libros, archivos, registros, sentencias), que se articulará mediante solicitud dirigida al Secretario Judicial del órgano judicial correspondiente. Éste deberá resolver en el plazo de dos días si facilita o no el acceso, a la vista del interés que el solicitante justifique, los derechos fundamentales en juego, y la necesidad de tratar los documentos a exhibir o de omitir datos de carácter personal en los testimonios o certificaciones a expedir.

Pues bien, el apartado 3 de ese artículo 4 (al que se remite el art. 94 RAA), señala que “sin perjuicio de lo establecido en las leyes de procedimiento, el acuerdo denegatorio del Secretario judicial será revisable por el Juez o Presidente a petición del interesado, que lo deberá solicitar en el plazo de tres días desde la correspondiente notificación. Si, transcurridos dos días desde la solicitud, no hubiere recaído acuerdo expreso del Secretario, ni se hubiere expedido el testimonio o certificación solicitados, o la exhibición de que se trate, se entenderá que la petición ha sido denegada y, en consecuencia, el interesado podrá ejercitar ante el Juez o Presidente el derecho de revisión mencionado anteriormente”. A su vez, se puntualiza que “contra el acuerdo del Juez o Presidente se podrán interponer los recursos establecidos en el Reglamento número 1/2000, de 26 de julio, de los órganos de Gobierno de Tribunales”. Estos recursos no son otros que el de alzada ante el Pleno del Consejo General del Poder Judicial, y el de revisión en su caso, tal y como se desprende del artículo 59.2 del Reglamento 1/2000, de forma directa para los Presidentes de Tribunales, Audiencias y Salas, y de forma indirecta –por la doble remisión de los artículos 92.2 y 88– para los Jueces. Por “Presidente”

debe entenderse a estos efectos, el que lo sea de la correspondiente Sala o Sección, de acuerdo con el art. 58.1 del Reglamento 1/2000.

Como puede verse, el RAA contiene un régimen *ad hoc* de los procedimientos de tutela de los derechos de acceso, rectificación, cancelación y oposición (derechos "ARCO"), cuando de ficheros dependientes de órganos judiciales se trate, incluido un sistema de recursos en vía gubernativa que en último extremo culminará en el Pleno del CGPJ. No obstante, este cauce particular ha resultado claramente infrautilizado en la práctica, habiéndose canalizado los recursos en materia de tutela a través de la AEPD, mediante la aplicación del régimen general que se desprende de la LOPD y de su reglamento de desarrollo. Por otro lado, lo que el RAA no contiene es una regulación específica de los procedimientos relativos al ejercicio de la potestad sancionadora en materia de datos personales tratados en ficheros judiciales. En este campo también se ha venido acudiendo a la intervención de la AEPD y a la aplicación de la LOPD y de su reglamento de desarrollo.

La creación, modificación y supresión de los ficheros judiciales se verifica mediante acuerdo del CGPJ que se adopta a propuesta de la correspondiente Sala de Gobierno (art. 95 RAA) y que se publicará en el Boletín Oficial del Estado y en los Diarios Oficiales de las Comunidades Autónomas y se notificará a la AEPD. En el caso de los ficheros dependientes del propio Consejo, la propuesta de creación procederá del Secretario General (art. 96).

Sin embargo, salvo para los ficheros dependientes del propio CGPJ, que quedan bajo la responsabilidad de su Secretario General, el RAA atribuye a los Secretarios Judiciales la condición de *responsables*

del fichero (art. 91), distinguiendo entre ficheros automatizados de órganos judiciales unipersonales, de los que será responsable el Secretario del Juzgado respectivo, y ficheros dependientes de los Tribunales, en cuyo caso la designación del Secretario Judicial responsable del tratamiento se verificará en el propio acuerdo de creación o modificación del fichero.

El hecho de que el CGPJ sea el órgano a quien se atribuye la facultad de crear, modificar y suprimir los ficheros automatizados de datos de carácter personal dependientes de los órganos judiciales, no parece implicar, desde la óptica del RAA, que también se le atribuya el rol de "responsable" de los mismos. La asignación de ese papel a los Secretarios Judiciales de cada órgano judicial dota al sistema de ficheros judiciales de una estructura descentralizada que es coherente con el hecho de que el Poder Judicial se encuentre disperso desde el punto de vista territorial. Como luego veremos, la atribución a los Secretarios Judiciales del rol de responsables de los ficheros debe ser preferentemente entendida en un sentido funcional, pues el Consejo no puede abdicar de la responsabilidad que le viene dada por el hecho de ser el sujeto que crea los ficheros y que, en última instancia, decide sobre los fines, medios y condiciones del tratamiento que se lleva a cabo a través de esos ficheros.

C) El Acuerdo plenario de 20 de septiembre de 2006, de creación de ficheros de carácter personal dependientes de los órganos judiciales.

Mediante Acuerdo de 20 de septiembre de 2006 (BOE de 12 de octubre) del Pleno del Consejo General del Poder Judicial, se procedió a la creación de ficheros de datos de carácter personal dependientes de los órganos judiciales.

En su Anexo I se crean los denominados “Ficheros jurisdiccionales”, dentro de los cuales se distingue a su vez entre los ficheros de “Asuntos Jurisdiccionales” y los ficheros de “Registro de Asuntos”. En el primero de ellos, cuya finalidad es la gestión, consulta de información y emisión de documentos procesales relativos a procedimientos tramitados ante los órganos judiciales, se contendrán los datos de carácter personal que deriven de las actuaciones jurisdiccionales y, en particular, los siguientes: (1) los que en atención a lo dispuesto en las leyes procesales sean necesarios para el registro e identificación del procedimiento con el que se relacionan; (2) los necesarios para la identificación y localización de quienes pudieran tener derecho a intervenir como parte; (3) los necesarios para la identificación de quienes asuman las labores de defensa o representación procesal o intervengan en cualquier otra calidad en el procedimiento; (4) los que exterioricen las resoluciones dictadas y las actuaciones en él realizadas; y (5) los derivados de la instrucción o tramitación de las diligencias judiciales.

Como responsable del tratamiento se señala al “órgano judicial que conozca el procedimiento”, si bien especificando que el funcionamiento del fichero queda “bajo la dependencia directa del Secretario Judicial”, lo que resulta coherente con lo dispuesto en el art. 91 RAA. Los afectados podrán ejercitar sus derechos en la sede del órgano judicial que conozca del procedimiento.

En cuanto al fichero de Registro de Asuntos, tiene marcada como finalidad la gestión, consulta y emisión de documentos relativos a los asuntos registrados y la información sobre el órgano judicial que conoce de los mismos, y contendrá los datos que sean necesarios para el

registro e identificación del procedimiento con el que se relacionan, así como para la identificación y localización de quienes pudieran tener derecho a intervenir como parte, y para la identificación de quienes asuman las labores de defensa o representación procesal o intervengan en cualquier otra calidad en el procedimiento. Como responsable del tratamiento figura el Secretario Judicial encargado del registro y los derechos de los afectados deberán ejercitarse en la sede del registro.

En el Anexo II del Acuerdo plenario de 20 de septiembre de 2006 se crean los “Ficheros gubernativos” dentro de los cuales se distinguen también dos tipos: el fichero “gubernativo” propiamente dicho y el fichero de “usuarios”. La finalidad del primero es la consulta y emisión de documentos gubernativos relativos a las plantillas de Jueces y Magistrados, Secretarios Judiciales, así como del resto del personal adscrito a la Oficina judicial, mientras que la del segundo es la gestión, mantenimiento y control de las cuentas de usuarios habilitadas en los sistemas de Gestión Procesal y demás aplicaciones informáticas, aprobadas por el CGPJ.

El fichero gubernativo contendrá los datos de carácter personal que deriven de los procedimientos gubernativos y los que, con arreglo a las normas administrativas aplicables, sean definitorios de la relación funcionarial o laboral de las personas destinadas en los órganos judiciales y de las situaciones e incidencias que en ella acontezca, así como los datos médicos imprescindibles relativos a dichas situaciones. El de usuarios contendrá los datos de carácter personal de los usuarios de las cuentas habilitadas en los sistemas de Gestión Procesal y demás aplicaciones informáticas, aprobadas por el CGPJ. En el caso del fichero gubernativo aparece como responsable del tratamiento el órgano gubernativo con competencia según las previsiones de la LOPJ,

debiéndose ejercer los derechos en la sede del órgano gubernativo correspondiente. Por su parte, en el fichero de usuarios, el responsable será la Administración Pública competente en la dotación de medios materiales, en su respectivo ámbito territorial.

En todos los casos –ficheros jurisdiccionales y gubernativos contemplados en los dos Anexos del Acuerdo– la cualidad de *encargado del tratamiento* se atribuye a las Administraciones Públicas competentes para la dotación de medios materiales, si bien en el caso concreto del Tribunal Supremo se puntualiza que el encargado del tratamiento será el Ministerio de Justicia, el cual deberá actuar en coordinación con el Gabinete de Información y Documentación del Alto Tribunal.

NOMBRE DEL FICHERO	FINALIDAD Y USOS	TIPOS DE DATOS	RESPONSABLE	ENCARGADO
Asuntos jurisdiccionales	Gestión, consulta de información y emisión de documentos procesales relativos a procedimientos tramitados ante los órganos judiciales	Los derivados de las actuaciones jurisdiccionales (necesarios para identificar procedimiento, partes, abogados y procuradores, y los obrantes en resoluciones y demás actuaciones y diligencias)	Órgano judicial que conozca el procedimiento, pero quedando el fichero bajo la dependencia directa del SJ	TS: MJU en coordinación con el Gabinete de Info. y Doc. del TS. Resto de órganos: Admón. competente en medios materiales
Registro de asuntos	Gestión, consulta y emisión de documentos relativos a los asuntos registrados y la información sobre el órgano que conoce de los mismos	Los que sean necesarios para identificar procedimiento, partes, abogados y procuradores	Secretario Judicial encargado del registro	Ídem
Gubernativo	Gestión, consulta y emisión de documentos relativos a los asuntos registrados y la información sobre el órgano judicial que conoce de los mismos	Los que deriven de procedimientos gubernativos y los definitorios de la relación funcionarial o laboral del personal de la OJ + situaciones e incidencias y datos médicos imprescindibles relativos a ellas	Órgano gubernativo con competencias conforme a la LOPJ	Ídem
Usuarios	Gestión, mantenimiento y control de las cuentas de usuarios habilitadas en los sistemas de gestión procesal y otras aplicaciones del CGPJ	Datos de los usuarios de las cuentas habilitadas en los sistemas de Gestión Procesal y demás aplicaciones del CGPJ	Admón. competente en la dotación de medios materiales	Ídem

Fig. 1.- Cuadro resumen de los distintos tipos de ficheros de datos personales dependientes de órganos judiciales

D) La supervisión en materia de datos personales en relación con los ficheros dependientes de órganos judiciales.

El CGPJ, pese a ostentar la competencia para la creación, modificación y supresión de los ficheros automatizados de carácter personal dependientes de los Juzgados y Tribunales, no tiene atribuida, ni por la LOPJ, ni por la LOPD, ni por los respectivos reglamentos de desarrollo, la competencia para actuar como autoridad de control sobre los ficheros por él creados, dependientes de los órganos judiciales.

Por el contrario, ha sido la Agencia Española de Protección de Datos (AEPD), en el marco de sus competencias y de conformidad con la normativa general sobre protección de datos personales, la que ha venido velando hasta el momento por el cumplimiento de la legislación sobre protección de datos, y operando como autoridad de control en la materia, con independencia de que las actuaciones de referencia tuvieran relación con datos personales obrantes en ficheros dependientes de órganos judiciales. A tal efecto, debe considerarse que la LOPD, a diferencia de su antecesora la LORTAD (L. O. 5/1992), no excluye expresamente al CGPJ del ámbito de control de la AEPD.

Ahora bien, dada la competencia del CGPJ en materia de inspección y vigilancia de Juzgados y Tribunales para la comprobación y control de funcionamiento de la Administración de Justicia (artículo 171 LOPJ), y a fin de conciliar esta competencia con la potestad de inspección de la AEPD dentro de su ámbito de actuación (artículo 40 LOPD), el CGPJ y la AEPD suscribieron el 3 de mayo de 2010 un Convenio de colaboración a los efectos de desarrollar inspecciones conjuntas dirigidas a verificar posibles infracciones del derecho de protección de datos de carácter personal. Hasta la fecha esa

colaboración se ha venido desarrollando sin incidencias, en un clima de máxima colaboración institucional, y ha cristalizado en diversas inspecciones conjuntas de inspectores del Servicio de Inspección del Consejo en coordinación con inspectores de la AEPD.

E) La Sentencia de la Sala Tercera del Tribunal Supremo de 2 de diciembre de 2011.

La Sentencia del Tribunal Supremo (Sala 3ª), de 2 de diciembre de 2011, vino a subvertir este esquema, al declarar la incompetencia de la AEPD para hacer la declaración de infracción en materia de protección de datos en el marco de un procedimiento sancionador seguido contra un órgano judicial. Y ello con base en que el CGPJ, en tanto órgano de gobierno del Poder Judicial, tendría singularmente reconocida la función tutelar en materia de protección de datos de carácter personal en relación con los ficheros judiciales por formar parte de su ámbito de gobierno interno, función que se justifica en la necesidad de preservar los principios de unidad e independencia de la organización judicial (art. 104 LOPJ), y que impide cualquier tipo de intromisión o ingerencia por parte de una autoridad administrativa, incluida la AEPD.

El Alto Tribunal encuentra una corroboración de esta competencia no sólo en el ya citado artículo 230 LOPJ, sino también en el artículo 107.3 LOPJ, que atribuye en exclusiva al órgano de gobierno las potestades precisas para el necesario control y observancia de los derechos y garantías, pues es únicamente a éste a quien corresponde la inspección de Juzgados y Tribunales. Según la Sentencia, el propio Consejo habría ratificado su competencia en la materia al hacer uso de la habilitación contenida en el artículo 230 LOPJ, mediante la aprobación

del RAA, en cuyo Título V se regula el establecimiento y gestión de los ficheros, tanto los del propio Consejo, como los dependientes de los Juzgados y Tribunales, situando todos ellos bajo el control del Consejo General del Poder Judicial y estableciendo un régimen propio de tutela del derecho a la protección de datos en relación con estos ficheros, mediante un sistema de reclamaciones y recursos y un régimen para el ejercicio de los derechos de acceso, rectificación y cancelación. Este régimen específico previsto para los ficheros antes mencionados es ajeno –según el Tribunal Supremo– a las competencias de la AEPD, que no puede ejercer en relación con estos ficheros facultades de supervisión y control, correspondiendo en exclusiva tales facultades al propio órgano de gobierno del Poder Judicial.

F) La diferente interpretación dada a la Sentencia por la AEPD y el CGPJ: el Acuerdo plenario de 31 de mayo de 2012.

Tras esta Sentencia, que parece erigir al Consejo General del Poder Judicial en autoridad de control añadida a las actualmente existentes –a saber, junto a la AEPD, las Agencias de Protección de Datos existentes en Cataluña, Madrid y País Vasco–, la AEPD se sintió desapoderada para tramitar todos aquellos expedientes de protección de datos que tuvieran como telón de fondo ficheros de los que fuesen responsables los órganos judiciales; y, en consecuencia, comenzó a remitir al Consejo tales expedientes en el entendimiento de que este Órgano constitucional era el competente para tramitarlos y resolverlos.

Sin embargo, la lectura que el Consejo hacía de la doctrina sentada en la STS de 2 de diciembre de 2011 distaba de la interpretación dada por la AEPD, y no permitía avalar esa drástica consecuencia. El 12 de abril de 2012 la Comisión de Estudios e

Informes aprobó un Informe que fue tomado como base por los Vocales designados para el Seguimiento del Convenio entre el CGPJ y la AEPD, quienes a su vez elevaron al Pleno una propuesta que fue aprobada por este último órgano el 31 de mayo de 2012. En esta propuesta se da especial significación al hecho de que la propia Sentencia estableciese que las funciones que han de corresponder al Consejo son únicamente aquellas que tengan por objeto la "defensa de la posición de independencia de Jueces y Magistrados que aparece proclamada en la propia norma constitucional" , o que vayan dirigidas a "preservar a Jueces y Magistrados de toda interferencia ajena, especialmente la procedente de otros poderes del Estado, tanto en el ejercicio de sus funciones jurisdiccionales como gubernativas".

En el Informe previo de la Comisión de Estudios se señalaba que eso implicaba que sólo debían trasladarse al Consejo las competencias de supervisión y control que se proyectasen estrictamente sobre la actuación de un órgano judicial de la que pudiera derivar el ejercicio de la potestad sancionadora sobre un Juez o Magistrado, permaneciendo la AEPD como autoridad de supervisión y control en el resto de casos.

Asimismo, se daba valor al hecho de que, conforme al Acuerdo del Pleno de 20 de septiembre de 2006, y a salvo los ficheros estrictamente gubernativos, no parecía asignarse a los Jueces y Magistrados, sino al Secretario Judicial, el tratamiento de ningún fichero de datos personales dependiente de órganos judiciales. En particular, destacaba que en el caso del fichero de "asuntos jurisdiccionales", pese a designarse como responsable al "órgano judicial que conozca el procedimiento", se puntualizaba que su funcionamiento quedaría "bajo la dependencia directa del Secretario Judicial", lo cual era coherente con la estructura de la Nueva Oficina Judicial, en la que al Secretario Judicial

se atribuye la función de impulsar el procedimiento y de dirigir en el aspecto técnico-procesal al personal integrante de la Oficina Judicial; de tal forma que las actuaciones de donde se recogerán los datos de que se nutre ese fichero no estarán realizadas bajo el control del Juez o Magistrado, sino del Secretario Judicial. Por ello, el Informe concluía que la supervisión y control de los ficheros de los que no sean responsables los Jueces y Magistrados, sino los Secretarios Judiciales, podría continuar siendo asumida por la AEPD, sin contravenir con ello la doctrina sentada en la STS de 2 de diciembre de 2011.

Análogamente, el Grupo de Trabajo constituido en el seno del Consejo –por ese mismo Acuerdo del Pleno de 31 de mayo de 2012– para estudiar la delimitación de competencias del CGPJ y la AEPD en esta materia, revisar el Convenio de colaboración entre ambos entes y atender la situación interina generada con los expedientes ya iniciados ante la AEPD, apreció que el número de casos en los que cabe establecer una competencia del CGPJ a título de autoridad de control sería muy pequeño, limitándose a aquéllos en los que, por ser preciso dirigir un requerimiento o intimación a un Juez o Magistrado, pudiera estar en juego la independencia judicial. Por el contrario, en la mayoría de los casos, la actividad de referencia (v. gr. el envío a un boletín oficial de un edicto con el extracto de una resolución judicial que contiene datos personales) es llevada a cabo por un Secretario Judicial en su calidad de responsable del tratamiento. En tales casos, el Grupo de Trabajo no veía razón para privar a la AEPD de su competencia para instruir y resolver los procedimientos correspondientes, al tiempo que hallaba obstáculos para que el CGPJ pueda desarrollar esa misma competencia, habida cuenta de que ello implicaría dirigir, por su parte, requerimientos o intimaciones a los Secretarios Judiciales, los cuales no están bajo su dependencia.

Debe, por último, consignarse que el Acuerdo plenario de 31 de mayo de 2012 no sólo disponía la creación del Grupo de Trabajo al que se ha hecho referencia, sino que también encomendaba a la Comisión de Estudios e Informes para que comenzase los trabajos de elaboración de una propuesta reglamentaria de modificación del RAA a fin de adecuarlo a la LOPD y a su reglamento de desarrollo, así como al modelo de la Nueva Oficina Judicial.

G) El Acuerdo plenario de 25 de julio de 2012 y el tratamiento de la cuestión en el Anteproyecto de Ley Orgánica de reforma del Consejo General del Poder Judicial.

Algunas semanas después de su puesta en funcionamiento, los miembros del Grupo de Trabajo trasladaron al Pleno su convicción, compartida con la AEPD, de que sería apropiado dirigirse conjuntamente al Ministerio de Justicia para que, a través de su impulso, el Gobierno pudiera adoptar la correspondiente iniciativa legislativa susceptible de fructificar en un texto de rango legal, en el cual quedase perfectamente perfilado el alcance de la competencia de la AEPD en el ámbito de aquellos procedimientos de protección de datos que afecten a ficheros bajo responsabilidad de los órganos judiciales, así como el papel que le cabría al Consejo en el seno de tales procedimientos como órgano de gobierno del poder judicial y garante, en suma, de la independencia judicial. Esta propuesta fue aprobada por Acuerdo plenario de 25 de julio de 2012.

Con posterioridad, ha tenido entrada en el registro del CGPJ, en fecha 8 de enero de 2013, el Anteproyecto de Ley Orgánica de reforma del Consejo General del Poder Judicial, por la que se modifica Ley

Orgánica 6/1985, de 1 de julio, del Poder Judicial, en concreto en todo lo tocante a la regulación del propio Consejo General del Poder Judicial (Título II del Libro II, que se prevé derogar, pasando su contenido a engrosar un nuevo Libro VIII de la Ley). El proyectado art. 560.19ª proclamaría la atribución del CGPJ "para ejercer con respecto a la Administración de Justicia las competencias propias de la Autoridad de Control en materia de protección de datos".

Si esta previsión superase todo el proceso de elaboración del proyecto de ley y la ulterior discusión parlamentaria, ello supondría una corroboración de la doctrina sentada en la STS de 2 de diciembre de 2011 y de la interpretación maximalista de ella efectuada por la AEPD, ya que no se limitaría a indicar la competencia del Consejo para operar como autoridad de control en materia de protección de datos relativos a los ficheros dependientes de órganos judiciales cuando pueda estar en juego la independencia judicial, por tratarse de la actuación de un Juez o Magistrado, sino que atribuiría al Consejo las competencias propias de autoridad de control en materia de protección de datos, con relación a toda la Administración de Justicia, lo que sin duda comprende también la labor de los Secretarios Judiciales, e incluso de las Administraciones públicas con competencias en materia de medios humanos y materiales de la Administración de Justicia.

IV
OBSERVACIONES SOBRE NORMATIVA ESPECÍFICA POTENCIALMENTE AFECTADA POR LA PROPUESTA

Como se desprende de lo señalado en el apartado anterior, la Propuesta de Reglamento comunitario sobreviene, por lo que se refiere a los ficheros judiciales que contienen datos de carácter personal, en un

momento en el que no sólo la normativa que es de aplicación a tales ficheros está pendiente de una puesta al día, sino que ni siquiera está del todo claro a quién corresponde desempeñar el rol de autoridad de control en este campo, siendo así que está en marcha un anteproyecto legislativo en el que se pretende explicitar la atribución de ese papel al CGPJ, con un alcance probablemente mayor que el que cabe inferir de la STS de 2 de diciembre de 2011.

Habida cuenta de ello, la valoración del impacto que podría tener la Propuesta debe ser convenientemente modulada, puesto que la normativa sobre la que dicho impacto se producirá está llamada a ser reformada, o se encuentra ya en trance de modificación. Ello puede además aconsejar que, a la hora de calibrar ese impacto, se tome como referencia no tanto la norma vigente como la norma proyectada. Desde otro punto de vista, la existencia de la Propuesta resulta enormemente oportuna, pues su contenido puede ser ya tomado como guía a la hora de acometer las reformas normativas en marcha.

Ocurre, sin embargo, que el Reglamento comunitario en ciernes está llamado a impactar sobre el sector de la protección de datos personales en su conjunto, lo que sin duda repercutirá en nuestra legislación orgánica sobre la materia y en su reglamentación de desarrollo. Dado que la modificación de la regulación de los ficheros automatizados bajo la responsabilidad de los órganos judiciales que se hace en el RAA tenía como objetivo procurar su adecuación a lo dispuesto en la LOPD y en el R. D. 1720/2007, podría considerarse apropiado no acometer aquella modificación reglamentaria hasta que, por su parte, estos instrumentos normativos hayan alcanzado una nueva configuración derivada de su adaptación a la Norma comunitaria ahora proyectada; en cualquier caso, dicha modificación debería llevarse a

cabo sin perder de vista la regulación de la Propuesta, en la medida en que ésta traerá consigo diversas innovaciones en nuestra legislación general sobre protección de datos de carácter personal.

Precisamente por esto, en rigor, la normativa que principalmente sufrirá el impacto del futuro Reglamento comunitario es la compuesta por la LOPD y el R. D. 1720/2007. Desde el punto de vista del CGPJ y de los ficheros automatizados bajo responsabilidad de los órganos judiciales, sólo podrían verse afectados los arts. 86 a 97 del RAA y el Acuerdo de 20 de septiembre de 2006 por el que se crean los ficheros de carácter personal dependientes de los órganos judiciales. En caso de prosperar lo previsto en el Anteproyecto de reforma del Consejo General del Poder Judicial, también podría verse afectado el futuro art. 560.19ª LOPJ.

En lo que sigue, procuraremos poner el énfasis en aquellos aspectos de la Propuesta –en caso de haberlos– que podrían tener incidencia más directa sobre las especialidades normativas que se refieren a los ficheros automatizados bajo responsabilidad de los órganos judiciales.

A) Principio relativos al tratamiento de datos personales.

El art. 5 de la Propuesta enumera una serie de principios a los que deberá atenerse el tratamiento de datos personales. Entre ellos, destaca el de que los datos personales tratados deberán ser "adecuados, pertinentes y limitados al mínimo necesario en relación a los fines para los que se traten" y el de que serán "conservados en una forma que permita identificar al interesado durante un período no

superior al necesario para los fines para los que se someten a tratamiento".

Estos principios podrían incidir en la delimitación que el art. 87.2 y 3 RAA hace del espectro de datos que pueden contener los ficheros automatizados dependientes de los órganos judiciales, ya sean jurisdiccionales o gubernativos, por cuanto algunos de los allí descritos podrían no responder al estándar del "mínimo necesario en relación a los fines para los que se tratan", debiendo recordarse que la Propuesta de Reglamento especifica que los datos "solo se tratarán si y siempre que estos fines [aquéllos para los que los datos se tratan] no pudieran alcanzarse mediante el tratamiento de información que no implique datos personales".

De igual modo, podría verse afectado el art. 89 del RAA, en tanto prevé que, en principio, los datos personales incorporados en los ficheros jurisdiccionales y gubernativos se conserven "en tanto su supresión no sea ordenada por una decisión judicial o de los órganos de gobierno propios del Poder Judicial dictada en ejercicio de sus competencias gubernativas", aunque también irán eliminándose "a medida que se culminen los trabajos periódicos de cancelación, los datos reflejados en las actuaciones procedimentales que el propio sistema identifique como sujetas a un plazo de caducidad informática". Sin embargo, esto no equivale exactamente a prevenir que los datos se conserven en una forma que permita identificar al interesado *durante un período no superior al necesario para los fines para los que se someten a tratamiento*. Debería reflejarse la necesidad de que todos los datos tratados sean objeto de conservación temporal, en función del fin perseguido con su tratamiento, de tal forma que transcurrido el plazo

necesario dejen de estar conservados en una forma que permita identificar a su titular.

Un tercer principio de gran importancia es el referido a que los datos deberán ser tratados bajo la responsabilidad del responsable del tratamiento, que será quien, para cada operación de tratamiento, deberá garantizar y demostrar el cumplimiento de las disposiciones del Reglamento. Pues bien, si observamos la definición que la Propuesta hace de «responsable del tratamiento» en su art. 4.5 ("persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o conjuntamente con otros determine los fines, condiciones y medios del tratamiento de datos personales"), idéntica por lo demás a la de la Directiva 95/46/CEE, que viene a estar recogida en nuestra LOPD (art. 3.d/), cabe la duda de si el RAA podrá seguir manteniendo la atribución al Secretario Judicial de la condición de «responsable» de los ficheros automatizados dependientes de los órganos judiciales. Más bien parece que el RAA deberá alinearse con lo dispuesto en los preceptos citados y asumir que el responsable del tratamiento debe ser el CGPJ en tanto éste es el que determina los fines, condiciones y medios del tratamiento de datos personales que se realiza en esos ficheros judiciales. En este sentido, podría ser oportuno emplear en el RAA una dicción similar a la que usa el Acuerdo CGPJ de 20 de septiembre de 2006, cuando en su Anexo I, apartado A.f), a renglón seguido de indicar que el responsable del tratamiento es el "órgano judicial que conozca el procedimiento", puntualiza que el funcionamiento del fichero quedará "bajo la dependencia directa del Secretario Judicial".

Ahora bien, eso supondría colocar al Secretario Judicial en una posición a caballo entre la de responsable y la de encargado del tratamiento, pues recuérdese que este último es el sujeto que lleva a

cabo el tratamiento de los datos *por cuenta del responsable* del tratamiento (vid. art. 3.g/ LOPD, art. 2.e/ de la Directiva 95/46 y art. 4.6 de la Propuesta), normalmente en el contexto de una externalización de la actividad de tratamiento (*outsourcing*). En el sistema de ficheros dependientes de órganos judiciales, como hemos visto al examinar el Acuerdo del CGPJ de 20 de septiembre de 2006, se considera que el encargado del tratamiento es siempre la Administración pública competente para la dotación de los medios materiales, con la salvedad de los ficheros dependientes del Tribunal Supremo, en donde ese rol lo desempeña el Ministerio de Justicia actuando en coordinación con el Gabinete de Información y Documentación del Alto Tribunal. La conclusión que cabe extraer de todo esto es que las categorías manejadas por el RAA casan mal con las definiciones de responsable y encargado del tratamiento que se contienen tanto en la legislación comunitaria como en la estatal.

A) Derechos de los interesados.

Conforme al art. 12 de la Propuesta, “el responsable del tratamiento establecerá procedimientos para facilitar la información contemplada en el artículo 14, y para el ejercicio de los derechos de los interesados contemplados en el artículo 13 y en los artículos 15 a 19”. Asimismo, deberá informar “sin demora al interesado y, a más tardar, en el plazo de un mes a partir de la recepción de la solicitud, de si se ha tomado alguna medida con arreglo a lo dispuesto en el artículo 13 y en los artículos 15 a 19 y facilitará la información solicitada”.

El RAA dispone que los derechos de acceso, rectificación y cancelación “se ejercerán de conformidad con las normas establecidas en 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 Datos de Carácter Personal, excepto cuanto se dispone en este artículo" (art. 93), a la par que introduce algunas especificidades sobre acceso, modificación o cancelación de ciertos tipos de datos. Admite que haya resoluciones expresas o presuntas del responsable del fichero, denegatorias del acceso, rectificación o cancelación (art. 94), pero no construye propiamente un procedimiento o mecanismo para facilitar la información a la que se refiere el art. 14 de la Propuesta, ni para ejercitar en general los derechos de los interesados. En esta medida su regulación se vería afectada por lo dispuesto en la Propuesta, aunque podría bastar con trazar una remisión a lo que disponga la LOPD y su reglamento de desarrollo, los cuales a su vez tendrán que adaptarse al futuro Reglamento comunitario.

Es importante notar que la Propuesta dispone que cuando los datos personales se sometan a tratamiento de forma automatizada, el responsable también proporcionará medios para que las solicitudes [de información y de ejercicio de derechos] se hagan por vía electrónica (art. 12.1). Esta previsión chocaría con lo señalado en el Anexo I del Acuerdo CGPJ de 20 de septiembre de 2006, cuando al referirse a los servicios ante los que se ejercerán los derechos menciona la "sede del órgano judicial que conozca del procedimiento" (fichero de asuntos jurisdiccionales), o la "sede del registro" (fichero de registro de asuntos). Ídem el Anexo II, que se refiere a la "sede del órgano gubernativo correspondiente" (fichero gubernativo). Todo apunta a que será necesario modificar esta previsión, que parece aludir a la «sede» en sentido físico, de forma que pase a admitirse explícitamente la posibilidad de ejercitar los derechos por conducto electrónico.

La Propuesta contempla expresamente el derecho del interesado a la supresión de los datos que le conciernen por parte del responsable del tratamiento, y a que éste se abstenga de darles más difusión (art. 17). La supresión podrá solicitarse, entre otras cosas, cuando los datos hayan dejado de ser necesarios para los fines para los que fueron recogidos, cuando el interesado haya ejercitado su derecho de oposición conforme al art. 19, o cuando el tratamiento no sea conforme con lo dispuesto en el Reglamento. Una vez ejercitado este derecho, el responsable del tratamiento deberá proceder a la supresión sin demora, salvo que la conservación de los datos sea necesaria por un elenco cerrado de motivos que se detallan en el art. 17.3, entre los cuales destaca el de que deba cumplirse una obligación legal de conservar los datos impuesta por la legislación del Estado miembro de que se trate o por el Derecho de la Unión.

El alcance de este “derecho al olvido y a la supresión”, como lo llama el art. 17 de la Propuesta, es mayor que el del actual derecho de cancelación, cuyos efectos en la LOPD (art. 16) no son tan inmediatos, ya que primeramente provocan el “bloqueo” de los datos, de tal forma que éstos seguirán quedando a disposición de las Administraciones públicas, Jueces y Tribunales para la atención de las posibles responsabilidades nacidas del tratamiento, procediéndose a su supresión cuando se cumpla el plazo de prescripción de tales responsabilidades. Así pues, cabe pronosticar que la LOPD deberá ser modificada para cohonestarla con la regulación que el futuro Reglamento comunitario hará del derecho a la supresión, y en la misma medida se verá afectado el RAA, que deberá dejar de referirse al derecho de cancelación para pasar a hacerlo al derecho a la supresión, evocando así los rasgos con que éste aparece definido en la Propuesta.

Un aspecto destacable del derecho a la supresión es el que se consigna en el apartado 2 del art. 17: cuando el responsable del tratamiento haya hecho públicos los datos personales, “adoptará todas las medidas razonables, incluidas medidas técnicas, en lo que respecta a los datos de cuya publicación sea responsable, con miras a informar a los terceros que estén tratando dichos datos de que un interesado les solicita que supriman cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos”, añadiéndose que “cuando el responsable del tratamiento haya autorizado a un tercero a publicar datos personales, será considerado responsable de esa publicación”. En el ámbito de los ficheros judiciales es frecuente que el responsable del tratamiento, a la sazón el Secretario Judicial, haya propiciado la publicación de los datos, por ejemplo mediante la plasmación de los mismos en un edicto que es objeto de inserción en un boletín oficial. La regulación de la Propuesta implicará que si un interesado ha solicitado la supresión de cualquier enlace o copia de sus datos, el responsable tendrá que adoptar medidas técnicas razonables dirigidas a informar de esa circunstancia a los terceros que estén tratando dichos datos, en la medida en que él mismo, al haber autorizado a un tercero a publicar los datos, es considerado el responsable de la publicación. Este régimen no encuentra reflejo en el RAA y, por consiguiente, éste deberá ser objeto de la oportuna modificación.

En otro orden de cosas, la Propuesta contempla también un nuevo “derecho a la portabilidad” (art. 18), consistente en que, “cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el interesado tendrá derecho a obtener del responsable del tratamiento una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos”. Nada semejante a este

derecho es objeto de previsión en el RAA –tampoco en la LOPD–, de tal forma que también aquí será necesario innovar aquél para ponerlo en concordancia con la futura Norma comunitaria.

Finalmente, por lo que hace al derecho de oposición (art. 19), que el RAA ya omitía por arrastre de su antecesor –cortado a su vez por el patrón de la LORTAD, que no contemplaba el derecho en cuestión–, la Propuesta lo define en los términos siguientes: "[e]l interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales sean objeto de un tratamiento basado en el artículo 6, apartado 1, letras d), e) y f), salvo que el responsable del tratamiento acredite motivos imperiosos y legítimos para el tratamiento que prevalezcan sobre los intereses o los derechos y libertades fundamentales del interesado". Las letras d), e) y f) del art. 6.1 se refieren respectivamente al tratamiento que sea necesario para proteger intereses vitales del interesado, para el cumplimiento de una misión de interés público, o para la satisfacción del interés legítimo perseguido por el responsable del tratamiento, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado; aunque esto último no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones. Así pues, el RAA deberá determinar qué margen cabe para el derecho de oposición en el ámbito de los ficheros dependientes de órganos judiciales, más allá de incluir alguna referencia explícita a este derecho, que a su vez tendrá que pasar a ser regulado en la LOPD de un modo consistente con la configuración que de él haga el futuro Reglamento.

C) Responsable del tratamiento y delegado de protección de datos.

Teniendo en cuenta lo que hemos señalado a propósito del «responsable del tratamiento» en el ámbito de los ficheros automatizados de datos personales dependientes de órganos judiciales, a saber, que si bien el responsable funcional es el Secretario Judicial, el CGPJ no deja de ser quien determina los fines, condiciones y medios del tratamiento de los datos contenidos en esos ficheros, y quien por tanto mediatamente ejerce esa responsabilidad, es de relieve lo que dice el art. 22 de la Propuesta sobre las obligaciones del responsable del tratamiento, a quien compete adoptar políticas e implementar medidas apropiadas "para asegurar y poder demostrar que el tratamiento de datos personales se lleva a cabo de conformidad con el presente Reglamento". Entre esas medidas se incluirán, de acuerdo con el segundo apartado de ese precepto:

– la conservación de la documentación con arreglo a lo dispuesto en el artículo 28;

– la implementación de los requisitos en materia de seguridad de los datos establecidos en el artículo 30;

– la realización de una evaluación de impacto en relación con la protección de datos con arreglo a lo dispuesto en el artículo 33;

– el cumplimiento de los requisitos en materia de autorización o consulta previas de la autoridad de control;

– la designación de un delegado de protección de datos con arreglo a lo dispuesto en el artículo 35.1.

Asimismo, el art. 22.3 previene que el responsable del tratamiento deberá implementar mecanismos para verificar la eficacia de las medidas contempladas en los apartados 1 y 2 de ese mismo artículo, verificaciones que, siempre que no sea desproporcionado, serán llevadas a cabo por auditores independientes internos o externos.

Así pues, son múltiples las obligaciones que pesan sobre el responsable del tratamiento, de acuerdo con la configuración plasmada en la Propuesta, y ello no podrá dejar de tener reflejo en el RAA (así como en la LOPD). Esas obligaciones se traducirán no sólo, o no tanto, en modificaciones normativas, sino en la asunción de los cometidos correspondientes por el CGPJ, aunque éste determine por vía reglamentaria –como hace ahora– que el desempeño material de esos deberes corresponderá, en todo o en parte, al responsable *funcional* de los ficheros, esto es, al menos para los ficheros jurisdiccionales, el Secretario Judicial del órgano o del registro de que se trate. Ocurre, sin embargo, que algunas de las obligaciones de que estamos hablando difícilmente pueden ser atendidas de forma dispersa o descentralizada, sino que deberán serlo de manera transversal o centralizada. Es el caso –creemos– de la designación del delegado de protección de datos, la realización de evaluaciones de impacto o la implementación de requisitos en materia de seguridad.

En este mismo orden de cosas, aunque el art. 22 no aluda a ello, el art. 23.1 señala que el responsable del tratamiento deberá implementar, tanto en el momento de la determinación de los medios de tratamiento como en el del tratamiento propiamente dicho, medidas y procedimientos técnicos y organizativos apropiados, de manera que el tratamiento sea conforme con las disposiciones del presente

Reglamento y garantice la protección de los derechos del interesado, todo ello a la vista de las técnicas existentes y de los costes asociados a su uso. Junto a ello, también deberá el responsable del tratamiento aplicar mecanismos con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales necesarios para cada fin específico del tratamiento y, especialmente, que no se recojan ni conserven más allá del mínimo necesario para esos fines, tanto por lo que respecta a la cantidad de los datos como a la duración de su conservación. Esta obligación de implementar la protección de datos desde el propio diseño de los medios de tratamiento y con una perspectiva en la que, por defecto, sólo sean tratados y conservados los datos mínimos imprescindibles y por el menor tiempo posible, es sin duda un deber que deberá asumirse en el trance de crear o modificar los ficheros automatizados de datos personales dependientes de los órganos judiciales, y es dable entender que el RAA, en cuyos arts.86 y siguientes no se recoge explícitamente esta obligación, habrá de sufrir la correspondiente modificación a fin de que dicha obligación quede plasmada.

Especialmente relevante nos parece la obligación de documentación, a la que se refiere el art. 28 de la Propuesta, conforme al cual “cada responsable y cada encargado del tratamiento, así como, en su caso, el representante del responsable,[1] deberán conservar la documentación de todas las operaciones de tratamiento efectuadas bajo su responsabilidad”. Esa documentación deberá contener, como mínimo, la siguiente información:

[1] Obsérvese que, conforme al art. 25 de la Propuesta, todo responsable del tratamiento que no esté establecido en el territorio de la UE, pero trate datos de interesados que sí residan en ella, debe designar un “representante”, quien actuará en lugar de aquél y al que podrá dirigirse cualquier autoridad de control en lo relativo a las obligaciones que incumben al responsable del tratamiento.

a) nombre y datos de contacto del responsable o responsables y del encargado o encargados del tratamiento;

b) nombre y datos de contacto del delegado de protección de datos;

c) fines del tratamiento;

d) descripción de las categorías de interesados y de las categorías de datos personales que les conciernen;

e) destinatarios o categorías de destinatarios de los datos, incluidos los responsables del tratamiento a quienes se comuniquen datos personales;

f) transferencias eventuales de datos a un tercer país o a una organización internacional;

g) indicación general de los plazos establecidos para la supresión de las diferentes categorías de datos;

h) descripción de los mecanismos de verificación de las medidas que permitan asegurar y demostrar que el tratamiento se lleva a cabo de acuerdo con el Reglamento.

De nuevo, el RAA deberá experimentar la correspondiente modificación a fin de reflejar los pormenores de esta obligación de documentación, que pesará probablemente sobre el Consejo, en tanto órgano a quien corresponde la potestad de creación, modificación y

supresión de los ficheros de los que venimos hablando, y por añadidura la facultad de determinar los fines, condiciones y medios del tratamiento de los datos.

Otro tanto cabe decir de la obligación de notificación de una violación de datos personales, que deberá practicarse tanto a la autoridad de control como al propio afectado (arts. 31 y 32 de la Propuesta). De conformidad con el primero de esos preceptos, en caso de violación de datos personales, el responsable del tratamiento deberá notificarla a la autoridad de control sin demora injustificada y, de ser posible, menos de veinticuatro horas después de que haya tenido constancia de ella, debiendo acompañar la notificación de una justificación motivada si la efectúa fuera de ese plazo. Esa notificación deberá, entre otras cosas, describir la naturaleza de la violación, las categorías y el número de afectados, así como las consecuencias de la violación, recomendar medidas tendentes a atenuar sus posibles efectos negativos y describir las medidas propuestas o ya adoptadas por el responsable del tratamiento a tal propósito. Se añade también (art. 31.4) que el responsable del tratamiento, al objeto de que la autoridad de control pueda verificar el cumplimiento de las disposiciones que el Reglamento contiene, documentará cualquier violación de datos personales, indicando su contexto, sus efectos y las medidas correctivas adoptadas.

Esa dicotomía entre responsable y autoridad de control que se refleja en el precepto, trasladándonos al caso de los ficheros dependientes de órganos judiciales, y en tanto el CGPJ podría estar abocado a asumir el papel de autoridad de control en materia de datos personales respecto de dichos ficheros, implicaría que la obligación de notificación de la violación pesase sobre el Secretario Judicial,

responsable *de facto* de la llevanza de los ficheros, y que el destinatario de la notificación a la que se refiere el art. 21 de la Propuesta fuese precisamente el CGPJ. Ya hemos dicho *supra* que el manejo riguroso de las categorías en materia de protección de datos, en particular la diferenciación entre responsable y encargado del tratamiento, no es el *punto fuerte* del RAA. Eso sin duda complicará el modo de reflejar en él el mecanismo de notificación de las violaciones regulado en la Propuesta, pero este mecanismo, en cualquier caso, deberá tener reflejo en el renovado RAA. Ello ha de hacerse extensible a la obligación de comunicación de la violación al interesado, la cual se contempla en el art. 32 de la Propuesta y pesa igualmente sobre el responsable del tratamiento, quien deberá proceder a ella, sin demora injustificada, después de haber llevado a cabo la notificación a la autoridad de control.

Todavía dentro del Capítulo IV de la Propuesta, debe prestarse atención a la figura del «delegado de protección de datos», que es objeto de tratamiento en los arts. 35 a 37. Al delegado de protección de datos se le asignan una serie de tareas, entre las que cabe destacar las siguientes:

a) informar y asesorar al responsable del tratamiento de las obligaciones que le incumben en virtud del presente Reglamento;

b) supervisar la implementación de las políticas en materia de protección de datos personales, incluida la formación del personal que participa en las operaciones de tratamiento y las auditorías correspondientes;

c) supervisar la aplicación del presente Reglamento, en particular por lo que hace a los requisitos relativos a la protección de datos desde el diseño, la protección de datos por defecto y la seguridad de los datos,

así como a la información de los interesados y las solicitudes presentadas en el ejercicio de sus derechos;

d) velar por la conservación de la documentación contemplada en el artículo 28;

e) supervisar la documentación, notificación y comunicación de las violaciones de datos personales;

f) supervisar la realización de la evaluación de impacto relativa a la protección de datos por parte del responsable del tratamiento;

Pues bien, para cuando el tratamiento de datos sea llevado a cabo por una autoridad u organismo público, como sería el caso que nos ocupa, el art. 35 de la Propuesta prevé la necesidad de que el responsable del tratamiento designe un delegado de protección de datos. Dicho delegado podrá ser designado para varias de las entidades de que se componga dicha autoridad u organismo, teniendo en cuenta su estructura organizativa. La Propuesta también especifica que el responsable del tratamiento designará al delegado de protección de datos en atención a sus cualidades profesionales, y en particular a sus conocimientos especializados de la legislación y las prácticas en materia de protección de datos, y a su capacidad para ejecutar las tareas contempladas en el artículo 37.

Parece clara la necesidad de reflejar todas estas cuestiones en la normativa sobre protección de datos personales objeto de tratamiento en los ficheros automatizados dependientes de órganos judiciales, pues sin duda se trata de un ámbito en el que será necesario efectuar la

designación de un delegado de protección de datos con todas esas características y funciones.

D) Autoridades de control.

La Propuesta parte de la premisa de que cada Estado miembro podrá disponer de una o varias autoridades públicas que se encarguen de supervisar la aplicación del Reglamento y de contribuir a su aplicación coherente en toda la Unión, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento de sus datos personales y de facilitar la libre circulación de datos personales en la Unión (art. 46.1). De hecho, en España, junto a la Agencia Estatal, vienen funcionando hasta la fecha algunas autoridades de control autonómicas, concretamente es el caso de Cataluña, Madrid y País Vasco. Asimismo, tal y como se ha indicado *supra*, el Anteproyecto de Ley Orgánica de reforma del Consejo General del Poder Judicial, que en estos momentos se encuentra en fase de informe por este Órgano, prevé la atribución al CGPJ de la competencia "para ejercer con respecto a la Administración de Justicia las competencias propias de la Autoridad de Control en materia de protección de datos" (vid. proyectado artículo 560.19ª LOPJ). Esta previsión, por tanto, no plantearía dificultades de encaje con el texto del futuro Reglamento comunitario.

Ahora bien, la Propuesta establece una serie de requisitos sobre los miembros de la autoridad de control que sí podrían suponer un obstáculo para la asignación al CGPJ del rol de autoridad de control en materia de protección de datos. No tanto por lo que se refiere a su independencia y a la no recepción de instrucciones de nadie (art. 47.1 y 2 de la Propuesta), lo que se viene a cohonestar con el estatuto que la

LOPJ diseña para los Vocales del Consejo (vid. art. 117.1 y 119.2 LOPJ), sino por lo que hace a la exclusividad con la que supuestamente deben desarrollar su función a tenor del art. 47.3 de la Propuesta ("los miembros de la autoridad de control se abstendrán de cualquier acción que sea incompatible con sus funciones y no participarán, mientras dure su mandato, en ninguna actividad profesional incompatible, sea o no remunerada"). Obsérvese también que, en virtud del art. 48.2 de la Propuesta, los miembros de la autoridad de control "serán elegidos entre personas que ofrezcan absolutas garantías de independencia y que posean experiencia y aptitudes acreditadas para el ejercicio de sus funciones, en particular en el ámbito de la protección de datos personales". La implementación de esta norma llevaría consigo la necesidad de que todos, o al menos algunos de los Vocales del CGPJ, reuniesen estas especiales aptitudes, a fin de lograr una debida conformación del órgano en tanto autoridad de control de datos personales.

Por lo demás, configurar al CGPJ como autoridad de control en materia de datos personales dentro del ámbito de la Administración de Justicia tendría la consecuencia de que, de acuerdo con el artículo 47.5 y 6 de la Propuesta, debería ser dotado de los recursos humanos, técnicos y financieros adecuados, así como de los locales y las infraestructuras necesarios para el ejercicio efectivo de sus funciones y poderes, así como de su propio personal, nombrado por el director de la autoridad de control y sujeto a su autoridad. El legislador debería tener en cuenta estas previsiones a la hora de proceder a una nueva configuración de la estructura orgánica del Consejo. Por lo demás, la explícita configuración del CGPJ como autoridad de control provocaría un indudable impacto en el RAA, que debería ser igualmente adaptado a esa realidad.

E) Reclamaciones, recursos y sanciones.

El último bloque de cuestiones en el que la Propuesta podría producir un impacto en el modo en que actualmente se halla articulado el establecimiento y gestión de los ficheros automatizados dependientes de órganos judiciales, es el relativo a las reclamaciones que los interesados pueden presentar ante la autoridad de control, los recursos judiciales contra las autoridades de control y las sanciones a imponer ante las infracciones de la normativa en materia de protección de datos.

Por lo que hace a las reclamaciones, el art. 73.1 señala que "sin perjuicio de los recursos administrativos o judiciales, todo interesado tendrá derecho a presentar una reclamación ante la autoridad de control de cualquier Estado miembro si considera que el tratamiento de sus datos personales no se ajusta a lo dispuesto en el presente Reglamento". Ciertamente, esta posibilidad estaría contemplada, hoy por hoy, en el RAA, cuyo art. 94 dispone la posibilidad de interponer un recurso en vía gubernativa dentro de los procedimientos de tutela. En la medida en que consideremos que el Consejo es la autoridad de control en este campo, y habida cuenta de que el sistema de recursos gubernativos culmina en el Pleno de este Órgano por mor de lo dispuesto en el Reglamento 1/2000, esa previsión colmaría las exigencias establecidas en la propuesta a este respecto.

No obstante, con independencia de que la dicción de la Propuesta parece comprender otras infracciones de la normativa sobre protección de datos no necesariamente ligadas con el ejercicio de los derechos "ARCO", hay que tener en cuenta que el RAA limita la legitimación activa para esta clase de recursos exclusivamente al afectado, mientras que el

art. 73.2 de la propuesta indica también que “todo organismo, organización o asociación que tenga por objeto proteger los derechos e intereses de los interesados por lo que se refiere a la protección de sus datos personales, y que haya sido correctamente constituido con arreglo a la legislación de un Estado miembro, tendrá derecho a presentar una reclamación ante una autoridad de control en cualquier Estado miembro por cuenta de uno o más interesados si considera que los derechos que les asisten en virtud del presente Reglamento han sido vulnerados como consecuencia del tratamiento de los datos personales”. Esta previsión no tiene reflejo en el RAA y, por consiguiente, en este punto debería ser objeto de la oportuna modificación.

En cuanto a los recursos judiciales, la Propuesta prevé que “toda persona física o jurídica tendrá derecho a un recurso judicial contra las decisiones de una autoridad de control que le conciernan” (art. 74.1), previsión que debe considerarse suficientemente cubierta en el caso del CGPJ en virtud del art. 143.2 LOPJ, que admite la posibilidad de recurrir en vía contencioso-administrativa los actos, resoluciones y disposiciones emanados del Pleno del CGPJ.

Junto a lo anterior, el art. 74.2 de la Propuesta señala que “todo interesado tendrá derecho a un recurso judicial que obligue a la autoridad de control a dar curso a una reclamación en ausencia de una decisión necesaria para proteger sus derechos, o en caso de que la autoridad de control no informe al interesado en el plazo de tres meses sobre el curso o el resultado de la reclamación” (art. 74.2). Quizás esta especialidad sí debería ser objeto de una inclusión expresa dentro de nuestra normativa nacional. Igualmente, debe tenerse en cuenta la posibilidad que contempla el art. 74.4 de la Propuesta, en virtud del cual “el interesado que se vea afectado por una decisión de una autoridad de

control de un Estado miembro en el que no tiene su residencia habitual podrá solicitar a la autoridad de control del Estado miembro en el que tiene su residencia habitual que ejercite en su nombre una acción contra la autoridad de control competente en el otro Estado miembro".

Por otro lado, la Propuesta establece que, junto a la reclamación ante la autoridad de control, el interesado persona física deberá tener derecho a un recurso judicial contra el responsable del tratamiento cuando considere que los derechos que le asisten en virtud del Reglamento han sido vulnerado como consecuencia de un tratamiento de sus datos personales no conforme con el mismo (art. 75.1). Esta posibilidad de entablar una acción judicial directa contra la actuación del responsable del tratamiento no se encuentra prevista en la normativa por la que se rige la gestión de los ficheros automatizados de datos dependientes de órganos judiciales, y por consiguiente dicha normativa debería ser objeto de la correspondiente innovación.

Finalmente, por lo que se refiere a las sanciones, el art. 78 de la Propuesta dispone que "los Estados miembros establecerán normas sobre las sanciones aplicables a las infracciones de las disposiciones del presente Reglamento y adoptarán todas las medidas necesarias para garantizar su cumplimiento". Por su parte, el art. 79 indica que "cada autoridad de control estará facultada para imponer sanciones administrativas de acuerdo con el presente artículo", el cual contempla únicamente sanciones de carácter pecuniario, de mayor o menor entidad en función de la naturaleza, gravedad y duración de la infracción, la intencionalidad o negligencia en la infracción, el grado de responsabilidad de la persona física o jurídica y anteriores infracciones de dicha persona, las medidas de carácter técnico y organizativo y los procedimientos aplicados de conformidad con el artículo 23, así como el

grado de cooperación con la autoridad de control con el fin de reparar la infracción. Creemos que este tipo de sanciones no son oportunas cuando hablamos de tratamiento de datos personales por parte de organismos o Administraciones públicas. Es de esperar que el Reglamento, tal y como se propone en el documento que recoge la Posición del Reino de España sobre la Propuesta (pp. 161-167), sea flexibilizado en este punto, para dar acogida a otro tipo de sanciones.

Sea como fuere, si el Consejo se configura como autoridad de control, es obvio que debería ostentar la correspondiente potestad sancionadora, con independencia de que la clase de sanciones a imponer no sean multas. Esto es algo que en el momento actual no sucede, previéndose a lo más un cauce específico para los procedimientos de tutela pero no para los de infracción, de modo que, con independencia de la Propuesta de Reglamento comunitario, la regulación de la materia debería reflejar este aspecto. Puesto que la regulación de la potestad sancionadora y la configuración de las infracciones y sanciones es materia que debe considerarse sujeta a reserva de ley, el prelegislador, que prevé configurar explícitamente al CGPJ como autoridad de control, debería ocuparse también de perfilar a nivel legal la potestad sancionadora del Consejo en este campo.

Obsérvese, como reflexión final, que el Anteproyecto de Ley Orgánica de reforma del Consejo General del Poder Judicial contempla una importante reducción del radio de alcance de la potestad reglamentaria del Consejo, pero no parece que ello deba incidir en la capacidad del Consejo para reglamentar lo relativo a la gestión de los ficheros automatizados dependientes de órganos judiciales (a salvo lo que acaba de decirse sobre la potestad sancionadora), modificando a tal efecto el Título V del RAA. El proyectado art. 560.16ª LOPJ indica, como

únicas materias en las que el Consejo conservará su potestad reglamentaria: la organización y funcionamiento del propio Consejo y su personal, los órganos de gobierno de Juzgados y Tribunales, el régimen de guardias de los órganos jurisdiccionales, la publicación de las resoluciones judiciales y la estadística judicial, además de poder reglamentar otros aspectos accesorios de las actuaciones judiciales que la ley expresamente le autorice, sin afectar en ningún caso al estatuto de Jueces y Magistrados, ni regular directa o indirectamente los derechos y deberes de terceras personas.

Pues bien, uno de esos aspectos accesorios cuya reglamentación la Ley autoriza expresamente al Consejo, en tanto no se prevé la modificación o derogación del actual art. 230.5 LOPJ, sería precisamente el de los requisitos y demás condiciones que afecten al establecimiento y gestión de los ficheros automatizados que se encuentren bajo la responsabilidad de los órganos judiciales, a fin de asegurar el cumplimiento de la normativa sobre protección de datos de carácter personal. Ello sería además coherente con el hecho de que el Anteproyecto planee configurar al Consejo como autoridad de control en este campo. Obsérvese que la disposición adicional primera del Anteproyecto estatuye que los actuales Reglamentos del CGPJ conserven su vigencia en tanto sean compatibles con la futura LOPJ, e incluso respecto de algunos de ellos, en todo o en parte, se prevé que se mantengan y que sólo puedan ser modificados en lo sucesivo mediante norma con rango de ley, lo que no es el caso del Título V del RAA.

IV
CONCLUSIONES

Como consecuencia del análisis efectuado en el anterior epígrafe, se compendian a continuación, de forma sucinta, los cambios que habría que introducir en el RAA y en el Acuerdo del CGPJ de 20 de septiembre de 2006, a fin de acomodarlos al futuro Reglamento comunitario:

PRIMERA.- Los arts. 87.2 y 3 RAA, que delimitan el espectro de datos que pueden contener los ficheros automatizados dependientes de los órganos judiciales, podrían verse afectados por alguno de los principios establecidos en el art. 5 de la Propuesta.

SEGUNDA.- El art. 89 RAA, sobre conservación de los datos contenidos en los ficheros dependientes de órganos judiciales, podría tener que acomodarse a la exigencia, plasmada en la Propuesta, de que los datos sean conservados por un periodo no superior al necesario para los fines para los que se someten a tratamiento.

TERCERA.- Es dudoso que el RAA pueda seguir manteniendo la atribución al Secretario Judicial de la condición de “responsable” de los ficheros jurisdiccionales dependientes de los órganos judiciales. Esa función debería corresponder al propio CGPJ, en tanto éste es quien determina los fines, condiciones y medios del tratamiento de los datos contenidos en esos ficheros. En general, se aprecia que las categorías manejadas por el RAA casan mal con las definiciones de responsable y encargado del tratamiento que se contienen tanto en la legislación comunitaria como en la estatal.

CUARTA.- El RAA debería modificarse para incluir procedimientos o mecanismos que sirvan para facilitar a los interesados la información a la que se refiere el art. 14 de la Propuesta, así como para el ejercicio de los derechos “ARCO” por parte de los afectados.

QUINTA.- Será necesario modificar la previsión del Acuerdo CGPJ de 20 de septiembre de 2006, a fin de admitir que los derechos de los interesados puedan ser ejercitados por conducto electrónico, pues en su versión actual sólo contempla la posibilidad de que ese ejercicio se desarrolle en la sede física del órgano u oficina donde se localiza el responsable del fichero.

SEXTA.- En lugar del derecho de cancelación, el RAA habrá de pasar a referirse al derecho al olvido y a la supresión, cuyos efectos, siguiendo los términos en que este último derecho se describe en el art. 17 de la Propuesta, son más poderosos. En particular, el RAA deberá reflejar el régimen descrito en el art. 17.2 de la Propuesta para cuando el responsable del tratamiento haya autorizado a un tercero a publicar los datos posteriormente objeto de la supresión solicitada por el interesado.

SÉPTIMA.- Será preciso reflejar en el RAA el nuevo derecho a la portabilidad de los datos, contemplado en el art. 18 de la Propuesta. Asimismo, el RAA deberá calibrar qué margen cabe para el derecho de oposición en el ámbito de los ficheros dependientes de órganos judiciales.

OCTAVA.- Las múltiples obligaciones que la Propuesta hace pesar sobre el responsable del tratamiento, deberán tener reflejo en el RAA, aunque más que, o además de, modificaciones normativas, esas obligaciones comportarán la asunción por parte del CGPJ de los

correspondientes cometidos (v. gr. en materia de seguridad de los datos, conservación de documentación o realización de evaluación de impacto).

NOVENA.- En esa misma línea, el Consejo deberá implementar la protección de datos desde el propio diseño de los medios de tratamiento y con una perspectiva en la que, por defecto, sólo sean tratados y conservados los datos mínimos imprescindibles y por el menor tiempo posible (art. 23 de la Propuesta). Otro tanto cabe decir de la obligación de notificación de una violación de datos personales (arts. 31 y 32 de la Propuesta), y de la necesidad de proceder a la designación de un «delegado de protección de datos» (art. 35 de la Propuesta).

DÉCIMA.- En el caso de que, como prevé el Anteproyecto de reforma del Consejo General del Poder Judicial, el cual se halla actualmente sometido a dictamen del propio CGPJ, este Órgano constitucional quede configurado como autoridad de control dentro del ámbito de los ficheros dependientes de órganos judiciales, podrían suscitarse algunos problemas derivados de los requisitos que la Propuesta contempla en relación con los miembros de las autoridades de control nacionales. Asimismo, en esa hipótesis, el Consejo debería ser dotado con los medios humanos, técnicos y materiales a los que se refiere el art. 47.5 y 6 de la Propuesta.

UNDÉCIMA.- En cuanto a las reclamaciones ante la autoridad de control en materia de protección de datos, el RAA debería ser objeto de la oportuna modificación a fin de ampliar los legitimados activos para entablar los correspondientes recursos, en consonancia con lo dispuesto en el art. 73.2 de la Propuesta. Igualmente, podría ser necesario reflejar la especialidad prevista en el art. 74.2 de la Propuesta, que contempla

un tipo de tutela judicial que puede derivar en la obligación para la autoridad de control de dar curso a la reclamación interpuesta por el afectado. Junto a ello, el RAA habría de contemplar la posibilidad de entablar acción judicial directa contra la actuación del responsable del tratamiento, conforme al art. 75 de la Propuesta.

DUODÉCIMA.- Si el Consejo se configura en el futuro como autoridad de control en materia de datos personales, no quedará más remedio que dotarle de una potestad sancionadora en este campo y prever un cauce procedimental específico para los casos de infracción, por más que quepa disentir del sistema de sanciones (únicamente pecuniarias) actualmente plasmado en la Propuesta.

Es todo cuanto tiene que informar el Pleno del Consejo General del Poder Judicial.

Y para que conste y surta efectos, extiendo y firmo la presente en Madrid, a veinticuatro de enero de dos mil trece.