

El anteproyecto objeto de informe persigue, en palabras de su Exposición de Motivos, un triple objetivo: “afianzar que el acceso a la justicia suponga la consolidación de derechos y garantías de los ciudadanos y ciudadanas; que su funcionamiento como servicio público se produzca en condiciones de eficiencia operativa; y que la transformación digital de nuestra sociedad reciba traslado correlativo en la Administración de Justicia”.

Para ello, el Título I regula los medios adecuados de solución de controversias en vía no jurisdiccional, con el fin de “potenciar la negociación entre las partes, directamente o ante un tercero neutral, partiendo de la base de que estos medios reducen el conflicto social, evitan la sobrecarga de los tribunales y son igualmente adecuados para la solución de la inmensa mayoría de las controversias en materia civil y mercantil”; el Título II recoge las reformas procesales tendentes a una mayor agilización en la tramitación de los procedimientos judiciales, introduciendo las modificaciones oportunas en la Ley de Enjuiciamiento Criminal, aprobada por el Real Decreto de 14 de septiembre de 1882; en la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa; en la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil; en la Ley 36/2011, de 10 de octubre, reguladora de la Jurisdicción Social; y en la Ley 15/2015, de 2 de julio, de la Jurisdicción Voluntaria; y el Título III se dedica a la “Transformación digital”, modificando la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

I

Desde la perspectiva de la protección del derecho fundamental a la protección de datos personales, la normativa general a la que deben ajustarse los tratamientos de datos personales contemplados en el Anteproyecto remitido es el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, RGPD), complementado por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). Y, tratándose del orden jurisdiccional penal, deberá atenderse a lo dispuesto en la recientemente aprobada Ley Orgánica 7/2021,

de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, por la que se ha procedido a la transposición de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

El RGPD constituye, por tanto, la normativa general sobre protección de datos de carácter personal y es directamente aplicable, siendo esta norma la que debe citarse, en primer término, en aquellos preceptos del Anteproyecto que se refieren a la normativa aplicable en materia de protección de datos personales y no la LOPDGDD (como ocurre, por ejemplo, en el Título III de la norma proyectada).

II

Una vez identificada la normativa aplicable a los tratamientos de carácter personal objeto del Anteproyecto, resulta preciso hacer una delimitación de las competencias que ostenta esta Agencia en relación con los mismos, atendiendo a que se trata, principalmente, de modificaciones de la normativa procesal.

A este respecto, la misma quedaba excluida, en relación con el ejercicio de las actividades de supervisión e inspección del cumplimiento de las obligaciones y garantías derivadas de la Ley Orgánica 15/1999 y sus disposiciones de desarrollo por parte de los órganos jurisdiccionales, a partir de la doctrina sentada por la Sentencia del Tribunal Supremo de 5 de diciembre de 2011, en que se estimó el recurso de casación interpuesto por el titular del Juzgado de lo Contencioso Administrativo nº 1 de A Coruña contra sentencia de la Audiencia Nacional que confirmaba la sanción impuesta a dicho órgano jurisdiccional por esta Agencia, cuyo fundamento de derecho tercero señala lo siguiente:

“La Ley Orgánica del Poder Judicial dedica fundamentalmente un precepto a la protección de datos de carácter personal. Se trata del art. 230, ubicado en el Título III (“De las actuaciones judiciales”) del Libro III, que habilita en su apartado primero a Juzgados y Tribunales a utilizar cualesquiera medios técnicos, electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y ejercicio de sus funciones, con sujeción a la normativa de protección de datos. En dicho precepto se establece además el deber de salvaguardar en todo momento la confidencialidad, privacidad y seguridad de los datos de carácter

personal contenidos en los ficheros judiciales. Estos deberes jurídicos, cuyos principales destinatarios son los propios Jueces y Magistrados, resultan obligados desde el reconocimiento de la protección de datos personales como derecho fundamental de la persona en la STC 292/2000 e inciden en la actuación de los Tribunales de muy diversas maneras, máxime si se tiene en cuenta que la legislación española y europea en general contiene una amplísima definición de lo que se entiende por dato personal (cualquier información concerniente a personas físicas identificadas o identificables). En definitiva, los datos de carácter personal forman parte consustancial de la actividad jurisdiccional, sirven de base para el funcionamiento de determinados ficheros judiciales y otros registros públicos de uso judicial y permiten llevar a cabo diligencias fundamentales para la investigación criminal, lo que plantea situaciones especialmente complejas, dado que pueden verse afectados otros derechos fundamentales, como sucede por ejemplo, en el acceso a los datos de tráfico en las comunicaciones electrónicas, a ficheros policiales o a la historia clínica. En todos estos supuestos, las posibilidades de actuación judicial en relación con los datos personales son ciertamente amplias, de ahí que tenga especial sentido el mandato de confidencialidad, privacidad y seguridad contenido en el art. 230 LOPJ.

Pero este precepto orgánico no se limita a ser simple recordatorio de los principios que deben regir la actividad de Jueces y Magistrados en virtud del derecho fundamental a la protección de datos. Hace algo más, apodera al Consejo General del Poder Judicial para dictar un Reglamento en el que se determinarán los requisitos y demás condiciones que afectan al establecimiento y gestión de los ficheros automatizados que se encuentren bajo responsabilidad de los órganos judiciales de forma que se asegure el cumplimiento de las garantías y derechos establecidos en la legislación de protección de datos de carácter personal. Este apoderamiento aparece además reiterado en el art. 107.10, inciso segundo, de la LOPJ, con la finalidad de asegurar también el cumplimiento de la legislación en materia de protección de datos personales en la elaboración de libros electrónicos de sentencias, recopilación de las mismas, su tratamiento, difusión y certificación, para velar por su integridad, autenticidad y acceso. Serán estas normas jurídicas reglamentarias dictadas por el CGPJ en virtud de los apoderamientos contenidos en el art. 230 y 107.10 de la LOPJ las que modularán y adaptarán el sistema de protección al ámbito judicial, introduciendo mecanismos de garantía específicos y fijando la extensión y límites de los derechos propios de este sistema jurídico -acceso, rectificación, cancelación, etc...- que la legislación general (LOPD) reconoce a los afectados, es decir a todas aquellas persona físicas que sean titulares de los datos que sean objeto de tratamiento en el ámbito de la Administración de Justicia. Es pues el Consejo General del Poder Judicial al que la LOPJ encarga de la función tuitiva en esta materia no

solo por razón del apoderamiento reglamentario al que el art. 230 hace referencia, sino también por tener atribuidas con carácter exclusivo las potestades precisas para el necesario control de la observancia de derechos y garantías, pues solo al órgano de gobierno judicial corresponde la inspección de Juzgados y Tribunales (art. 107.3 LOPJ).

Además, en línea con lo que estamos exponiendo, el contenido del art. 230 cobra pleno sentido si tenemos en cuenta que cuando fue incorporado el precepto en su redacción actual a la LOPJ por la Ley Orgánica 16/1994, de 8 de noviembre, la norma que estaba vigente en materia de protección de datos era la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. (vigente hasta el 14 de enero de 2000), norma que excluía directamente en su Disposición Adicional Primera la aplicación de los Títulos dedicados a la Agencia de Protección de Datos y a las Infracciones y Sanciones respecto de los ficheros automatizados de los que eran titulares las Cortes Generales, el Defensor del Pueblo, el Tribunal de Cuentas, el Consejo General del Poder Judicial y el Tribunal Constitucional, exclusión que se justificaba no solo en el hecho de que se trate de órganos constitucionales diferenciados del Gobierno y de la Administración sino también porque, como poderes del Estado, gozan de una garantía constitucional de independencia respecto del poder ejecutivo, poder público en el que, como ya dijimos, se enmarca orgánica y funcionalmente la Agencia Española de Protección de Datos, aunque lo sea con un estatuto de independencia de su Director respecto del Gobierno. Además, por lo que se refiere en concreto al Consejo General del Poder Judicial y a su ámbito de gobierno, la exclusión del poder de decisión de la Agencia se justificaba entonces -y ahora- por una razón añadida a la ya expuesta, aunque nada se diga en la vigente LOPD, y es que tiene 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 a que se refiere el art. 104 de la LOPJ y que impide cualquier tipo de intromisión o injerencia por parte de una autoridad administrativa.

La existencia de estas limitaciones a las potestades de la Agencia Española de Protección de Datos por razón de la específica naturaleza de órgano susceptible de supervisión no es incompatible con el sistema europeo de protección recogido en la Directiva 95/46/CE, del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, pues ninguno de sus preceptos obliga a la existencia en cada Estado miembro de una sola Autoridad de Control que monopolice o concentre esta función,

encargándose la propia LOPD, que transpone la Directiva, de desmentir todo pretendido monopolio de la Agencia al prever en su texto (art. 41) la coexistencia de varias de ellas en territorio nacional (la estatal y las autonómicas) para supervisar a las propias Administraciones Públicas.

Sirva de complemento argumental a lo que llevamos dicho hasta ahora el propio sistema europeo de supervisión en materia de protección de datos de carácter personal en las instituciones comunitarias. El Reglamento (CE) nº 45/2001, del Parlamento Europeo y del Consejo por el que se crea el Supervisor Europeo de Protección de Datos, al regular sus funciones, establece en el art. 46 que le corresponde supervisar y asegurar la aplicación del Reglamento y de cualquier otro acto comunitario relacionado con la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de una institución u organismo comunitario, con excepción del Tribunal de Justicia de las Comunidades Europeas cuando actúe en el ejercicio de sus funciones jurisdiccionales.

El propio Consejo General del Poder Judicial, con posterioridad a la LOPD, ha ratificado su competencia en esta materia en virtud del apoderamiento del art. 230 LOPJ al aprobar el Reglamento 1/2005, de 15 de septiembre, de los Aspectos Accesorios de las Actuaciones Judiciales. Este Reglamento dedica su Título V, en desarrollo del art. 230 de la LOPJ, a regular el establecimiento y gestión de los ficheros automatizados bajo responsabilidad de los órganos judiciales, comprendiendo tanto los ficheros de datos automatizados de carácter personal dependientes de los Juzgados y Tribunales como los del Consejo General del Poder Judicial, e incluyendo también en su ámbito tanto los ficheros jurisdiccionales (aquellos que incorporan datos de carácter personal que deriven de actuaciones jurisdiccionales), como los ficheros no jurisdiccionales o gubernativos (aquellos que incorporan datos de carácter personal que deriven de los procedimientos gubernativos así como los que, con arreglo a las normas administrativas aplicables, sean definitivos de la relación funcional o laboral de las personas destinadas en tales órganos y de las situaciones e incidencias que en ella acontezcan) y a todos ellos sitúa bajo el control del Consejo General del Poder Judicial con sujeción a un régimen específico de tutela ante los órganos de gobierno interno, mediante la articulación del correspondiente sistema de reclamaciones y recursos, en cuanto al ejercicio de los derechos de acceso, rectificación y cancelación. Régimen de protección del que es ajeno la Agencia Española de Protección de Datos, a la que no se reconoce facultades de intervención, correspondiendo éstas a los órganos de gobierno judicial.”

Posteriormente, la Ley Orgánica 7/2015, de 21 de julio, por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, procedió a la

regulación de la protección de datos en el ámbito de los Tribunales, que carecía hasta entonces de una regulación completa y actualizada, introduciendo un nuevo capítulo I bis en el título III del libro III, que comprende los artículos 236 bis a 236 decies. Como señala su preámbulo “El modelo distingue con claridad entre ficheros jurisdiccionales y los no jurisdiccionales. De esta forma, el responsable de los ficheros jurisdiccionales es el órgano jurisdiccional y éstos se rigen por las leyes procesales en cuanto a los derechos ARCO –acceso, rectificación, cancelación y oposición–. La autoridad de control de tales ficheros será el Consejo General del Poder Judicial. Por otro lado, el responsable de los ficheros no jurisdiccionales es la Oficina judicial, al frente de la cual está un Letrado de la Administración de Justicia. Ese tipo de ficheros se regirán por la normativa existente en materia de protección de datos de carácter personal y la autoridad de control de estos ficheros será la Agencia Española de Protección de Datos”.

En el momento actual, a la necesidad de preservar la independencia de los jueces en el ejercicio de sus funciones jurisdiccionales se refiere específicamente el Considerando 20 del RGPD:

[...] A fin de preservar la independencia del poder judicial en el desempeño de sus funciones, incluida la toma de decisiones, la competencia de las autoridades de control no debe abarcar el tratamiento de datos personales cuando los tribunales actúen en ejercicio de su función judicial. El control de esas operaciones de tratamiento de datos ha de poder encomendarse a organismos específicos establecidos dentro del sistema judicial del Estado miembro, los cuales deben, en particular, garantizar el cumplimiento de las normas del presente Reglamento, concienciar más a los miembros del poder judicial acerca de sus obligaciones en virtud de este y atender las reclamaciones en relación con tales operaciones de tratamiento de datos.

Consecuentemente, el artículo 55.3. del RGPD dispone expresamente que “Las autoridades de control no serán competentes para controlar las operaciones de tratamiento efectuadas por los tribunales en el ejercicio de su función judicial”, previendo el artículo 44.3 de la LOPDGDD que “La Agencia Española de Protección de Datos y el Consejo General del Poder Judicial colaborarán en aras del adecuado ejercicio de las respectivas competencias que la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia”, habiéndose suscrito el 6 de julio de 2017 el “Convenio de colaboración entre el Consejo General del Poder Judicial y la Agencia Española de Protección de Datos sobre colaboración en el ejercicio de las funciones propias de las autoridades de control en materia de protección de datos”.

En relación con los tratamientos en el ámbito penal, se pronuncia en idéntico sentido el Considerando 80 de la Directiva 2016/680:

Aunque la presente Directiva también se aplica a las actividades de los órganos jurisdiccionales nacionales y otras autoridades judiciales, la competencia de las autoridades de control no debe abarcar el tratamiento de datos personales cuando los órganos jurisdiccionales actúen en ejercicio de su función jurisdiccional, con el fin de garantizar la independencia de los jueces en el desempeño de sus funciones. Esta excepción debe limitarse a actividades judiciales en juicios y no debe aplicarse a otras actividades en las que puedan estar implicados los jueces, de conformidad con el Derecho del Estado miembro. Los Estados miembros pueden disponer también que la competencia de la autoridad de control no abarque el tratamiento de datos personales realizado por otras autoridades judiciales independientes en el ejercicio de su función jurisdiccional, por ejemplo la fiscalía. En todo caso, el cumplimiento de las normas de la presente Directiva por los órganos jurisdiccionales y otras autoridades judiciales independientes debe estar sujeto siempre a una supervisión independiente de conformidad con el artículo 8, apartado 3, de la Carta.

Y el artículo 45.2. de la misma dispone que “Los Estados miembros dispondrán que cada autoridad de control no sea competente para controlar las operaciones de tratamiento efectuadas por los órganos jurisdiccionales en el ejercicio de su función judicial. Los Estados miembros podrán disponer que su autoridad de control no sea competente para controlar las operaciones de tratamiento efectuadas por otras autoridades judiciales independientes en el ejercicio de su función judicial”.

Recientemente, la Ley Orgánica 7/2021 ha dado nueva redacción a los artículos de la LOPJ dedicados a la protección de datos personales, para adecuarlos a las modificaciones introducidas por la misma, destacando, entre sus novedades, la creación de una autoridad de control específica en el ámbito de la fiscalía, modificando en su disposición final primera bis la Ley 50/1981, de 30 de diciembre, reguladora del Estatuto Orgánico del Ministerio Fiscal:

Uno. Se modifica el artículo 12 para incluir en nuevo apartado n) con la siguiente redacción:

«n) La Unidad de Supervisión y Control de Protección de Datos.»

Dos. Se modifica el artículo 20 incluyendo un nuevo apartado Cuatro con la siguiente redacción:

«Cuatro. En la Fiscalía General del Estado, de igual modo, existirá la Unidad de Supervisión y Control de Protección de Datos que ejercerá las competencias que corresponden a la autoridad de protección de datos con fines jurisdiccionales sobre el tratamiento de los mismos realizado por el Ministerio Fiscal, de acuerdo con lo establecido en el artículo 236 octies de la Ley Orgánica del Poder Judicial en el ámbito de

sus competencias y facultades. Su regulación se remitirá a los términos previstos en la Ley Orgánica del Poder Judicial en cuanto le sea de aplicación.

Y, en cuanto a las modificaciones que introduce en la LOPJ en su disposición final primera ter interesan, en este momento, destacar las siguientes:

Seis. El artículo 236 ter queda redactado como sigue:

«Artículo 236 ter.

1. El tratamiento de los datos personales llevado a cabo **con ocasión de la tramitación por los órganos judiciales y fiscalías de los procesos de los que sean competentes**, así como el realizado dentro de la gestión de la Oficina judicial y fiscal, se regirá por lo dispuesto en el Reglamento (UE) 2016/679, la Ley Orgánica 3/2018 y su normativa de desarrollo, sin perjuicio de las especialidades establecidas en el presente Capítulo y en las leyes procesales.

2. En el **ámbito de la jurisdicción penal**, el tratamiento de los datos personales llevado a cabo con ocasión de la tramitación por los órganos judiciales y fiscalías de los procesos, diligencias o expedientes de los que sean competentes, así como el realizado dentro de la gestión de la Oficina judicial y fiscal, se regirá por lo dispuesto en la Ley Orgánica de protección de datos personales tratados con fines de prevención, detección, investigación o enjuiciamiento de infracciones penales y de ejecución de sanciones penales, sin perjuicio de las especialidades establecidas en el presente Capítulo y en las leyes procesales y, en su caso, en la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal.

3. No será necesario el consentimiento del interesado para que se proceda al tratamiento de los datos personales **en el ejercicio de la actividad jurisdiccional**, ya sean estos facilitados por las partes o recabados a solicitud de los órganos competentes, sin perjuicio de lo dispuesto en las normas procesales para la validez de la prueba.»

Siete. El artículo 236 quáter queda redactado como sigue:

«Artículo 236 quater.

Cuando se proceda al tratamiento con **finés no jurisdiccionales** se estará a lo dispuesto en el Reglamento (UE) 2016/679, la Ley Orgánica 3/2018 y su normativa de desarrollo.»

Ocho. El artículo 236 quinquies queda redactado como sigue:

«Artículo 236 quinquies.

1. Las resoluciones y actuaciones procesales deberán contener los datos personales que sean adecuados, pertinentes y limitados a lo

necesario en relación con los fines para los que son tratados, en especial para garantizar el derecho a la tutela judicial efectiva, sin que, en ningún caso, pueda producirse indefensión.

2. Los Jueces y Magistrados, los Fiscales y los Letrados de la Administración de Justicia, conforme a sus competencias, podrán adoptar las medidas que sean necesarias para la supresión de los datos personales de las resoluciones y de los documentos a los que puedan acceder las partes durante la tramitación del proceso siempre que no sean necesarios para garantizar el derecho a la tutela judicial efectiva, sin que, en ningún caso, pueda producirse indefensión.

3. Los datos personales que las partes conocen a través del proceso deberán ser tratados por estas de conformidad con la normativa general de protección de datos. Esta obligación también incumbe a los profesionales que representan y asisten a las partes, así como a cualquier otro que intervenga en el procedimiento.

4. **Se deberán comunicar a los órganos competentes dependientes del Consejo General del Poder Judicial, de la Fiscalía General del Estado y del Ministerio de Justicia, en lo que proceda, los datos tratados con fines jurisdiccionales que sean estrictamente necesarios para el ejercicio de las funciones de inspección y control establecidas en esta Ley, y su normativa de desarrollo.** También se deberán facilitar los datos tratados con fines no jurisdiccionales cuando ello esté justificado por la interposición de un recurso o sea necesario para el ejercicio de las competencias que tengan legalmente atribuidas.

5. Las Oficinas de Comunicación establecidas en esta Ley, en el ejercicio de sus funciones de comunicación institucional, deberán velar por el respeto del derecho fundamental a la protección de datos personales de aquellos que hubieran intervenido en el procedimiento de que se trate. Para cumplir con su finalidad, podrán recabar los datos necesarios de las autoridades competentes.

6. Los Letrados de la Administración de Justicia deberán facilitar a la Abogacía del Estado los datos personales, la información y los documentos que sean requeridos para el desempeño de la representación y defensa del Reino de España ante el Tribunal Europeo de Derechos Humanos y otros órganos internacionales en materia de protección de derechos Humanos, en particular ante el Comité de Naciones Unidas. A tales efectos, se establecerán igualmente los mecanismos de comunicación con la Fiscalía General del Estado, a través de sus unidades competentes.»

Nueve. El artículo 236 sexies queda redactado como sigue:
«Artículo 236 sexies.

1. La Administración competente deberá suministrar los medios tecnológicos adecuados para que se proceda al tratamiento de los datos personales conforme a las disposiciones legales y reglamentarias.

2. La Administración competente deberá cumplir con las responsabilidades que en materia de tratamiento y protección de datos personales se le atribuya como administración prestacional.

3. Se deberán adoptar las medidas organizativas adecuadas para que la Oficina judicial y fiscal realice un adecuado tratamiento de los datos personales. Previo informe del Consejo General del Poder judicial, y, en su caso, de la Fiscalía General del Estado, el Ministerio de Justicia deberá elaborar y actualizar los códigos de conducta destinados a contribuir a la correcta aplicación de la normativa de protección de datos personales en la Oficina judicial y fiscal, adecuando los principios de la normativa general a los propios de la regulación procesal y organización de la Oficina judicial y fiscal.

4. El Ministerio de Justicia y las Comunidades Autónomas con competencias en la materia, dentro de las políticas de apoyo a la Administración de Justicia y desarrollo de la gestión electrónica de los procedimientos, podrán realizar el tratamiento de datos no personales para el ejercicio de sus competencias de gestión pública, incluyendo el desarrollo e implementación de sistemas automáticos de clasificación documental orientados a la tramitación procesal, con cumplimiento de la normativa de interoperabilidad, seguridad y protección de datos que resulte aplicable.»

Diez. El artículo 236 septies queda redactado como sigue:

«Artículo 236 septies.

1. En relación con el tratamiento de los datos personales con fines jurisdiccionales, los derechos de información, acceso, rectificación, supresión, oposición y limitación se tramitarán conforme a las normas que resulten de aplicación al proceso en que los datos fueron recabados, Estos derechos deberán ejercitarse ante los órganos judiciales, fiscalías u Oficina judicial en los que se tramita el procedimiento, y las peticiones deberán resolverse por quien tenga la competencia atribuida en la normativa orgánica y procesal.

2. En todo caso se denegará el acceso a los datos objeto de tratamiento con fines jurisdiccionales cuando las diligencias procesales en que se haya recabado la información sean o hayan sido declaradas secretas o reservadas,

3. En relación con el tratamiento de los datos personales con fines no jurisdiccionales, los interesados podrán ejercitar los derechos de información, acceso, rectificación, supresión, oposición y limitación en los términos establecidos en la normativa general de protección de datos.»

Once. El artículo 236 octies queda redactado como sigue:

«Artículo 236 octies.

1. Respecto a las operaciones de tratamiento efectuadas con fines jurisdiccionales por los Juzgados, Tribunales, Fiscalías, y las Oficinas judicial y fiscal, corresponderán al Consejo General del Poder Judicial y a la Fiscalía General del Estado, en el ámbito de sus respectivas competencias, las siguientes funciones:

a) Supervisar el cumplimiento de la normativa de protección de datos personales mediante el ejercicio de la labor inspectora otorgada en la presente Ley y el Estatuto Orgánico del Ministerio Fiscal.

b) Promover la sensibilización de los profesionales de la Administración de Justicia y su comprensión de los riesgos, normas, garantías, derechos y obligaciones en relación con el tratamiento.

c) Emitir informe sobre los códigos de conducta destinados a contribuir a la correcta aplicación de la normativa de protección de datos personales en la Oficina judicial y fiscal.

d) Previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos en materia de protección de datos.

e) Tramitar y responder las reclamaciones presentadas por un interesado o por asociaciones, organizaciones y entidades que tengan capacidad procesal o legitimación para defender intereses colectivos, en los términos que determinen las leyes de aplicación al proceso en que los datos fueron recabados. Se informará al reclamante sobre el curso y resultado de la reclamación en un plazo razonable, previa realización de la investigación oportuna si se considera necesario.

2. Los tratamientos de datos con fines no jurisdiccionales estarán sometidos a la competencia de la Agencia Española de Protección de Datos, que también supervisará el cumplimiento de aquellos tratamientos que no sean competencia de las autoridades indicadas en el apartado anterior.

3. El Consejo General del Poder Judicial, la Fiscalía General del Estado y la Agencia Española de Protección de Datos colaborarán en aras del adecuado ejercicio de las respectivas competencias que la presente Ley Orgánica les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia.

4. Cuando con ocasión de la realización de actuaciones de investigación relacionadas con la posible comisión de una infracción de la normativa de protección de datos, las autoridades competentes a las que se refieran los apartados anteriores apreciaran la existencia de indicios que supongan la competencia de otra autoridad, darán inmediatamente traslado a esta última a fin de que prosiga con la tramitación del procedimiento.»

Doce. El artículo 236 nonies, queda redactado como sigue:

«Artículo 236 nonies.

1. Las competencias que corresponden a la autoridad de protección de datos personales con fines jurisdiccionales serán ejercidas respecto del tratamiento de los mismos realizado por Juzgados y Tribunales de acuerdo con lo establecido en el artículo 236 octies, por la Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial.

2. Al frente de la Dirección de Supervisión y Control de Protección de Datos se nombrará por mayoría absoluta del Pleno del Consejo General del Poder Judicial una persona titular de la Dirección, de entre juristas de reconocida competencia con al menos quince años de ejercicio profesional y con conocimientos y experiencia acreditados en materia de protección de datos.

3. La duración del mandato de la persona titular de la Dirección de Supervisión y Control de Protección de Datos será de cinco años, no renovable. Durante su mandato permanecerá, en su caso, en situación de servicios especiales y ejercerá exclusivamente las funciones inherentes a su cargo. Solo podrá ser cesada por incapacidad o incumplimiento grave de sus deberes, apreciados por el Pleno mediante mayoría absoluta.

4. El régimen de incompatibilidades de la persona titular de la Dirección de Supervisión y Control de Protección de Datos será el mismo que el establecido para los Magistrados al servicio de los órganos técnicos del Consejo General del Poder Judicial. La persona titular de la Dirección de Supervisión y Control de Protección de Datos deberá ejercer sus funciones con absoluta independencia y neutralidad.

5. La persona titular y el resto de personal adscrito a la Dirección de Supervisión y Control de Protección de Datos estarán sujetos al deber de secreto profesional, tanto durante su mandato como después del mismo, con relación a las informaciones confidenciales de las que hayan tenido conocimiento en el cumplimiento de sus funciones o el ejercicio de sus atribuciones. Este deber de secreto profesional se aplicará en particular a la información que faciliten las personas físicas a la Dirección de Supervisión y Control de Protección de Datos en materia de infracciones de la presente normativa.

6. La composición, organización y funcionamiento de la Dirección de Supervisión y Control de Protección de Datos será regulada reglamentariamente. El Consejo General del Poder Judicial deberá velar porque la Dirección cuente, en todo caso, con todos los medios personales y materiales necesarios para el adecuado ejercicio de sus funciones.»

Trece. El artículo 236 decies, queda redactado como sigue:

«Artículo 236 decies.

1. Los tratamientos de datos llevados a cabo por el Consejo General del Poder judicial y la Fiscalía General del Estado en el

ejercicio de sus competencias quedarán sometidos a lo dispuesto en la legislación vigente en materia de protección de datos personales. Dichos tratamientos no serán considerados en ningún caso realizados con fines jurisdiccionales.

2. Las operaciones de tratamiento de datos personales del Consejo General del Poder Judicial y de los órganos integrantes del mismo serán autorizados por acuerdo del Consejo General del Poder Judicial, a propuesta de la Secretaría General, que ostentará la condición de responsable del tratamiento respecto de los mismos.

3. Las operaciones de tratamiento de datos personales de la Fiscalía General del Estado serán autorizadas según determine el Estatuto Orgánico del Ministerio Fiscal y las Instrucciones que se dicten al respecto.»

Por consiguiente, las competencias de esta Agencia quedan limitadas, en cuanto a los tratamientos de datos llevados a cabo por los Juzgados, Tribunales y Fiscalía, a los que se realicen con fines no jurisdiccionales, por lo que siendo la parte principal del anteproyecto la modificación de la normativa procesal, la competencia para informar el texto remitido corresponde, en cuanto autoridad de control, al Consejo General del Poder Judicial y, en su caso, a la Unidad de Supervisión y Control de Protección de Datos que se cree en la Fiscalía General del Estado.

III

En el ámbito de las competencias de esta Agencia, interesa destacar, en primer lugar, que el mismo comprende los tratamientos de datos personales que se realicen a través de los medios adecuados de solución de controversias en vía no jurisdiccional a que se refiere el Título I del Anteproyecto, incluido el supuesto en que las actuaciones se desarrollen por medios telemáticos contemplado en el artículo 5, estableciendo un deber de confidencialidad y secreto profesional en su artículo 6.

Los tratamientos de datos personales necesarios para el desarrollo de las diferentes modalidades de negociación que el Anteproyecto contempla quedan sujetos a las previsiones contenidas en el RGPD y en la LOPDGDD, por lo que **sería conveniente introducir una disposición en el Título I que haga referencia a la necesidad de cumplir con la normativa sobre protección de datos personales, sugiriendo esta Agencia la siguiente redacción:**

Los tratamientos de datos de carácter personal de las personas físicas se realizarán con estricta sujeción a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, 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 y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

IV

Por otro lado, el anteproyecto pretende acelerar la adaptación de la legislación española a las nuevas realidades, en lo concerniente a la implementación de nuevas tecnologías de la información y la comunicación en el servicio público de Justicia, mediante la modificación de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

En cuanto a las modificaciones que propone el texto remitido, se introducen, en primer término, los cambios mínimos necesarios para adaptar nuestra legislación al marco regulatorio establecido por el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento eIDAS), incluyendo la referencia a los sistemas de identificación y autenticación mediante remisión directa a sus homólogos de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. En este sentido, la Ley 39/2015 regula en su artículo 9 los sistemas de identificación y en el artículo 10 los sistemas de firma, estableciendo garantías adicionales, por lo que la remisión a los mismos se estima adecuada desde la perspectiva de la protección de datos de carácter personal.

Por otro lado, se introducen modificaciones que permiten generalizar la celebración de vistas y otro tipo de declaraciones a través de videoconferencias, evitando, en la medida de lo posible, el desplazamiento de los ciudadanos y profesionales, así como la concentración de personas en las oficinas judiciales. De este modo, solo se acudirá al auxilio judicial cuando no sea posible la práctica de una actuación por medio de videoconferencia, ello con las garantías y exclusiones que se contemplan. Asimismo, se introducen modificaciones relativas a la práctica de actos de comunicación, de modo que los únicos que no están obligados a comunicarse electrónicamente con la Administración de Justicia son las personas físicas que no se hayan obligado previa y contractualmente a hacerlo o que no hayan optado voluntariamente por comunicarse en dicha forma, exceptuándose la obligación contractual en determinados supuestos. Asimismo, se facilita la notificación a las personas jurídicas y otras entidades en la Dirección Electrónica Habilitada (DEH).

Esta Agencia ha tenido ocasión de pronunciarse en relación con el uso de las tecnologías de la información y la comunicación en la Administración de

Justicia en distintas ocasiones, como el informe 330/2012, relativo al Proyecto de Real Decreto de creación del Comité Técnico Estatal de la Administración Judicial Electrónica (Real Decreto 396/2013, de 7 de junio, por el que se regula el Comité técnico estatal de la Administración judicial electrónica), el informe 210/2015, referente al borrador de Real Decreto sobre comunicaciones telemáticas en la Administración de Justicia (Real Decreto 1065/2015, de 27 de noviembre) o el informe de 11 de mayo de 2015, referido al Proyecto de Orden de creación de la Sede Judicial Electrónica correspondiente al ámbito territorial del Ministerio de Justicia.

A este respecto, debe partirse de que la Ley 18/2011 incluye determinadas previsiones dirigidas a garantizar la observancia de la normativa sobre protección de datos personales. En este sentido, el artículo 4, referido a los derechos de los ciudadanos, incluye entre los mismos, En el apartado 2, letra g), el derecho “A la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de la Administración de Justicia en los términos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales”, y el artículo 6, referido a los derechos y deberes de los profesionales del ámbito de la justicia, incluye entre sus derechos, en el apartado 2, letra e) el derecho “A la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de la Administración de Justicia en los términos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales”.

En el momento actual, tal y como se ha señalado anteriormente, la normativa vigente en materia de protección de datos de carácter personal es el RGPD, que goza de efecto directo, complementado por la LOPDGGDD, que ha derogado expresamente la Ley Orgánica 15/1999, y en el ámbito penal, por la reciente Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, que ha procedido a la transposición de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Por tanto, deberían realizarse las modificaciones oportunas en dichos preceptos, así como en cualesquiera otros que remitan a la Ley Orgánica 15/1999, para adaptarlos a la normativa vigente. Asimismo, hay que tener en cuenta que la protección otorgada por dichas normas es mucho más amplia que lo referente a la seguridad y confidencialidad de la información, que es solo una de las garantías que contempla dicha normativa (en virtud del principio de «integridad

y confidencialidad» recogido en el artículo 5.1.f) del RGPD), por lo que debería sustituirse dicha referencia por un reconocimiento genérico del derecho a la protección de datos personales, del que la seguridad y confidencialidad son dos garantías, pero siendo preciso tener en cuenta el necesario respeto a los restantes principios y derechos establecidos en dicha normativa para el tratamiento de datos personales.

Por ello, se propone la siguiente redacción de la letra d), apartado 2 del artículo 4 y de la letra e) apartado 2 del artículo 6:

“A la protección de datos de carácter personal y, en particular, a la seguridad y confidencialidad de los datos que sean objeto de tratamiento por la Administración de Justicia, en los términos establecidos en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales.”

Por otro lado, debe hacerse especial referencia a las medidas de seguridad que deben adoptarse para salvaguardar el derecho a la protección de datos, al no existir ya, a diferencia de lo que ocurría en el momento de aprobación de la Ley 18/2011, un elenco cerrado de las mismas establecido por la legislación de protección de datos.

En este punto, hay que tener en cuenta que el RGPD ha supuesto un cambio de paradigma al abordar la regulación del derecho a la protección de datos personales, que pasa a fundamentarse en el principio de «accountability» o «responsabilidad proactiva» tal y como ha señalado reiteradamente la AEPD (Informe 17/2019, entre otros muchos) y se recoge en la Exposición de motivos de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD): “la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan”. Dentro de este nuevo sistema, es el responsable del tratamiento el que, a través de los instrumentos regulados en el propio RGPD como el registro de actividades del tratamiento, el

análisis de riesgos o la evaluación de impacto en la protección de datos personales, debe garantizar la protección de dicho derecho mediante el cumplimiento de todos los principios recogidos en el artículo 5.1 del RGPD, documentando adecuadamente todas las decisiones que adopte al objeto de poder demostrarlo.

Así, el artículo 24.1 del Reglamento General de Protección de Datos dispone que “Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario”.

Esta previsión se completa con lo señalado en el considerando 75 del Reglamento, según el cual “Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados”.

A su vez, en relación con la seguridad de los datos personales, el artículo 32.1 establece que “Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo”.

De lo que acaba de indicarse se desprenden que la evolución del modelo desde la lista de cumplimiento a la responsabilidad activa impone la necesidad de realizar un análisis de riesgos en materia de protección de datos y, en su caso una evaluación de impacto en la misma, sin que sea suficiente una mera remisión a las normas de protección de datos, habida cuenta que éstas ya no establecen un modelo tasado de cumplimiento.

Particularmente relevante sería la adopción de las medidas tendentes a garantizar la protección del derecho fundamental a la protección de datos personales, incluida su seguridad, en la configuración de los registros, archivos y las transmisiones de datos personales por videoconferencia o por cualquier otro medio.

Por ello debería hacerse constar expresamente en alguno de los preceptos que regulan el Esquema judicial de interoperabilidad y seguridad, por ejemplo, en el artículo 47 de la Ley 18/2011, que, previo análisis de los riesgos para los derechos y libertades de las personas físicas, se incorporarán las medidas técnicas y organizativas destinadas a garantizar y poder demostrar que el tratamiento es conforme con la normativa de protección de datos personales, que serán revisadas y actualizadas cuando sea necesario.

Asimismo, dicha previsión debería incorporarse, igualmente, en la nueva redacción que el anteproyecto da al artículo 53 de la Ley 18/2011, relativo a los elementos básicos de la seguridad judicial electrónica. Además, debería clarificarse en dicho precepto que las medidas a implantar como consecuencia del citado análisis de riesgos, en caso de resultar agravadas respecto de las previstas en el Esquema judicial de interoperabilidad y seguridad, deberían prevalecer sobre éstas últimas, a fin de dar adecuado cumplimiento a lo exigido por el Reglamento General de Protección de Datos. E incluir, en su apartado 2, relativo a las dimensiones de la seguridad judicial electrónica, la protección de datos de carácter personal.

Y en el artículo 29, referido al Archivo electrónico de documentos y expedientes, en el cuarto párrafo de su apartado 1, incluir la referencia a la normativa sobre protección de datos personales

V

Por último, se aborda la regulación del registro electrónico de apoderamientos judiciales apud acta, dependiente del Ministerio de Justicia, que sustituye a los que estaban previstos en la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, y que debían existir en cada una de las oficinas

judiciales con funciones de registro, o incluso los que se podían haber creado en cualquiera de las otras oficinas judiciales. Esta reforma, junto con la modificación relativa a las formas de identificación y autenticación llevadas a cabo en esta ley, permitirá que el otorgamiento de poderes apud acta se lleve a cabo en gran medida a través de medios telemáticos sin necesidad de desplazamiento de los ciudadanos a las sedes judiciales.

Por las razones expuestas anteriormente, en la nueva redacción que se da al artículo 32 bis debería recogerse que en el registro electrónico de apoderamientos judiciales, previo análisis de los riesgos para los derechos y libertades de las personas físicas, se incorporarán las medidas técnicas y organizativas destinadas a garantizar y poder demostrar que el tratamiento es conforme con la normativa de protección de datos personales, que serán revisadas y actualizadas cuando sea necesario.

Por otro lado, el citado registro permitirá comprobar válidamente la representación que ostentan quienes actúen ante la Administración de Justicia en nombre de un tercero, pero sin hacer referencia a la forma en la que se realizará dicha comprobación. A este respecto, procede traer a colación lo señalado por esta Agencia en el informe 4/2021, referente al Proyecto de Orden por la que se regula el Registro electrónico de apoderamientos en el ámbito de la Administración General del Estado:

IV

El artículo 10 regula las consultas de los órganos y organismos públicos:

El REA-AGE ofrecerá a los organismos interesados las siguientes vías de acceso a la información:

a) Descarga, bajo petición, de un fichero, que contendrá todos los apoderamientos vigentes y válidos para los trámites y actuaciones por medios electrónicos de los que el órgano administrativo petionario sea competente. El fichero contendrá todos los datos de los apoderamientos que se enumeran en el artículo 3 de esta Orden.

b) Acceso en línea mediante servicios web, a los efectos de comprobar, automáticamente y en tiempo real desde las aplicaciones, que un apoderamiento está vigente. Las peticiones al REA-AGE, relativas a los apoderamientos vigentes y válidos para los procedimientos y trámites por medios electrónicos de las que el órgano administrativo petionario sea competente, se enviarán por un canal seguro de comunicaciones y deberán firmarse con firma electrónica avanzada cualificada o sello electrónico cualificado del citado órgano o

administración de adscripción. La aplicación de soporte al Registro mantendrá trazabilidad de todas las peticiones recibidas.

Dicho precepto mantiene las dos posibilidades de acceso previstas en el artículo 11 de la Orden HAP/1637/2012, de 5 de julio, por la que se regula el Registro Electrónico de Apoderamientos. No obstante, esta Agencia considera que, de acuerdo con los principios recogidos en el artículo 5 del RGPD, el mantenimiento de ambas posibilidades resulta excesivo e incrementa los riesgos derivados del tratamiento de datos personales.

En primer lugar, la descarga del fichero procede solo en los casos en los que así se solicite, por lo que en otro caso debería acudir al acceso en línea previsto en la letra b). Además, no se establece la periodicidad con la que debe realizarse dicha descarga, lo que plantea el problema de dar cumplimiento al principio de exactitud de los datos previsto en la letra d) del artículo 5.1. del RGPD, de acuerdo con el cual los datos personales serán “exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan”. Por ello, pese a la descarga del archivo, y salvo que la misma se realizara de una manera prácticamente constante a fin de acreditar la vigencia de los poderes o las posibles rectificaciones realizadas en los datos de carácter personal, seguiría siendo necesario acudir al acceso en línea, para el cual, además, se han previsto unas garantías adicionales que no se establecen en el supuesto de descarga del fichero.

Por otro lado, la descarga del fichero va a permitir a los órganos y organismos de la Administración General del Estado y de otras administraciones que se adhieran al mismo acceder a todos los datos personales obrantes en el fichero, en la medida en que se refieran a trámites y actuaciones por medios electrónicos de los que el órgano administrativo peticionario sea competente, independientemente de que se correspondan con la tramitación de un procedimiento concreto, lo que sería excesivo y contrario al principio de minimización de datos, así como a la doctrina establecida por el Tribunal Constitucional contraria a los accesos masivos e indiscriminados a datos personales, recogida, entre otras, en su sentencia del Tribunal Constitucional 17/2013, de 31 de enero.

Por todo ello, la descarga del fichero supondría un acceso masivo a datos personales que, además, no excluye la necesidad de acudir al acceso en línea para verificar la vigencia del poder siendo, por tanto, contraria al principio de minimización de datos y al principio de

proporcionalidad, en la medida en que exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad, recogido, entre otras, en la sentencia del Tribunal Constitucional 14/2003, de 28 de enero.

Por consiguiente, esta Agencia que el procedimiento de acceso a los datos personales obrantes en el Registro que mejor se adecúa a la normativa sobre protección de datos personales es el contemplado en la letra b, el acceso en línea, para el cual el precepto establece unas garantías adicionales, sin perjuicio del resto de garantías que deban adoptarse conforme a lo que se señalará en el apartado siguiente. No obstante, también en este supuesto se deberán adoptar las medidas técnicas y organizativas que garanticen el cumplimiento del citado principio de minimización, de modo que se acceda a los datos estrictamente necesarios para verificar la existencia, vigencia y alcance del poder en relación con la concreta actuación administrativa que se pretende realizar y para poder comunicarse con el representante.

Todo ello sin perjuicio de que deban arbitrarse otras medidas que permitan, respetando igualmente el citado principio de minimización, acceder a los datos en los casos de fallo del sistema y siempre que, por razones de urgencia, no pueda esperarse al restablecimiento del mismo, debiendo preverse las garantías oportunas.

Teniendo en cuenta que, de acuerdo con la doctrina constitucional (sentencias 292/2000 y 76/2019), la ley que limita el derecho fundamental a la protección de datos personales debe prever las garantías oportunas, se estima conveniente que en dicho precepto se haga referencia a la forma en la que se podrá consultar el mismo, teniendo en cuenta lo señalado por esta Agencia y evitando, en todo caso, un acceso masivo e indiscriminado a los datos personales.

Por último, atendiendo igualmente al principio de minimización de datos, debe hacerse referencia a la nueva regulación que se contiene en el apartado 3 del artículo 32 bis respecto de los datos personales que deben figurar en el registro, a diferencia de la regulación actual, incluye entre los mismos el teléfono fijo y /o móvil y dirección de correo electrónico del poderdante y del apoderado, “en su caso”.

En ambos supuestos, si se trata de personas físicas, y por aplicación del citado principio, únicamente sería admisible su aportación si los mismos resultan necesarios atendiendo a la finalidad perseguida por la norma. Teniendo en cuenta que dicha finalidad es la comprobación de la representación, y no facilitar el contacto con el poderdante o el apoderado, se considera que el número de teléfono de las personas físicas no es un dato necesario para la finalidad del registro, del mismo modo que tampoco lo es el

dato del correo electrónico cuando el poderdante es una persona física que no esté obligada a relacionarse por medios electrónicos. Por tanto, la aportación del número de teléfono y el correo electrónico, en los supuestos indicados, debería ser optativa y su falta de cumplimentación no impedir la inscripción.