



Doi: <https://doi.org/10.17398/2695-7728.40.485>

EL TRATAMIENTO DE DATOS PERSONALES CON FINES  
JURISDICCIONALES Y EL EJERCICIO DEL DERECHO DE  
AUTODETERMINACIÓN INFORMATIVA «HABEAS DATA»

*THE PROCESSING OF PERSONAL DATA FOR JURISDICTIONAL  
PURPOSES AND THE EXERCISE OF THE RIGHT TO  
INFORMATIONAL SELF-DETERMINATION «HABEAS DATA»*

**MATI DE LOS ÁNGELES HERNÁNDEZ ALFARO**

*Universidad Pontificia Comillas*

Recibido: 30/10/2024      Aceptado: 20/11/2024

RESUMEN

El ejercicio de la potestad jurisdiccional exige la adecuada ponderación entre el principio de publicidad del proceso y la protección de los datos personales de todos los implicados en el procedimiento judicial. En el presente trabajo se analiza el marco normativo que rige la actividad jurisdiccional en esta materia y las dificultades prácticas que genera su escasa regulación de cara a la efectiva protección de los derechos de los interesados.

*Palabras clave:* Protección de datos personales, jurisdicción, habeas data, autoridad de control, responsable de tratamiento.

ABSTRACT

*The exercise of jurisdictional power requires an appropriate balance between the principle of publicity of the process and the protection of the personal data of those involved in the judicial procedure. This paper analyzes the regulatory framework*

*governing the jurisdictional activity in this area and the practical difficulties generated by its scarce regulation with a view to the effective protection of the rights of the interested parties.*

*Keywords: personal data protection, jurisdiction, habeas data, supervisory authority, data controller.*

*Sumario: I. Introducción. II. El tratamiento jurisdiccional de datos personales, 2.1. Marco normativo del tratamiento de datos personales en el ámbito judicial, 2.2. El tratamiento de datos personales por la Administración de Justicia: tratamientos con fines jurisdiccionales y no jurisdiccionales, 2.3. Los datos objeto de tratamiento en el ámbito jurisdiccional, 2.4. La autoridad de control y sus funciones en el tratamiento de datos personales en el ámbito jurisdiccional, 2.5. El responsable de tratamiento de los datos con fines jurisdiccionales. III. Algunas especialidades en materia de tratamiento de datos personales con fines jurisdiccionales en el procedimiento penal. IV. El ejercicio de los derechos de información, acceso, rectificación, supresión, oposición y limitación «habeas data» cuando se produzca el tratamiento de datos personales con fines jurisdiccionales. V. Conclusiones. VI. Bibliografía.*

## I. INTRODUCCIÓN

Los procedimientos judiciales producen una importante cantidad de documentación en la que se recoge información relativa a las circunstancias personales de los ciudadanos inmersos en el proceso, tanto de quienes litigan como de los profesionales que de una u otra forma intervienen en el procedimiento (abogados, peritos, jueces, fiscales etc.), o de los terceros llamados a colaborar con la administración de justicia (*vgr.* los testigos). Los titulares de datos personales obtenidos en el ejercicio de la función jurisdiccional conservan los mismos derechos y facultades que la Constitución española (en adelante, CE)<sup>1</sup> y la Ley les reconoce a todos los ciudadanos, aunque, como se explica en el presente trabajo, esa protección debe adaptarse a ciertas especialidades que vienen determinadas por la propia organización y las normas que afectan a la esfera de la Administración de Justicia.

---

<sup>1</sup> BOE núm. 311, de 29 de diciembre de 1978.

Por ello, si bien, se reconoce a los jueces y tribunales el ejercicio de la potestad jurisdiccional, este ejercicio debe realizarse de modo que se asegure a los ciudadanos la tutela efectiva de sus derechos, tales como el derecho al honor, a la intimidad y a la propia imagen, a la vez que se cumple con el principio de publicidad del proceso<sup>2</sup>. Así, con el ánimo de evitar posibles desafueros, se ha desarrollado un sistema jurisdiccional con una serie de límites y garantías, entre los que destaca el principio de legalidad, que persigue reducir al máximo el arbitrio de los jueces en el ejercicio de la tutela de los derechos de los ciudadanos.

En lo referente al tratamiento de datos personales de los administrados, debe tenerse en cuenta que, tal y como ha declarado el Tribunal Constitucional (en adelante, TC)<sup>3</sup>, un sistema normativo que, autorizando la recogida de datos incluso con fines legítimos y de contenido aparentemente neutro, no incluyese garantías adecuadas frente a su uso potencialmente invasor de la vida privada del ciudadano, vulneraría el derecho a la intimidad de la misma manera en que lo harían las intromisiones directas en el contenido nuclear de ésta. A estos efectos, el TC recuerda que para la restricción por parte de los poderes públicos de cualesquiera derechos constitucionales debe garantizarse el respeto de los principios de previa habilitación normativa y superación de los juicios de proporcionalidad en sentido amplio, y de idoneidad, necesidad y proporcionalidad en sentido estricto, *ad exemplum*, la sentencia TC 123/2002, de 20 de mayo de 2002 (ECLI:ES:TC:2002:123), cuando que: «(...) para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad es necesario constatar si cumple estos tres requisitos: a) si la medida acordada puede conseguir el objetivo propuesto (juicio de idoneidad); b) si es necesaria en el sentido de que no exista otro medio más moderado para conseguir el fin propuesto con igual eficacia (juicio de necesidad); c) si la medida es ponderada o equilibrada por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)»<sup>4</sup>.

---

<sup>2</sup> Arts. 18, 24, 120 y Título VI CE. Al respecto, RODRÍGUEZ VALLS, María Teresa, «Principio de publicidad procesal y derecho a la protección de datos de carácter personal: aproximación a la problemática actual en Juzgados y Tribunales españoles», *La ley penal: revista de derecho penal, procesal y penitenciario*, núm. 71, 2010.

<sup>3</sup> Así lo ha reconocido el TC en Sentencia 143/1994, de 9 de mayo de 1994, recurso de amparo 3192/1992 (ECLI:ES:TC:1994:143). Véase también, RODRÍGUEZ VALLS, María Teresa, «Principio de publicidad procesal y derecho a la protección de datos ...», *ob. cit.*

<sup>4</sup> En el mismo sentido, el TS en sentencia 610/2016, 7 de Julio de 2016 (ECLI:ES:TS:2016:3621), recuerda que la afectación a la intimidad habrá de graduarse conforme a los factores y circunstancias concurrentes en cada caso, y recordando la necesidad de un permanente ajuste al principio de

Por ello, con el fin de establecer un criterio interpretativo en lo que respecta al tratamiento de los datos personales en el ámbito judicial debe recordarse que nos encontramos ante un derecho fundamental protegido por el artículo 18.4 CE<sup>5</sup>, el cual establece que: «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». El artículo 18.4 CE incorpora un instituto de garantía de otros derechos, principalmente el honor y la intimidad, la garantía de la intimidad entendida en su vertiente positiva se traduce en un derecho de control sobre los datos relativos a la propia persona<sup>6</sup>.

Así, el artículo 18.4 CE garantiza un ámbito de protección específico, pero también más idóneo que el que podían ofrecer, por sí mismos, los derechos fundamentales mencionados en el apartado 1 del mismo precepto -honor e intimidad-, por tanto, aunque los bienes protegidos por los derechos a la intimidad, al honor y a la protección de datos se encuentran parcialmente entrelazados, su objeto no es necesariamente coincidente. La protección de los datos personales permite en muchos casos la salvaguarda de la intimidad personal y el honor,

---

proporcionalidad en la triple vertiente de adecuación, necesidad y proporcionalidad en sentido estricto.

<sup>5</sup> La inclusión del precepto cuarto en el artículo 18 CE constituye un hito, en un momento, 1978, en el que sólo la Constitución portuguesa de 1976 hacía referencia a la utilización de la informática –en su artículo 35– («1. Todos los ciudadanos tienen derecho a tener conocimiento de lo que consta en registro mecanográfico respecto a ellos y del fin a que se destinan informaciones, pudiendo exigir la rectificación de los datos y su actualización, al respecto STC 94/1998, de 4 de mayo de 1998 (ECLI:ES:TC:1998:94).

Configurado por la jurisprudencia constitucional como derecho fundamental al menos desde la STC 292/2000, de 30 de noviembre de 2000 (ECLI:ES:TC:2000:292), construyéndolo a partir del contenido del art. 18.4 CE (y previa su distinción con el derecho a la intimidad personal y familiar del 18.1 CE). También se recoge como derecho fundamental en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea (*DOUE C 364/1*, de 18 de diciembre de 2000), además, el texto literal del este artículo 8 ha sido incorporado como artículo II-68 al Proyecto de Constitución para Europa (*DOUE C310/1* de 16 de diciembre de 2004), que también recoge el derecho a la protección de datos en su Primera Parte, concretamente en el artículo I-51, dentro del Título VI, «La vida democrática de la Unión», al respecto, debe destacarse que el texto de la Carta/Constitución no sólo establece el derecho, sino que lo regula en sus elementos esenciales. Asimismo, el derecho a la protección de datos se encuentra incorporado en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea (*DOUE C 83/47*, de 30 de marzo de 2017). Véase al respecto GUERRERO PICÓ, María del Carmen, *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, Thomson Civitas-Aranzadi, Cizur Menor, Madrid, 2006, p. 135.

<sup>6</sup> Cfr. la STC 254/1993, de 20 de julio de 1993 (ECLI:ES:TC:1993:254). En el mismo sentido, la STC 290/2000, de 30 de noviembre de 2000 (ECLI:ES:TC:2000:290), establece el vínculo entre los apartados 1 y 4 del art. 18 CE, poniendo de manifiesto que el art. 18.4 CE contiene un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos, sin que, por ello, deje de ser un derecho fundamental, «el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos».

pero también la protección de otros derechos tales como el la libertad sindical o la ausencia de discriminación, entre otros<sup>7</sup>.

Como ha reconocido el TC en sentencia 290/2000, de 30 de noviembre (ECLI:ES:TC:2000:290), el derecho fundamental a la intimidad (art. 18.1 CE) no aporta por sí solo una protección suficiente frente a las realidades derivadas del acelerado avance tecnológico, por lo que en el apartado 4 del artículo 18 CE se pone de manifiesto la existencia de los riesgos asociados a este progreso encomendando al legislador el desarrollo de mecanismos de garantía «como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona», pero que es también, «en sí mismo, un derecho o libertad fundamental»<sup>8</sup>.

En consecuencia, la llamada «libertad informática», configurada en el artículo 18.4 CE, es el derecho del ciudadano a controlar el uso de los datos insertos en un programa informático y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (*habeas data*)<sup>9</sup>. En este sentido, el TC en su sentencia 94/1998, de 4 de mayo de 1998 (ECLI:ES:TC:1998:94), reconoció que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados.

Además, el derecho configurado en el artículo 18.4 CE es un derecho autónomo e independiente, que consiste en un poder de disposición y de control sobre los datos personales, que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al titular de los datos personales saber quién los posee y para qué finalidades, pudiendo oponerse a esa posesión

---

<sup>7</sup> BAYO DELGADO, Joaquín, «La protección de datos de la Unión Europea: la Administración de Justicia», en *Revista Derecho y Jueces El Derecho*, núm. 27, 1 de septiembre de 2005.

<sup>8</sup> Fundamento Jurídico 4º STC 290/2000, de 30 de noviembre de 2000 (ECLI:ES:TC:2000:290).

<sup>9</sup> *Vid.* STC 254/1993, de 20 de julio (ECLI:ES:TC:1993:254), la «libertad informática», reconocida por el art. 18.4 CE, ya no es la libertad de negar información sobre los propios hechos privados o datos personales, sino la libertad de controlar el uso de esos mismos datos insertos en un programa informático: lo que se conoce con el nombre de *habeas data*. En el mismo sentido, el Fundamento Jurídico Quinto de la STC 292/2000, de 30 de noviembre de 2000 (ECLI:ES:TC:2000:292) y la jurisprudencia citada en la misma. Al respecto véase PÉREZ-LUÑO ROBLEDO, Enrique César, *El procedimiento de habeas data: El derecho procesal ante las nuevas tecnologías*, Dykinson, Madrid, 2017, pp. 53 y ss.

o uso<sup>10</sup>. En definitiva, el derecho fundamental comprende un conjunto de facultades que el ciudadano puede ejercer frente a quienes sean titulares, públicos o privados, de ficheros de datos personales, partiendo del conocimiento de tales ficheros y de su contenido, uso y destino, por el registro de éstos.

Como veremos en el presente trabajo, pese a la importancia que tiene el derecho de protección de datos personales como derecho fundamental, uno de los principales problemas del sistema actual de protección de datos es la insuficiencia del marco normativo vigente en su aplicación al ámbito de la Administración de Justicia, que hace muy difícil resolver los conflictos existentes entre las normas procesales y las normas específicas de protección de datos.

## II. EL TRATAMIENTO JURISDICCIONAL DE DATOS PERSONALES

### 2.1. Marco normativo del tratamiento de datos personales en el ámbito judicial

La concreción y desarrollo del derecho fundamental de protección de las personas físicas en relación con el tratamiento de datos personales se asienta sobre 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<sup>11</sup> (en adelante, RGPD). La eficacia directa de dicho texto normativo trajo consigo la necesidad reforma de la

---

<sup>10</sup> Cfr. la STC Sentencia 292/2000, de 30 de noviembre de 2000 (ECLI:ES:TC:2000:292. El concepto actual de privacidad tiene sus orígenes en los Estados Unidos de América, donde el juez americano Thomas Cooley asentó en 1888 la definición de privacidad como «*the right to be let alone*», o el derecho a que ser dejado solo o a ser dejado en paz, *vid. MCINTYRE COOLEY, Thomas, A Treatise on the Law of Torts, Or the Wrongs which Arise Independently of Contract*, vol. 1, Callaghan & Co., Chicago, 1907, esta idea respecto a la libertad del individuo a controlar todo lo referente a su privacidad fue acogida por WARREN II, Samuel D., BRANDEIS, Louis, «The right to privacy», *Harvard Law Review*, Vol. IV, núm. 5, diciembre 15, 1890, disponible en [https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy\\_brand\\_warr2.html](https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html), estos autores ponían de manifiesto su preocupación por cómo los avances tecnológicos de la época -las fotografías instantáneas- afectaban a la protección de la imagen y la privacidad de las personas, y abogaban por ofrecer algún remedio legal frente a la circulación no autorizada de retratos de personas privadas. Por su parte, PÉREZ GIL, Julio, «Investigación penal y nuevas tecnologías: algunos de los retos pendientes», *Revista Jurídica de Castilla y León*, núm. 7, 2005, p. 227, señala que: «la protección de datos personales en su dimensión de autodeterminación informativa, esto es, entendida como la facultad de un sujeto de decidir qué es lo que los demás conocen de él». En un sentido similar, LUCENA CID se refiere a “la facultad de toda persona para ejercer control sobre la información personal almacenada en medios informáticos tanto por las administraciones públicas como entidades u organizaciones privadas”, en LUCENA CID, Isabel Victoria, «La protección de la intimidad en la era tecnológica: hacia una reconceptualización», *Revista internacional de pensamiento político*, I época, volumen 7, 2012, p. 135.

<sup>11</sup> DOUE L 119/1, de 4 de mayo de 2016.

legislación nacional vigente, lo cual se materializó en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPD)<sup>12</sup>.

Los apartados 4 y 5 del artículo 2 de la LOPD remiten la protección de datos de carácter personal en el ámbito de la Administración de Justicia a la directa aplicación del RGPD, así, establecen que el tratamiento de datos llevado a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina Judicial y por el Ministerio Fiscal deberán regirse por lo dispuesto en el RGPD, la LOPD y las disposición de la Ley Orgánica del Poder Judicial (en adelante, LOPJ)<sup>13</sup> que le sean aplicables<sup>14</sup>. Todo ello, a pesar de que, como podremos constatar en el presente trabajo, el régimen jurídico previsto en el RGPD tiene difícil adaptación a las características estructurales, organizativas y funcionales de los órganos jurisdiccionales tal y como vienen establecidas en la CE y en la LOPJ<sup>15</sup>.

Por otro lado, la Ley Orgánica 7/2015, de 21 de julio<sup>16</sup>, añadió un nuevo capítulo a la LOPJ, bajo la rúbrica «Protección de datos de carácter personal en el ámbito de la Administración de Justicia». Se trata del capítulo I *Bis* del Título III del Libro III, integrado por los artículos 236 *bis* a 236 *decies*, a todos los cuales ha dado nueva redacción la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección,

---

<sup>12</sup> BOE núm. 294, de 6 de diciembre de 2018.

<sup>13</sup> Ley Orgánica 6/1985, de 1 de julio, publicada en el BOE núm. 157, de 2 de julio de 1985.

<sup>14</sup> Vid. RODRÍGUEZ ROCA, Alejandro, *La protección de datos personales en los juzgados y tribunales. Un enfoque desde la perspectiva laboral*, La Ley, Madrid, 2022, p. 23, destaca que la superposición de las normas de protección y datos y las del Derecho Procesal tiene dos consecuencias: «la primera es que las disposiciones procesales deben respetar el derecho a la protección de datos, porque de lo contrario estarían vulnerando un derecho fundamental. La segunda es que, respetando ese núcleo esencial, la ley procesal específica puede regular, razonablemente y de modo adecuado al caso concreto, cómo ejercer determinados aspectos o facultades previstas de forma genérica en la normativa de protección de datos. Un ejemplo puede ser el derecho de acceso a los propios datos: la particular forma de su ejercicio puede ser modulada por la ley procesal, pues la LOPD, siendo general, no puede descender a los detalles de todas sus posibles aplicaciones».

<sup>15</sup> TRONCOSO REIGADA, Antonio, *La Protección de Datos Personales. En Busca del Equilibrio*, Tirant Lo Blanch, Valencia, 2011, p. 283. Véase también, RODRÍGUEZ ROCA, Alejandro, *La protección de datos personales en los juzgados...*, ob. cit., sostiene que el contenido del artículo 236 *bis* LOPJ constituye una mera declaración de intenciones sin apoyo normativo suficiente, porque no basta con enunciar que la normativa de protección de datos es aplicable a la Administración de Justicia, sino que es necesario adaptar sus instituciones a un ámbito que de por sí revela una aparente colisión entre principios esenciales, y destaca que este marco normativo es difícil de adaptar a la Administración de Justicia dada su estructura orgánica y organizativa que la hace muy diferente del resto de organismos del poder público del Estado.

<sup>16</sup> BOE núm. 174, de 22 de julio de 2015.

investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (en adelante, LO 7/2021)<sup>17</sup>.

Por su parte, la LO 7/2021 es el resultado de la transposición de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, que deroga la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal<sup>18</sup>, esta Directiva se aprobó con el objetivo de establecer un marco más sólido y coherente para la protección de datos personales en la Unión Europea, y para facilitar la libre circulación de datos personales entre las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, ya que la fragmentación y complejidad de la regulación existente en este campo perjudicaba la necesaria confianza entre los actores de la cooperación policial y judicial penal en Europa, quienes mostraban recelos a compartir información, entre otros motivos, por la ausencia de una mínima armonización en cuanto a la protección de los datos de carácter personal.

## 2.2. El tratamiento de datos personales por la Administración de Justicia: tratamientos con fines jurisdiccionales y no jurisdiccionales

El artículo 236 *bis* LOPJ, en la redacción dada al mismo por la LO 7/2021, señala en su apartado 1 que el tratamiento de los datos personales en el ámbito de la Administración de Justicia podrá realizarse con fines jurisdiccionales o no jurisdiccionales, estableciendo que tendrá fines jurisdiccionales el tratamiento de los datos que se encuentran incorporados a los procesos que tengan por finalidad el ejercicio de la actividad jurisdiccional. El carácter jurisdiccional del tratamiento requiere, por tanto, el cumplimiento de dos condiciones: en primer lugar, que los datos que se tratan se encuentren incorporados a un procedimiento judicial y, en segundo lugar, que la finalidad del tratamiento sea el ejercicio mismo de la actividad jurisdiccional.

Los tratamientos con fines jurisdiccionales, como su nombre indica, se vinculan al ejercicio de la actividad judicial, rigiéndose por lo regulado en el RGPD, la LOPD, así como las especialidades recogidas tanto en la LOPJ y en las normas

---

<sup>17</sup> BOE núm. 126, de 27 de mayo de 2021.

<sup>18</sup> DOUE L 119/89, de 4 de mayo de 2016.



procesales<sup>19</sup>. El control de los datos tratados con fines jurisdiccionales corresponde, respecto a los tratamientos de los juzgados y tribunales, a la Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial (en adelante, CGPJ) y a la Unidad de Supervisión y Control de Protección de Datos respecto a aquellos tratamientos cuya responsabilidad sea de la Fiscalía General del Estado<sup>20</sup>. Por su parte, los tratamientos de datos de con finalidad no jurisdiccional, también conocidos con el nombre de gubernativos, son aquellos que obviamente no están relacionados con el ejercicio de la función jurisdiccional, siendo de aplicación el RGPD y la LOPD<sup>21</sup>.

La diferenciación de tipos de tratamiento incide especialmente en la determinación de la autoridad de control de tales tratamientos, a la que se asigna, entre otras funciones, la supervisión del cumplimiento de la normativa de protección de datos y la constatación de los posibles indicios de infracciones en esta materia a través de los correspondientes procedimientos. Asimismo, el tipo de tratamiento determina el régimen de ejercicio de los derechos de información, acceso, rectificación, supresión, oposición y limitación y, además, afecta al régimen de las comunicaciones o cesiones de datos entre ambos tipos de tratamientos.

---

<sup>19</sup> El artículo 2 LOPD establece en lo relativo al ámbito de aplicación de sus Títulos I a IX y de sus artículos 89 a 94 que: «El tratamiento de datos llevado a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina Judicial, se regirán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente ley orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, que le sean aplicables». Al respecto CREMADES LÓPEZ DE TERUEL, Fernando Javier, «La nueva Ley Orgánica de Protección de Datos y el Poder Judicial: un juego de mercaderes en el templo del Reglamento General de la Unión Europea», *Diario La Ley*, núm. 9430, 2019, crítica que la LOPD no haya realizado una adaptación del RGPD, y que el tratamiento que hace la LOPD de la protección de datos en el ámbito del Poder Judicial resulta escueto, aunque no exento de contenido, lo cual afecta al sistema de fuentes que ha de serle aplicable.

<sup>20</sup> La autoridad de control de la Fiscalía General del Estado no se encuentra en funcionamiento debido que está pendiente de dotación presupuestaria y desarrollo reglamentario. Sin perjuicio de ello, Fiscalía General del Estado aprobó, con fecha 20 de diciembre de 2020, la Instrucción 2/2019, de 20 de diciembre, sobre la protección de datos en el ámbito del Ministerio Fiscal: el responsable y el Delegado de Protección de Datos, en la que se realiza una identificación del Ministerio Fiscal como responsable del tratamiento de datos, con sus obligaciones incluyendo las relativas de las diferentes fiscalías, unidades y demás órganos, las obligaciones de todos los fiscales, y las funciones y actuaciones de su delegado de protección de datos, que estará apoyado por sus adjuntos, uno en cada Comunidad Autónoma. Publicada en el BOE núm. 19, de 22 de enero de 2020.

<sup>21</sup> En cuanto al ejercicio de derechos, se podrá llevar a cabo según lo dispuesto en ambas normas y la competencia para su control se atribuye a la Agencia Española de Protección de Datos (en adelante, AEPD), no obstante, los datos tratados con finalidad no jurisdiccional pueden ser comunicados al CGPJ, a la Fiscalía General del Estado y a la Ministerio de Justicia, siempre y cuando estas comunicaciones estén justificada y resulten necesarias para el ejercicio de sus respectivas competencias.

### 2.3. Los datos objeto de tratamiento en el ámbito jurisdiccional

El ejercicio de la potestad jurisdiccional trae consigo la creación de ficheros de datos personales de titularidad pública que, como ya hemos mencionado, se clasifican en función de su finalidad en jurisdiccionales o no jurisdiccionales, de acuerdo con lo dispuesto en el artículo 236 *bis* LOPJ, la existencia de esta clasificación condiciona la asignación de las funciones de responsables de los correspondientes tratamientos, según se considere que el fichero tiene una u otra finalidad.

Para la determinación de la finalidad del fichero como jurisdiccional o no jurisdiccional resulta necesario diferenciar cuáles son los datos que tienen una relación directa con el ejercicio de la actividad jurisdiccional de los que no la tienen. En principio, el tratamiento debe circunscribirse a los que resulten estrictamente necesarios para la tramitación de los procesos y su adecuada gestión realizada por las Oficinas Judiciales, las Unidades Procesales de Apoyo Directo y los Servicios Comunes. En esta misma línea, deberá entenderse como ficheros con fines jurisdiccionales los datos que se encuentran en LexNet, puesto que las notificaciones y presentación de escritos dentro del proceso son necesarios para el ejercicio de la potestad jurisdiccional<sup>22</sup>.

En lo que respecta al tratamiento de datos personales con fines jurisdiccionales, lo primero que debe tenerse en cuenta es que existe una limitación legal respecto a los datos deben ser tratados, de modo que sólo deben figurar en las resoluciones y actuaciones procesales los que resulten «adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados». En este sentido, el artículo 236 *quinquies* LOPJ<sup>23</sup> reconoce a jueces, magistrados, fiscales y a letrados de la Administración de Justicia la facultad de 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

---

<sup>22</sup> Cfr. SANCHO ALONSO, Jesús, *La función institucional del secretario judicial-letrado de la Administración de Justicia*. Tesis dirigida por Ángel Sánchez Blanco, Universidad de Málaga, Departamento de Derecho público, 2017, p. 407, disponible en: <https://riuma.uma.es/xmlui/handle/10630/16630>, fecha de la consulta 14 de septiembre de 2024.

<sup>23</sup> Del mismo modo, la Circular 2/2022, de 20 de diciembre, de la Fiscalía General del Estado, sobre la actividad extraprocésal del Ministerio Fiscal en el ámbito de la investigación penal, sostiene que no se aprecian obstáculos que impidan aplicar las reglas recogidas en el art. 236 *quinquies* LOPJ a la actividad extraprocésal del Ministerio Fiscal, pues el acceso a los datos personales de víctimas, sospechosos, testigos y peritos, tales como el domicilio personal, documento de identidad, número de teléfono, dirección de correo electrónico u otros análogos, no solo no contribuye al mejor ejercicio de los derechos de defensa y/o a la tutela judicial efectiva, sino que supone una limitación innecesaria del derecho a la intimidad.

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<sup>24</sup>.

Por su parte, el artículo 236 *ter* LOPJ, que regula el sistema de garantías procesales dentro del sistema de protección de datos personales, en su apartado 3 exige del requisito del consentimiento del titular para el tratamiento con fines jurisdiccionales. Así, los datos personales tratados con fines jurisdiccionales podrán ser recabados sin el consentimiento del interesado, con independencia de que se trate de datos facilitados por las partes u obtenidos a solicitud de los órganos competentes, todo ello, sin perjuicio de lo dispuesto en las normas procesales respecto a los requisitos para la validez de los medios de prueba (artículo 236 *ter*.3 LOPJ).

Por tanto, la Administración de Justicia no requiere del consentimiento del interesado para el tratamiento de sus datos cuando se realice en atención del interés público (artículo 6.1.c) RGPD), o bien, en el ejercicio de las potestades conferidas al responsable del tratamiento (artículo 6.1.c) RGPD). La causa que legitima el tratamiento es el ejercicio de la función pública y la existencia de normas que autorizan la obtención y almacenamiento de los de datos de carácter personal, tanto de las partes del proceso como de terceros.

#### 2.4. La autoridad de control y sus funciones en el tratamiento de datos personales en el ámbito jurisdiccional

La figura de la autoridad de control se ha venido contemplando desde la aparición de las primeras normas en materia de protección de datos<sup>25</sup>, así, el

---

<sup>24</sup> RODRÍGUEZ ROCA, Alejandro, *La protección de datos personales en los juzgados...*, ob. cit., advierte que la labor de supresión de datos personales puede dar lugar a indefensión, con la consiguiente vulneración del artículo 24.2 CE, a la parte que tenga que defenderse de los documentos que sean anonimizados, ya que puede llevarle a desconocer datos que pueden resultar determinantes para su defensa, importancia ésta que resulta muy difícil de predecir en el momento de la supresión de los datos personales y considera que se trata de una ambigua la salvaguarda que puede llevar incluso a plantearnos su constitucionalidad. Del mismo modo, FRIEYRO ELÍCEGUI, Sofía, «Tratamiento de datos personales en el orden jurisdiccional penal. Protección de menores de edad y personas con discapacidad necesitadas de especial protección», *Diario La Ley*, Sección Doctrina, 8 de febrero de 2023, se pronuncia sobre la posible controversia en la valoración de cuándo la supresión de datos personales en las resoluciones y documentos que obren en un procedimiento penal puede afectar al derecho a la tutela judicial efectiva. Se puede entender que se deja en manos de los letrados de la Administración de Justicia, que no tienen por qué conocer el fondo del asunto, la valoración de la afectación de dicho derecho fundamental en las resoluciones de su competencia.

<sup>25</sup> En España, la derogada Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de carácter personal, *BOE* núm. 262, de 31 de octubre de 1992 - derogada

Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, del Consejo de Europa, de 28 de enero de 1981<sup>26</sup>, también conocido como núm. 108, hacía referencia a la autoridad «controladora del fichero» como un organismo independiente con competencia para decidir cuál era la finalidad del fichero automatizado, las categorías de datos que debían registrarse y las operaciones de tratamiento que se le debían aplicar, afirmando su función como garante del cumplimiento de la normativa sobre la materia<sup>27</sup>.

En cuanto a la actuación de la autoridad de control en el ámbito judicial, cabe recordar que antes de la reforma de la LOPJ, introducida por la Ley Orgánica 7/2015, de 21 de julio<sup>28</sup>, se atribuía a la AEPD la competencia de autoridad de control en materia de protección de datos sobre juzgados y tribunales, en este periodo la AEPD desarrolló intervenciones de inspección en los órganos jurisdiccionales, sin embargo, el Tribunal Supremo (en adelante, TS), en sentencia núm. 8497/2011, de 2 de diciembre de 2011 (ECLI:ES:TS:2011:8497), declaró la incompetencia de la AEPD para ejercer función de autoridad de control sobre juzgados y tribunales y para declarar la infracción en los requerimientos dirigidos a los mismos, entendiendo que el ejercicio de estas competencias por al AEPD suponían una injerencia en la independencia del Poder Judicial<sup>29</sup>.

---

por la Ley Orgánica 15/1999, de 13 de diciembre-, fue la primera norma en asignar el control de su aplicación a un organismo independiente, la denominada Agencia de Protección de Datos, posteriormente, el RD 428/1993, de 26 de marzo, *BOE*, núm. 106, de 4 de mayo de 1993, derogado por RD 389/2021, de 1 de junio, aprobó su Estatuto y dedicó el Título VI LOPD a la regulación de la naturaleza, régimen jurídico y funciones. Con estas disposiciones el legislador español se anticipó al contenido del artículo 28 de la Directiva 95/46/CE, -derogada por Reglamento 2016/679, de 27 de abril-, que obligaba al establecimiento de una autoridad de control, encargada de vigilar la aplicación de las normas relativas al tratamiento de datos de carácter personal, si bien, esta última norma tuvo algunas repercusiones en el funcionamiento de la Agencia que tendrían que corregirse posteriormente a través de la LOPD.

<sup>26</sup> Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, publicado en el *BOE* núm. 274, de 15 de noviembre de 1985.

<sup>27</sup> STC 290/2000, de 30 de noviembre de 2000 (ECLI:ES:TC:2000:20), recuerda que las autoridades de control ejercen una función tuitiva.

<sup>28</sup> *BOE* núm. 174, de 22 de julio de 2015.

<sup>29</sup> El TS considera excluido el poder de decisión de la AEPD en base a que el CGPJ tiene 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 y, así preservar los principios de unidad e independencia de la organización judicial e impedir cualquier tipo de intromisión o injerencia por parte de una autoridad administrativa. *Vid.* FRESNEDA PLAZA, Felipe, «Régimen sancionador y protección de datos», *Cuadernos Digitales de Formación del Consejo General del Poder Judicial*, núm. 29, 2012. LESMES SERRANO, Carlos, «Las potestades de fiscalización de la agencia española de protección de datos en el ámbito de la Administración de Justicia», *Revista de Jurisprudencia El Derecho*, núm. 1, 2012, p. 2. Disponible en <https://revistas.lefebvre.es/revista-de-jurisprudencia/>

Con la aprobación del RGPD se impuso un cambio estructural de carácter sustantivo, introduciendo las reglas para la determinación de las condiciones de constitución, organización y funcionamiento de las autoridades de control, que deben cumplirse para que sean consideradas como tales y para que puedan asumir las funciones que se les atribuyen, como consecuencia de ello, el RGPD dispone que cada Estado miembro debe encomendar a una autoridad de control (o varias) la supervisión de la aplicación del Reglamento -en España, la AEPD y las agencias de carácter autonómico-.

Sin embargo, el RGPD no contiene normas específicas relativas a la implementación de la protección de datos en el ámbito de la Administración de Justicia<sup>30</sup>, existiendo una falta de reserva jurisdiccional explícita en materia de tratamiento de datos a cargo de los tribunales de justicia, esto genera inseguridad jurídica puesto que el sistema general de protección de datos personales no puede adaptarse con facilidad a la Administración de Justicia, debido a las complejidades de su propia organización y de los principios que lo regulan<sup>31</sup>.

Tal y como se explica en el considerando 20 del RGPD, con el 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, así, el artículo 55.3 RGPD establece 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» y, en consecuencia, 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 RGPD, concienciar a los miembros del Poder Judicial acerca de sus obligaciones y atender las reclamaciones en relación con tales operaciones de tratamiento de datos.

---

hemeroteca/tribunas/1557 . MARCOS AYJÓN, Miguel, *La protección de datos de carácter personal en la justicia penal*, Bosch, Barcelona, 2020, p. 226.

<sup>30</sup> Véase al respecto SOLAR CALVO, María del Puerto, «Nueva regulación europea en protección de datos. Urgente necesidad de una normativa nacional», *Unión Europea Aranzadi*, núm. 7, 2018. RODRÍGUEZ ROCA, Alejandro, *La protección de datos personales en los juzgados...*, ob. cit., califica como una oportunidad perdida que el RGPD no contenga una regulación específica respecto a los datos tratados en el ámbito de la Administración de Justicia, y destaca que hay tres aspectos relevantes en los que resulta precisa una regulación expresa en determinados para conseguir conciliar los derechos de los diferentes sistemas de ordenación, a saber: la cuestión de los ficheros policiales; la cesión de datos entre Administraciones y; el acceso al expediente penitenciario.

<sup>31</sup> TRONCOSO REIGADA, Antonio, *La Protección de Datos Personales...*, ob. cit., p. 279.

En este contexto, la LOPJ ha asignado al CGPJ las competencias propias de la autoridad de control de protección de datos, en el caso de los tratamientos de datos personales con fines jurisdiccionales<sup>32</sup> (artículo 236 *octies* LOPJ), las cuales son ejercidas por la Dirección de Supervisión y Control de Protección de Datos del CGPJ, con arreglo a lo dispuesto en el artículo 236 *nonies*<sup>33</sup>. De este modo, aunque en la LOPD no se diga nada, el CGPJ tiene reconocida la función de tutela de los ficheros judiciales en materia de protección de datos, ello se justifica en la necesidad de preservar los principios de unidad e independencia de la organización judicial (artículo 104 LOPJ), y de evitar cualquier tipo de injerencia por parte de otra autoridad administrativa<sup>34</sup>. Sin perjuicio de lo anterior, los tratamientos de datos personales en la Administración de Justicia deben llevarse a cabo por el órgano competente y dentro de él, por quien tenga la competencia

---

<sup>32</sup> Cabe señalar que anteriormente la STS 8497/2011, Sala Tercera, de 2 de diciembre 2011, Rec. 2706/2008 (ECLI:ES:TS:2011:8497), determinó que el control sobre posibles incumplimientos en los tratamientos de datos jurisdiccionales recaía en el CGPJ y no en la AEPD, como había ocurrido anteriormente a que se dictase dicha sentencia: «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)».

<sup>33</sup> La designación del CGPJ como autoridad de control, en el caso de los tratamientos de datos con fines jurisdiccionales, ha sido cuestionada por parte de la doctrina, por considerar que no garantiza el cumplimiento de los requisitos establecidos en los artículos 51 a 59 RGPD, esto es: que la autoridad de control ha de ser independiente, con recursos propios, materiales, personales y financieros, y, en concreto, se ha de asegurar que el miembro o los miembros de cada autoridad de control sean ajenos a toda influencia externa, ya sea directa o indirecta, y no soliciten ni admitan ninguna instrucción; ha de disponer en todo momento de los recursos humanos, técnicos y financieros, así como de las infraestructuras necesarias para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes; ha de elegir y disponer de su propio personal; y ha de estar sujeta a un control financiero que no afecte a su independencia, disponiendo de un presupuesto anual, público e independiente. Véase también, CREMADES LÓPEZ DE TERUEL, Fernando Javier, «La nueva Ley ...», ob. cit., véase también RODRÍGUEZ ROCA, Alejandro, *La protección de datos personales en los juzgados...*, ob. cit., critica que en España se sigue aplicando la LOPJ sin valorar las contradicciones que su articulado tiene con el vigente RGPD, para este autor, quien está ejerciendo las competencias de autoridad de control sobre los tribunales es el CGPJ y puesto que la propia LOPJ diferencia entre los tratamientos con fines jurisdiccionales y los tratamientos sin fines jurisdiccionales, el régimen jurídico de los datos que se almacenan en la Administración de Justicia es especial o común dependiendo de aquella clasificación. Véase también, CREMADES LÓPEZ DE TERUEL, Fernando Javier, SANCHO ALONSO, Jesús, «Protección de datos y Poder Judicial», *Diario La Ley*, núm. 9293, Sección Tribuna, noviembre de 2018.

<sup>34</sup> Vid. MARCOS AYJÓN, Miguel, «La protección de datos de carácter personal en la Oficina Judicial Penal», *La Ley Penal*, núm. 135, noviembre-diciembre 2018, señala que: «Como se ha expuesto en el epígrafe sobre la autoridad de control, contenido en el Capítulo II, es el CGPJ quien tiene singularmente reconocida la función tutelar en materia de protección de datos en relación a los ficheros judiciales, toda vez que forman parte de su ámbito de gobierno, circunstancia que se justifica en la necesidad de preservar los principios de unidad e independencia de la organización judicial, y que impide cualquier tipo de intromisión e injerencia por parte de una autoridad administrativa». Asimismo, DELGADO MARTÍN, Joaquín, «Reflexiones sobre la protección de datos personales en la Administración de Justicia», *Diario La Ley*, núm. 9363, Sección Tribuna, 21 de febrero de 2019.

atribuida por la normativa vigente, a quien asume la función de responsable del tratamiento como analizaremos más adelante<sup>35</sup>.

Por su parte, la Directiva (UE) 2016/680 exige que la autoridad de control designada pueda ejercer con plena independencia las facultades de inspección, supervisión, la posible adopción de medidas cautelares, y sanción, bien directamente, bien mediante la comunicación de los hechos a la autoridad judicial que, con arreglo al derecho nacional, tenga capacidad para imponerlas<sup>36</sup>. Por tanto, las funciones asignadas al CGPJ como autoridad de control de protección de datos respecto de los tratamientos con fines jurisdiccionales se ejercen, con arreglo a lo dispuesto en el artículo 236 *nonies* LOPJ, por la Dirección de Supervisión y Control de Protección de Datos. Tales funciones se relacionan en el apartado 1 del artículo 236 *octies* LOPJ, dichas funciones son la supervisión del cumplimiento de la normativa; la sensibilización de los profesionales de la Administración de Justicia; la emisión de informes sobre los códigos de conducta; contribuir a la correcta aplicación de la normativa; informar a los interesados sobre el ejercicio de sus derechos; y tramitar reclamaciones presentadas por los interesados.

Por último, cabe tener en cuenta que, a pesar de que se atribuya al CGPJ las competencias de la autoridad de control respecto a los datos tratados con fines jurisdiccionales, los artículos el 44.3 LOPD y 236 *octies* apartado 3 LOPJ prevén la necesidad de establecer mecanismos de colaboración entre el CGPJ la AEPD, para asegurar el adecuado ejercicio de las respectivas competencias atribuidas.

En cumplimiento de este mandato, se ha suscrito el Convenio de colaboración entre el CGPJ y la AEPD, firmado el 6 de julio de 2017<sup>37</sup>, en virtud del

---

<sup>35</sup> De acuerdo con lo establecido en el apartado 2 del artículo 236 *bis* de la LOPJ.

<sup>36</sup> En este sentido el artículo 28.3 de la Directiva (UE) 2016/680 establece que las autoridades de control deberán disponer de poderes de investigación, como el derecho de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control; poderes efectivos de intervención y garantizar una publicación adecuada de dichos dictámenes, o el de ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento, o el de dirigir una advertencia o amonestación al responsable del tratamiento o el de someter la cuestión a los parlamentos u otras instituciones políticas nacionales; y capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la Directiva o de poner dichas infracciones en conocimiento de la autoridad judicial. Además, las decisiones de la autoridad de control lesivas de derechos podrán ser objeto de recurso jurisdiccional.

<sup>37</sup> Disponible en el siguiente enlace: <https://www.aepd.es/sites/default/files/2020-02/convenio-aepd-cgpj.pdf>, fecha de la consulta 15 de septiembre de 2024. El Convenio contiene cuatro líneas de actuación como son: (1) inspección, en el que ambas partes se compromete a prestar asistencia en la realización de las mismas; (2) responsabilidad activa, consistente en la generación de instrumentos para el mejor cumplimiento de las obligaciones de protección de datos, incluyendo la elaboración,

mismo, la AEPD se compromete prestar asistencia a los órganos inspectores del CGPJ ante la posible comisión de una infracción de la normativa de protección de datos en los ficheros jurisdiccionales. Mientras que, cuando se trate del supuesto de ficheros jurisdiccionales, el CGPJ se compromete a notificar a la AEPD su intención de iniciar una inspección a un determinado órgano judicial para investigar si existe una posible infracción del derecho a la protección de datos, estas inspecciones se realizan con la presencia de profesionales de ambas entidades, de modo que la AEPD presta asistencia técnica al CCPJ, sin que ello suponga asunción de ninguna competencia<sup>38</sup>.

## 2.5. El responsable de tratamiento de los datos con fines jurisdiccionales

De acuerdo con lo previsto por el artículo 4.7 RGPD, el responsable de tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento, la determinación de estos los fines y medios de los tratamientos en el ámbito judicial viene en gran medida establecida en la normativa orgánica judicial y las propias leyes procesales. No obstante, ante la falta de una atribución específica de la condición de responsable del tratamiento por la LOPJ, que se limita a establecer en el apartado 2 del artículo 236 *bis* que los tratamientos de datos personales en la Administración de Justicia se llevarán a cabo por el órgano competente y, dentro de él, por quien tenga la competencia atribuida por la normativa vigente, la condición de responsable del tratamiento recae en el órgano jurisdiccional u oficina judicial ante el que se sigue el proceso, respecto de los tratamientos de los datos obrantes en el mismo desarrollados en el ejercicio de la actividad jurisdiccional (ficheros de datos personales con fines jurisdiccionales) con arreglo a las previsiones contenidas en las normas orgánicas y procesales.

Así las cosas, en el caso de los ficheros tratados con fines jurisdiccionales, el responsable del tratamiento es el órgano jurisdiccional y dentro del él, el juez o el letrado de la Administración de Justicia según las normas de competencia.

---

modificación o ampliación de códigos de buenas prácticas para usuarios de los sistemas de información de la Administración de Justicia; (3) formación, con la impartición de cursos y seminarios de forma conjunta; y (4) ayuda recíproca, facilitándose ambas partes información útil y prestación de asistencia mutua de conformidad con lo dispuesto en el RGPD.

<sup>38</sup> La colaboración abarca, además, el intercambio para la elaboración de códigos de buenas prácticas para usuarios de los sistemas de información de la Administración de Justicia y, por último, el Convenio establece la posibilidad de desarrollar actuaciones conjuntas en materia de formación sobre normativa española y comunitaria de protección de datos.



El responsable del tratamiento tendrá entre sus funciones la tramitación y resolución del ejercicio de los derechos derivados del sistema de protección de datos personales (información, acceso, rectificación, supresión, oposición y limitación) de acuerdo con el artículo 236 *septies* LOPJ, que se tramitarán conforme a las normas de aplicación al proceso en que fueron recabados. Asimismo, el responsable del tratamiento podrá dar instrucciones pertinentes para que el tratamiento de los datos de carácter personal contenidos en los ficheros judiciales se realice de acuerdo con los derechos y principios previstos en el sistema de protección de datos<sup>39</sup>.

Por otro lado, en cuanto a la figura del responsable de tratamiento de datos personales en el ámbito jurisdiccional, es necesario tener en cuenta que la Fiscalía General del Estado aprobó, con fecha 20 de diciembre de 2020, la Instrucción 2/2019, de 20 de diciembre, sobre la protección de datos en el ámbito del Ministerio Fiscal, en la que se realiza una identificación del Ministerio Fiscal como responsable del tratamiento de datos, con sus obligaciones incluyendo las relativas de las diferentes fiscalías, unidades y demás órganos, las obligaciones de todos los fiscales, y las funciones y actuaciones de su delegado de protección de datos, que estará apoyado por sus adjuntos, uno en cada Comunidad Autónoma<sup>40</sup>.

Por su parte, el apartado 7.4 de la Instrucción 2/2019 establece la obligación de los integrantes del Ministerio Fiscal y de la plantilla de funcionarios que prestan servicio en las distintas fiscalías de conocer y cumplir las normas, procedimientos e instrucciones impartidas en materia de protección de datos así como la participación en actividades formativas; en concreto en el apartado 7.3 letra f) recoge medidas básicas que se deberán cumplir, de manera semejante a como hace el CGPJ, entre otras, la destrucción de forma segura de documentos y dispositivos en desuso, o no abrir archivos o enlaces adjuntos que puedan acompañar a correos electrónicos remitidos por fuentes desconocidas.

---

<sup>39</sup> Vid. MARCOS AYJÓN, Miguel, «La protección de datos de carácter personal en la Oficina ...», ob. cit., p. 12.

<sup>40</sup> El apartado 7.1 de la citada instrucción, establece los principios que deben regir la actuación del Ministerio Fiscal como responsable del tratamiento de datos personales, y que son: licitud, lealtad y transparencia en relación con el interesado; limitación de la finalidad, de manera que los datos se traten con fines determinados, explícitos y legítimos; minimización de datos, pues se deben limitar a lo necesario en relación con los fines del tratamiento; exactitud, debiéndose mantener los datos actualizados; limitación del plazo de conservación; integridad y confidencialidad, a cuyos efectos se deberán adoptar medidas técnicas y organizativas apropiadas para garantizar una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento y acceso no autorizado o ilícito y contra la pérdida, destrucción o daño accidental.

### III. ALGUNAS ESPECIALIDADES EN MATERIA DE TRATAMIENTO DE DATOS PERSONALES CON FINES JURISDICCIONALES EN EL PROCEDIMIENTO PENAL

En relación al tratamiento de los datos personales llevados a cabo con ocasión de la tramitación de los procesos penales por fiscalías y órganos judiciales, el artículo 236 *ter.2* LOPJ se remite a lo previsto en la LO 7/2021, todo ello, sin perjuicio de las especialidades establecidas en la propia LOPJ 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<sup>41</sup>.

La LO 7/2021 tiene por objeto establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal por parte de las autoridades competentes con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública (artículo 1 LO 7/2021), siendo de aplicación tanto al tratamiento total o parcialmente automatizado de datos personales, como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero<sup>42</sup>.

La conservación de los datos referidos a estos procedimiento sólo puede hacerse durante el tiempo necesario para cumplir los fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública, y se debe revisar por el responsable del tratamiento, como máximo cada tres años, la necesidad de conservar, limitar o suprimir los datos personales contenidos en cada una de las actividades de tratamiento, en atención a la edad del afectado, el carácter de los datos y a la conclusión de una investigación o procedimiento penal (artículo 8 LO 7/2021). Se establece también un plazo máximo de 20 años para la supresión de los datos, con determinadas excepciones que son la existencia de investigaciones abiertas, delitos que

---

<sup>41</sup> Publicada en el *BOE* núm. 11, de 13 de enero de 1982.

<sup>42</sup> Además, la LO 7/2021 establece un deber de colaboración de las administraciones públicas y de cualquier persona física o jurídica con las autoridades judiciales, el Ministerio Fiscal y con la policía judicial, cuando actúe en el ejercicio de las funciones que le encomienda el artículo 549.1 LOPJ, solamente se excluye este deber de colaboración en los supuestos en que legalmente sea exigible la autorización judicial para recabar los datos. Con carácter general, a efectos de garantizar la actividad investigadora, se prevé que el interesado no sea informado de la transmisión de sus datos a las autoridades competentes, ni de que se ha facilitado el acceso a sus datos de cualquier forma.

no hayan prescrito, la no conclusión de la ejecución de la pena, en supuestos de reincidencia, o en que exista una necesidad de proteger a las víctimas u por otras circunstancias motivadas<sup>43</sup>.

Por otro lado, se prohíbe la elaboración de perfiles que produzcan efectos jurídicos negativos para el interesado o que le afecten significativamente, salvo autorización expresa por norma legal o de derecho de la Unión Europea (artículo 14 LO 7/2021); y se prohíbe, en todo caso, la elaboración de perfiles que dé lugar a una discriminación de las personas físicas sobre la base de las categorías especiales de datos personales a que se refiere el artículo 13 LOPJ. Asimismo, la LO 7/2021 regula el ejercicio de derechos por parte del interesado, en particular, los derechos de información, de acceso a sus datos personales del interesado, derechos a la rectificación de datos inexactos o a que se completen sus datos, supresión de datos personales por infracción de los artículos 6,11 o 13. Además, se establece la limitación de su tratamiento en aquellos casos en que el interesado ponga en duda la exactitud de los datos personales y no pueda determinarse su exactitud o inexactitud, o bien cuando los datos personales tengan que conservarse a efectos probatorios; estos derechos pueden ser limitados o se puede denegar su ejercicio cuando ello resulte necesario y proporcional para la consecución de determinados fines delimitados en el artículo 24 LO 7/2021<sup>44</sup>.

El artículo 26 LO 7/2021 se refiere específicamente a los derechos de los interesados como consecuencia de investigaciones y procesos penales, supuestos en que para el ejercicio de los derechos de información, acceso, rectificación, supresión y limitación del tratamiento se deberá atender a lo previsto en las normas procesales penales cuando los datos personales figuren en una resolución judicial, o en un registro, diligencias o expedientes tramitados en el curso de investigaciones y procesos penales. Si los datos son objeto de tratamiento con fines jurisdiccionales del que sea responsable un órgano del orden jurisdiccional

---

<sup>43</sup> Cuando se trate de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, así como de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, los datos relativos a la salud o a la vida sexual o a la orientación sexual de una persona física, sólo se permite su tratamiento cuando sea estrictamente necesario, con sujeción a las garantías adecuadas para los derechos y libertades del interesado y cuando se cumplan alguna de las circunstancias que menciona el artículo 13 LO 7/2021, a saber: previsión legal; que sea necesario para proteger intereses vitales o derechos y libertades fundamentales del interesado o de otra persona física; o que el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos.

<sup>44</sup> Los fines dispuestos en el artículo 24 LO 7/2021 son: impedir que se obstaculicen investigaciones o procedimientos judiciales; evitar que se cause perjuicio a la prevención, detección, investigación y enjuiciamiento de infracciones penales o a la ejecución de sanciones penales; proteger la seguridad pública; proteger la seguridad nacional y proteger los derechos y libertades de otras personas.

penal, o el Ministerio Fiscal, el ejercicio de estos derechos se debe realizar conforme a lo previsto en la LOPJ, en las normas procesales y en su caso, en el Estatuto Orgánico del Ministerio Fiscal y, a falta de una regulación en dichas normas, se prevé la aplicación de la LO 7/2021.

Del mismo modo, a los efectos del tratamiento de datos personales con fines jurisdiccionales en materia penal es necesario tener en cuenta el contenido de la Circular 2/2022, de 20 de diciembre, de la Fiscalía General del Estado<sup>45</sup>. En esta Circular se reconoce la posibilidad de aplicar las reglas del art 236 *quinquies* LOPJ a la actividad extraprocesal del Ministerio Fiscal, pues el acceso a los datos personales de víctimas, sospechosos, testigos y peritos, como el domicilio personal o el documento de identidad, no contribuye al mejor ejercicio de los derechos de defensa y/o tutela judicial efectiva, y sí supone una limitación innecesaria del derecho a la intimidad.

La citada Circular reconoce que estos datos de naturaleza personal se recojan en documento o archivo aparte y que se adjunten al atestado policial en sobre cerrado o en archivo aparte en caso de remitirse digitalmente y, además, insiste la conveniencia de que la policía judicial ponga una diligencia de constancia con expresión del dato puesto en conocimiento de la persona sospechosa en los casos en que ello sea necesario para garantizar el ejercicio efectivo de su derecho de defensa. Igualmente, en la tramitación de las diligencias de investigación, los datos personales de víctimas, encausados, testigos y peritos deben ser recogidos en documento anexo que se adjuntará a las diligencias en sobre cerrado o archivo aparte, en caso de tratarse de un expediente digital.

Igualmente, se prevé que, al formular denuncia o querrela, los fiscales deberán solicitar al órgano judicial que mantenga el carácter reservado de los datos personales impidiendo su acceso a las partes; los fiscales deberán dictar decreto motivado exponiendo, en su caso, la conveniencia de que la persona sospechosa acceda a alguno de los datos personales para garantizar su derecho de defensa. Además, en el curso de la tramitación de las diligencias de investigación, los fiscales únicamente han de recabar y consignar aquellos datos personales que sean adecuados, pertinentes y limitados a lo necesario para los fines de estas actuaciones, debiéndose siempre tener en cuenta que el derecho a la protección de datos no puede prevalecer sobre el derecho a la tutela judicial efectiva ni impedir al Ministerio Fiscal el ejercicio de sus funciones.

---

<sup>45</sup> BOE núm. 1, de 2 de enero de 2023.

#### IV. EL EJERCICIO DE LOS DERECHOS DE INFORMACIÓN, ACCESO, RECTIFICACIÓN, SUPRESIÓN, OPOSICIÓN Y LIMITACIÓN «HABEAS DATA» CUANDO SE PRODUZCA EL TRATAMIENTO DE DATOS PERSONALES CON FINES JURISDICCIONALES

La protección de datos personales se consigue a través de la consolidación de un elenco de derechos subjetivos a favor de los titulares de los datos personales: información, acceso, rectificación, supresión, oposición y limitación, recogidos en los artículos 15 a 21 del RGPD. El ejercicio de estos derechos se realiza a través de un procedimiento de defensa de la autodeterminación informativa conocido como *habeas data*, el cual se materializa en una acción que sirve de instrumento para proteger los derechos de los titulares de datos personales que están amparados por el sistema de protección frente a los perjuicios que puede ocasionarles el tratamiento de información personal errónea, antigua o falsa, o frente a un uso indebido, no autorizado, potencialmente discriminatorio o lesivo del derecho a la intimidad personal o familiar<sup>46</sup>.

El ejercicio de los derechos derivados del sistema de protección de datos personales presenta algunas especialidades en el ámbito de la Administración de Justicia, como veremos a continuación<sup>47</sup>. En primer lugar, en cuanto al régimen jurídico aplicable, el artículo 236 *octies* LOPJ prevé que las solicitudes de ejercicio de los derechos de acceso, rectificación, cancelación y oposición en relación con los datos tratados con fines jurisdiccionales se tramitarán conforme a las normas que resulten de aplicación al proceso en que los datos fueron recabados, no siendo de aplicación las disposiciones establecidas al efecto por la legislación vigente en materia de protección de datos de carácter personal.

En segundo lugar, a falta de un desarrollo específico en la LOPD para el ámbito de la Administración de Justicia, resulta necesario acudir al contenido del Reglamento 1/2005, de los aspectos accesorios de las actuaciones judiciales del CGPJ<sup>48</sup> (en adelante, RAA), en el que se establecen las disposiciones que afectan principalmente al derecho de acceso, rectificación y cancelación,

---

<sup>46</sup> PÉREZ-LUÑO ROBLEDO, Enrique César, *El procedimiento de habeas data...*, ob. cit., p. 117.

<sup>47</sup> El artículo 2.4 LOPD establece que el tratamiento de datos llevado a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina Judicial, se regirán por lo dispuesto en el RGPD y en la propia LOP, sin perjuicio de las disposiciones de la LOPJ que le sean aplicables.

<sup>48</sup> Acuerdo de 15 de septiembre de 2005, del Pleno del Consejo General del Poder Judicial, por el que se aprueba el Reglamento 1/2005, de los aspectos accesorios de las actuaciones judiciales, publicado en el *BOE* núm. 231, de 27 de septiembre de 2005.

recogiendo especialidades en el procedimiento de ejercicio del *habeas data* en el seno de la Administración de Justicia.

Estas especialidades nacen del contenido de las disposiciones legales que regulan el secreto de sumario en el ámbito penal y la tutela de la intimidad ajena, que se consideran motivos por los que se puede denegar el acceso a datos personales (artículos 84.3 y 4 RAA) y, además, se justifican en la cautela encaminada a impedir que el derecho de autodeterminación informativa se utilice para alterar las circunstancias que constan en el proceso judicial, lo que permite fundamentar la denegación de los derechos de rectificación o de cancelación (artículo 84.5 RAA).

En cuanto al ejercicio de los derechos de acceso, rectificación y cancelación, el artículo 93.1 del RAA establece que podrán reivindicarse por el afectado en la sede del órgano judicial titular del fichero y ante el responsable de este. Así, pues, aunque el derecho de acceso se encuentre regulado en el artículo 13 LOPD, su ejercicio está sujeto a lo dispuesto en el artículo 93 del RAA, por tanto, salvo que el afectado acredite debidamente un interés legítimo al respecto<sup>49</sup>, la solicitud de acceso será denegada cuando los datos afecten a unas diligencias judiciales penales que sean o hayan sido declaradas secretas (artículo 93.3 RAA)<sup>50</sup>; y

---

<sup>49</sup> Del mismo modo, en lo referente al acceso a los datos, el artículo 236 *septies.2* LOPJ señala que en todo caso se denegará el acceso a los datos objeto de tratamiento con fines jurisdiccionales cuando las diligencias judiciales en que se haya recabado la información hayan sido declaradas secretas o reservadas. El primero se refiere sólo a los datos personales que consten en el fichero, mientras que el segundo es un derecho que permite conocer el contenido de las actuaciones judiciales, sin embargo, en muchas ocasiones esta diferencia no es tan nítida puesto que dentro de las resoluciones habrá datos respecto de los cuales será aplicable la protección en cuanto a tales. El derecho de acceso se encuentra regulado por el artículo 15 RGPD como la facultad de todo ciudadano a conocer la información almacenada sobre sí mismo y, en virtud del cual, el interesado tendrá derecho a obtener del responsable del tratamiento la confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, el afectado puede dirigirse al titular del fichero para conocer los datos que sobre él tiene registrados. Véase también el artículo 8.2 de la Carta de Derechos Fundamentales de la Unión Europea.

<sup>50</sup> En lo que respecta a la publicidad de las actuaciones judiciales y el ejercicio del de derecho de acceso, salvo que las actuaciones judiciales hayan sido declaradas secretas o reservadas conforme a la ley, el artículo 234 LOPJ reconoce a los interesados el derecho a que los letrados de la Administración de Justicia y los funcionarios competentes de la oficina judicial les faciliten cuanta información soliciten sobre el estado de las actuaciones procesales, pudiendo examinarlas. Asimismo, se reconoce a las partes y a cualquier persona que acredite un interés legítimo y directo el derecho a obtener, copias simples de los escritos y documentos que consten en los autos, no declarados secretos ni reservados, así como a que se les expidan testimonios y certificados conforme a las leyes procesales. Se permite también, por el artículo 235 LOPJ, el acceso, por quienes no son parte en el procedimiento pero acrediten un interés legítimo y directo, a las resoluciones judiciales, o a determinados extremos de las mismas, o a otras actuaciones procesales, previa disociación, anonimización u otra medida de protección de los datos de carácter personal que las mismos contengan y con pleno respeto al derecho a la intimidad, a los derechos de las personas que requieran un especial deber de tutela o a la garantía del anonimato de las víctimas o perjudicados.

tampoco podrá ejercitarse en perjuicio del derecho a la intimidad de terceros (artículo 93.4 RAA) <sup>51</sup>.

Además, el RAA establece una prohibición de modificación o cancelación de datos, mediante el ejercicio del *habeas data*, cuando esos datos reflejen hechos constatados en un procedimiento jurisdiccional o en un expediente gubernativo (artículo 93.5 RAA) <sup>52</sup>. En definitiva, todas estas medidas están encaminadas a evitar que el ejercicio de derechos de protección de datos impida o perjudiquen la función jurisdiccional.

Por otro lado, en lo que respecta al derecho de oposición, su ejercicio tiene difícil aplicación frente a la Administración de Justicia. En la práctica resulta complicado encontrar una vía para hacer prevalecer el interés particular del afectado por el tratamiento de los datos sobre el interés general de la función jurisdiccional para que prospere la oposición ante el órgano correspondiente. No obstante, no se puede descartar totalmente la posibilidad del ejercicio del derecho de oposición, por ejemplo, en los casos en que el juez o el letrado de la Administración de Justicia incurrieran en algún tipo de exceso a la hora de recabar datos del afectado, en este supuesto podría ejercitarse el derecho ante el responsable del fichero o del tratamiento de acuerdo con lo que prevé el RAA.

En cuanto al procedimiento de *habeas data* en el seno de la Administración de Justicia, el RAA mantiene en su artículo 93.1 que las solicitudes de acceso, rectificación y cancelación deberán formularse ante el responsable del fichero, de acuerdo con lo establecido en el artículo 91 RAA. En sintonía con lo dispuesto en el RGPD y en la LOPD, el plazo para obtener la rectificación o la cancelación, cuando procedan, se fija en diez días, mientras que el plazo establecido para que el responsable del fichero resuelva sobre el acceso será de un mes. Además, 17.2 LOPD establece legalmente la gratuidad de los procedimientos relativos al

---

<sup>51</sup> El derecho de acceso, como contenido del derecho a la protección de datos en la Administración de Justicia, difiere del derecho de acceso a las actuaciones judiciales que forma parte del contenido del derecho a la tutela judicial efectiva, esta distinción es importante para evitar equívocos sobre el régimen aplicable.

<sup>52</sup> El uso de la expresión “datos que reflejen hechos constatados” ha sido criticada por parte de la doctrina, por entender que sólo se puede afirmar que un hecho ha quedado constatado cuando haya sido declarado probado en la resolución judicial que ponga fin al proceso, lo que daría lugar a que no puedan ser modificados o cancelados, de acuerdo con este artículo, únicamente cuando se trate de hechos probados, excluyendo el resto de datos que de acuerdo con el RGPD sean datos personales, véase al respecto MARTÍN-CASALLO LÓPEZ, Juan José, «La agencia de protección de datos y los ficheros de datos jurisdiccionales. La protección del derecho a la intimidad de las personas (fichero de datos)», *Cuadernos de Derecho Judicial*, vol. 13, 1997, pp. 87 y ss. RODRÍGUEZ ROCA, Alejandro, *La protección de datos personales en los juzgados...*, ob. cit.

ejercicio de los derechos del afectado, así, prevé que «no se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación y cancelación».

Finalmente, es preciso señalar que cabe la posibilidad de solicitar la impugnación de las resoluciones expresas o presuntas denegatorias de cualquiera de las solicitudes de acceso, cancelación o rectificación ante la Administración de Justicia, así, el artículo 94 RAA remite al procedimiento previsto en su artículo 4.3. RAA, en el que se dispone que, sin perjuicio de lo establecido en las leyes de procedimiento, el acuerdo denegatorio del letrado de la Administración de Justicia 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 letrado, ni se hubiere expedido el testimonio o certificación solicitados, ni realizada tampoco la exhibición de que se trate, se entenderá que la petición ha sido denegada y, en su consecuencia, el interesado podrá ejercitar ante el juez o presidente el derecho de revisión mencionado anteriormente. 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<sup>53</sup>.

## V. CONCLUSIONES

La protección de datos requiere de la existencia de un sistema eficaz, sustentado en un desarrollo normativo completo y preciso, por lo que, la insuficiencia del marco normativo actual que hace muy difícil resolver los conflictos que se ponen de manifiesto entre las normas procesales y las de protección de datos.

El sistema de protección de datos no se ha desarrollado poniendo el énfasis en la Administración pública, ni mucho menos en la Administración de Justicia, la mayoría de sus normas están encaminadas a salvaguardar los derechos de los ciudadanos frente a la actuación de las empresas privadas. Esta falta de especificidad tiene como efectos que haya dificultades para coordinar el contenido de las normas de protección de datos con las normas de organización de la Administración de Justicia, así, mientras el sistema de protección de datos se basa en la garantía de la privacidad, las normas procesales desarrollan un sistema

---

<sup>53</sup> Acuerdo de 26 de julio de 2000, del Pleno del Consejo General del Poder Judicial, por el que se aprueba el Reglamento 1/2000, de los Órganos de Gobierno de Tribunales, publicado en el *BOE* núm. 216, de 8 de septiembre de 2000.



basado en la publicidad, lo cual es un punto de partida en el que resulta difícil la conciliación de ambos sistemas, y una mera remisión – como ha hecho en la LOPD- no permite dar una adecuada respuesta a toda la problemática práctica que se puede presentar en esta materia.

Se requiere un desarrollo más específico de algunos aspectos relevantes del sistema de protección, el cual debe realizarse a través de una Ley Orgánica, al tratarse de un derecho fundamental. En particular, entendemos que el legislador debe concretar el contenido del procedimiento por el cual se ejercitan los derechos de datos personales: información, acceso, rectificación, supresión, oposición y limitación, recogidos en los artículos 15 a 21 del RGPD y, en particular, resulta necesario revisar y actualizar la regulación del derecho de acceso a las actuaciones judiciales, ya que su tratamiento afecta directamente al derecho de defensa.

Además, la posición de responsable del tratamiento de datos personales incorporados en ficheros judiciales, en los términos del sistema general de protección de datos, pero adaptado a la Administración de Justicia es de naturaleza compleja. Por un lado, tenemos a los órganos jurisdiccionales y dentro de éstos, los letrados de la Administración de Justicia y los jueces, según el ejercicio de sus respectivas competencias son los responsables funcionales del tratamiento de los datos y, por otro lado, el CGPJ que es quien, de acuerdo con lo previsto LOPJ y el RGPD, tiene la capacidad para determinar la finalidad, contenido y uso de los ficheros judiciales, facultad que, de acuerdo con el propio RGPD, se atribuye al responsable del tratamiento, en atención de dicha facultad, el CGPJ debe adoptar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento que se lleva a cabo en los órganos jurisdiccionales cumple con el sistema de protección de datos personales.

Otro aspecto relevante que requiere una mayor reflexión es el que se refiere a la independencia de la autoridad de control la cual, de acuerdo con las disposiciones del RGPD, debe disponer de recursos suficientes para el ejercicio de sus funciones. Así, aunque el órgano llamado a desempeñar las funciones de la autoridad de control en nuestro caso es el CGPJ, con competencia para el control de los juzgados y tribunales, preocupa el hecho de que la financiación de los medios materiales del CGPJ y de los órganos jurisdiccionales dependa, en su caso, del Ministerio de Justicia o de la Comunidad Autónoma correspondiente, lo cual plantea la necesidad de concretar también el papel que desempeñan las Administraciones con competencia en la dotación de medios, pues se trata de un

elemento fundamental para garantizar la protección de los datos personales que obran en manos de la Administración de Justicia.

## REFERENCIAS BIBLIOGRÁFICAS

- Bayo Delgado, Joaquín, «La protección de datos de la Unión Europea: la Administración de Justicia», en *Revista Derecho y Jueces El Derecho*, núm. 27, 1 de septiembre de 2005.
- Cremades López de Teruel, Fernando Javier, «La nueva Ley Orgánica de Protección de Datos y el Poder Judicial: un juego de mercaderes en el templo del Reglamento General de la Unión Europea», *Diario La Ley*, núm. 9430, 2019.
- Cremades López de Teruel, Fernando Javier, Sancho Alonso, Jesús, «Protección de datos y Poder Judicial», *Diario La Ley*, núm. 9293, Sección Tribuna, noviembre de 2018.
- Delgado Martín, Joaquín, «Reflexiones sobre la protección de datos personales en la Administración de Justicia», *Diario La Ley*, núm. 9363, Sección Tribuna, 21 de febrero de 2019.
- Fresneda Plaza, Felipe, «Régimen sancionador y protección de datos», *Cuadernos Digitales de Formación del Consejo General del Poder Judicial*, núm. 29, 2012.
- Frieyro Elícegui, Sofía, «Tratamiento de datos personales en el orden jurisdiccional penal. Protección de menores de edad y personas con discapacidad necesitadas de especial protección», *Diario La Ley*, Sección Doctrina, 8 de febrero de 2023.
- Guerrero Picó, María del Carmen, *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, Thomson Civitas-Aranzadi, Cizur Menor, Madrid, 2006.
- Lesmes Serrano, Carlos, «Las potestades de fiscalización de la agencia española de protección de datos en el ámbito de la Administración de Justicia», *Revista de Jurisprudencia El Derecho*, núm. 1, 2012.
- Lucena Cid, Isabel Victoria, «La protección de la intimidad en la era tecnológica: hacia una reconceptualización», *Revista internacional de pensamiento político*, I época, volumen 7, 2012, pp. 117-144.
- Marcos Ayjón, Miguel, «La protección de datos de carácter personal en la Oficina Judicial Penal», *La Ley Penal*, núm. 135, noviembre-diciembre 2018.
- Marcos Ayjón, Miguel, *La protección de datos de carácter personal en la justicia penal*, Bosch, Barcelona, 2020.
- Martín-Casallo López, Juan José, «La agencia de protección de datos y los ficheros de datos jurisdiccionales. La protección del derecho a la intimidad de las personas (fichero de datos)», *Cuadernos de Derecho Judicial*, vol. 13, 1997, pp. 87-150.
- Mcintyre Cooley, Thomas, *A Treatise on the Law of Torts, Or the Wrongs which Arise Independently of Contract*, vol. 1, Callaghan & Co., Chicago, 1907.

- Pérez Gil, Julio, «Investigación penal y nuevas tecnologías: algunos de los retos pendientes», *Revista Jurídica de Castilla y León*, núm. 7, 2005, pp. 211-234.
- Pérez-Luño Robledo, Enrique César, *El procedimiento de habeas data: El derecho procesal ante las nuevas tecnologías*, Dykinson, Madrid, 2017.
- Rodríguez Roca, Alejandro, *La protección de datos personales en los juzgados y tribunales. Un enfoque desde la perspectiva laboral*, *La Ley*, Madrid, 2022.
- Rodríguez Valls, María Teresa, «Principio de publicidad procesal y derecho a la protección de datos de carácter personal: aproximación a la problemática actual en Juzgados y Tribunales españoles», *La ley penal: revista de derecho penal, procesal y penitenciario*, núm. 71, 2010.
- Sancho Alonso, Jesús, *La función institucional del secretario judicial-letrado de la Administración de Justicia*. Tesis dirigida por Ángel Sánchez Blanco, Universidad de Málaga, Departamento de Derecho público, 2017, disponible en: <https://riuma.uma.es/xmlui/handle/10630/16630>
- Sempere Samaniego, Javier, «Tribunal Justicia Unión Europea se pronuncia sobre el concepto de “función judicial” del art. 55.3 RGPD», *La Ley privacidad*, núm. 12 (abril-junio), Sección Espacio Europeo de protección de datos, 2022.
- Solar Calvo, María del Puerto, «Nueva regulación europea en protección de datos. Urgente necesidad de una normativa nacional», *Unión Europea Aranzadi*, núm. 7, 2018.
- Troncoso Reigada, Antonio, *La Protección de Datos Personales. En Busca del Equilibrio*, Tirant Lo Blanch, Valencia, 2011.
- Warren II, Samuel D., Brandeis, Louis, «The right to privacy», *Harvard Law Review*, Vol. IV, núm. 5, diciembre 15, 1890.

MATI DE LOS ÁNGELES HERNÁNDEZ ALFARO  
Universidad Pontificia Comillas  
Área de Derecho Mercantil  
Profesora Colaboradora Asistente de la  
Facultad de Derecho (ICADE),  
Departamento de Derecho Económico y Social  
[mlahernandez@comillas.edu](mailto:mlahernandez@comillas.edu)  
ORCID: 0000-0002-1924-6647

