RESOLUCIÓN

Exp.: 103/2025
Archivo de actuaciones
Fecha entrada: 1/10/2025

ANTECEDENTES

PRIMERO.- Con fecha 1 octubre de 2025 tiene entrada en el Registro general del Consejo General del Poder Judicial, reclamación efectuada por D. Dámaso, referida al Juzgado de Juzgado de Primera Instancia núm. 1 de DIRECCION000, cuyo contenido es el siguiente:

«1. Incorporación indebida de documento patrimonial: En el curso del procedimiento de ejecución NUM000 tramitado ante el Juzgado de Primera Instancia n.º 1 de DIRECCION000, la Letrada de la Administración de Justicia D.ª Estrella incorporó a las actuaciones un documento de carácter patrimonial relativo al ejecutado (el reclamante), sin que mediara resolución judicial habilitante ni petición de parte que justificase tal aportación. Dicho documento, de naturaleza estrictamente privada, contenía información financiera y patrimonial detallada del aquí reclamante y de terceros ajenos al procedimiento, revelando datos especialmente sensibles (cuentas bancarias, deudas, identificaciones de terceros, entre otros). (Se adjunta como documento nº 1 el documento que se dio traslado a las partes):

2. Traslado de datos sensibles a la parte contraria: La mencionada Letrada trasladó íntegramente este documento patrimonial a la parte contraria (parte ejecutante), es decir, puso a disposición de la contraparte toda la información personal y de terceros contenida en él. Tal entrega se realizó sin aplicar anonimización, disociación ni restricción alguna sobre los datos, proporcionando a la parte adversa datos sensibles que excedían con mucho de lo necesario para la ejecución. No consta que la contraparte hubiera solicitado dicho documento ni que existiera autorización judicial específica para compartir esa información confidencial.

3. Ausencia de habilitación legal y oposición expresa: El reclamante, al tener conocimiento de esta actuación, manifestó inmediatamente su más firme oposición a la difusión de sus datos personales y patrimoniales, advirtiendo que no existía base legal ni motivo procesal que amparase tal comunicación. No se dictó en ningún momento resolución judicial que ordenara la entrega de ese documento ni se apreció relevancia procesal en su contenido para la ejecución en trámite. Pese a ello, la Letrada actuante procedió a compartir la totalidad de los datos, incurriendo así en una clara extralimitación de sus funciones.

4. Que resulta especialmente alarmante que, en el marco de dicha actuación irregular, se haya llegado incluso a trasladar a terceros información personal de mi representado correspondiente a hechos ocurridos hace más de treinta años,

concretamente la circunstancia de haber percibido en su día una prestación por desempleo.

Esta información, absolutamente irrelevante para el objeto del procedimiento de ejecución, carece de toda conexión con la finalidad procesal perseguida y su comunicación constituye un exceso manifiesto y una vulneración flagrante del principio de minimización de datos previsto en el artículo 5.1.c) del Reglamento (UE) 2016/679 (RGPD).

La cesión de datos históricos, desvinculados de cualquier interés legítimo actual, no solo supone una intromisión injustificada en la esfera privada del afectado, sino que evidencia una falta total de control y de criterio jurídico por parte del órgano que ordenó o permitió dicha difusión, pues nada justifica que se revele a la parte contraria –ni a ningún tercero– información obsoleta, archivada y ajena a los hechos litigiosos.

Este episodio ilustra con nitidez la dimensión de la vulneración sufrida, ya que la difusión de datos personales de naturaleza estrictamente laboral y de hace tres décadas no responde a ninguna finalidad legítima, proporcional ni necesaria, incurriendo por tanto en una infracción directa del principio de limitación de finalidad (art. 5.1.b RGPD) y del deber de confidencialidad previsto en el artículo 5 de la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

5. Grave perjuicio al derecho fundamental del reclamante: Como consecuencia de lo anterior, el reclamante ha visto gravemente vulnerado su derecho fundamental a la protección de datos personales, consagrado en el artículo 18.4 de la Constitución Española.

Sus datos financieros privados –e incluso datos de terceras personas– han quedado expuestos a quien no debía conocerlos, generando un perjuicio irreparable en su privacidad y seguridad jurídica. Esta situación le ha ocasionado una profunda inquietud, al haberse desvelado información íntima y sensible al margen de cualquier cauce legal.

6. Que esta parte tuvo conocimiento de esta difusión de sus datos al acceder al expediente, que le fue conferido el 05/09/2025, donde comprobó que la otra parte había recibido copia de su informe patrimonial completo. Inmediatamente expresó su disconformidad ante el órgano judicial, dejando constancia de la posible vulneración de su derecho fundamental a la protección de datos. Pese a ello, no consta hasta la fecha la adopción de medidas efectivas por parte del Juzgado para reparar la situación (por ejemplo, retirar o anonimizar datos del informe, o limitar su acceso) ni para prevenir un uso indebido ulterior de los datos comunicados.

7. Que los hechos descritos implican un tratamiento de datos personales no consentido ni legalmente autorizado, consistente en la comunicación o divulgación de datos a tercero (la contraparte procesal) fuera de los supuestos previstos en la normativa. Esta actuación vulnera frontalmente los principios y garantías establecidos en la legislación vigente de protección de datos, tal como se desarrolla en los Fundamentos Jurídicos siguientes.

8. Por todo lo expuesto en los hechos anteriores, el reclamante considera que se ha producido una infracción muy grave en materia de protección de datos por parte de la Sra. Estrella, Letrada de la Administración de Justicia, con responsabilidad directa del órgano judicial en que presta servicios. Procede por ello que ese Consejo General del Poder Judicial, a través de la Subdirección General de Inspección de Datos, examine los hechos y actúe en consecuencia.

FUNDAMENTOS JURÍDICOS:

1. Vulneración de los principios fundamentales de protección de datos (RGPD y LOPDGDD): La actuación descrita infringe frontalmente los principios de licitud, minimización y confidencialidad en el tratamiento de datos personales recogidos en el Reglamento (UE) 2016/679 (RGPD). En particular:

(a) Principio de licitud: no existió base jurídica válida ni autorización para el tratamiento y comunicación de los datos (art. 6 RGPD);

(b) Principio de minimización de datos: se comunicaron datos excesivos y ajenos a los estrictamente necesarios para la finalidad del proceso, vulnerando la limitación de finalidad y proporcionalidad; y

(c) Principio de integridad y confidencialidad: la Letrada incumplió el deber de secreto y seguridad, al revelar información personal de manera no autorizada. La Ley Orgánica 3/2018, de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD) también consagra estos principios y su infracción está tipificada como muy grave. De hecho, el art. 72.1.a) LOPDGDD considera infracción muy grave el tratamiento de datos vulnerando los principios del art. 5 RGPD, y el art. 72.1.i) califica igualmente como muy grave la vulneración del deber de confidencialidad. En el presente caso, tanto la falta de licitud de la cesión (sin consentimiento ni habilitación legal) como la quiebra de la confidencialidad y la ausencia de minimización en los datos entregados suponen una vulneración sustancial de la normativa vigente en protección de datos personales.

2. Carácter desproporcionado de la entrega de datos – Jurisprudencia constitucional y europea: La revelación masiva de información sensible efectuada por la Letrada resulta absolutamente desproporcionada y contraria a la exigible tutela del derecho fundamental a la protección de datos. Según la jurisprudencia del Tribunal Constitucional, este derecho fundamental otorga a cada persona un "poder de disposición y control" sobre sus datos personales frente a terceros, incluidas las Administraciones Públicas Así lo han establecido, entre otras, las SSTC 94/1998 y 292/2000, reconociendo la autonomía del derecho a la protección de datos y su función garante de la privacidad más allá del derecho a la intimidad clásica [6]. En consecuencia, ninguna autoridad pública puede disponer de datos personales de un ciudadano y comunicarlos a terceros sin habilitación expresa y respetando los principios de necesidad y proporcionalidad. Esta exigencia ha sido reiterada también por el Tribunal de Justicia de la Unión Europea (TJUE). En el asunto C‑92/09 y C‑93/09 (Caso Schecke, 2010), el TJUE anuló una norma europea que obligaba a publicar datos personales de beneficiarios de ayudas, precisamente por considerarla desproporcionada y contraria al derecho fundamental a la protección de datos. El TJUE enfatizó que incluso cuando se persiguen fines legítimos (como la

transparencia), deben arbitrarse medidas menos intrusivas y limitar la difusión de datos personales a lo estrictamente necesario, evitando divulgaciones indiscriminadas. En palabras del propio Tribunal, si un derecho o interés concurre con el derecho a la protección de datos, este último solo puede ceder "en la medida estrictamente necesaria" para salvaguardar el interés prevalente. En nuestro caso, la falta de anonimización o filtro alguno al compartir la información patrimonial del reclamante con la contraparte supone una clara transgresión de este principio de proporcionalidad: no se valoró ninguna medida menos lesiva (por ejemplo, ocultar datos irrelevantes o sensibles de terceros) y se sacrificó totalmente el derecho del afectado sin justificación jurídica. En este sentido, la actuación diligente y conforme a Derecho habría debido limitarse exclusivamente a comunicar la existencia de cuentas corrientes con saldo suficiente para atender la ejecución, sin necesidad de aportar más detalle ni dato identificativo alguno.

Sin embargo, se ha procedido a trasladar a la parte contraria información desmesurada y totalmente innecesaria, incluyendo el número completo de los IBAN bancarios, los movimientos asociados a dichas cuentas, así como datos de carácter estrictamente personal y carentes de toda relevancia procesal, tales como la fecha en que mi representado obtuvo su permiso de conducir o la fecha de renovación de su Documento Nacional de Identidad, e incluso la referencia a que hace más de treinta años percibió una prestación por desempleo.

Esta transmisión indiscriminada y carente de filtro alguno constituye una vulneración palmaria de los principios de necesidad y minimización de datos (artículo 5.1.c del RGPD), además de una quiebra del deber de confidencialidad y proporcionalidad exigido por el artículo 5 de la Ley Orgánica 3/2018.

La cesión de tal volumen de información personal, obsoleta y ajena al objeto del proceso, no responde a ninguna finalidad legítima ni resulta necesaria para el cumplimiento de la función jurisdiccional, suponiendo una injerencia injustificada en la intimidad del afectado y una infracción especialmente grave del derecho fundamental a la protección de datos personales.

3. Inexcusable responsabilidad del órgano judicial – La excusa informática (@Adriano) no exime del cumplimiento normativo: El argumento esgrimido por el Juzgado –basado en pretendidas limitaciones del sistema informático Adriano para seleccionar la información a compartir– carece de validez jurídica. Ninguna deficiencia técnica puede servir de excusa para vulnerar derechos fundamentales ni exonerar a la Administración de Justicia de sus deberes legales. Tanto el RGPD como la LOPDGDD imponen a los responsables del tratamiento (incluidos los órganos judiciales, cuando gestionan datos personales) la obligación proactiva de garantizar la seguridad y confidencialidad de los datos mediante medidas técnicas y organizativas adecuadas (principio de "accountability" o responsabilidad proactiva, arts. 5.2 y 24 RGPD, y principio de "privacy by design and by default", art. 25 RGPD). En este sentido, si el sistema informático presenta deficiencias, corresponde a los responsables encontrar soluciones (por ejemplo, extracción manual de los datos sensibles antes del traslado, uso de formatos segregados, autorización judicial previa, etc.), pero nunca trasladar automáticamente la carga al ciudadano afectado

permitiendo una divulgación ilícita de sus datos. La propia LOPDGDD en su artículo 32 obliga al bloqueo de datos cuando proceda, y los artículos 25 y 32 del RGPD exigen garantizar que por defecto solo se traten los datos necesarios y protegerlos con medidas de seguridad apropiadas. Es claro que en la actuación objeto de reclamación no se observó tal diligencia. Admitir que un fallo de software justifica la entrega masiva de datos personales equivaldría a vaciar de contenido las garantías legales, algo inadmisible en un Estado de Derecho. El Tribunal Supremo ha señalado reiteradamente que las normas de protección de datos deben cumplirse en todo caso por las Administraciones, anulando incluso disposiciones reglamentarias que las contradigan. Así, por ejemplo, la STS de 15 de julio de 2010 (Sala 3ª) declaró nulo el art. 18 del Reglamento de desarrollo de la LOPD por ser contrario a Derecho, enfatizando la prevalencia de la ley y de los derechos fundamentales sobre cualquier deficiencia operativa o reglamentaria [9]. En suma, la responsabilidad del órgano judicial es ineludible: la invocación de Adriano no exime de culpa ni repara la infracción cometida, y corresponde al propio CGPJ asegurar que los medios técnicos se adecuen a las exigencias legales, no al revés.

4. Calificación jurídica de los hechos – Infracciones muy graves (LOPDGDD) y falta disciplinaria muy grave (LOPJ): Los hechos relatados, a juicio del reclamante, configuran infracciones muy graves en materia de protección de datos, en los términos previstos por la LOPDGDD. Como se ha indicado, se ha vulnerado sustancialmente el art. 5 RGPD (principios básicos) y se ha incumplido el deber de confidencialidad sobre datos personales, supuestos ambos recogidos en el art. 72.1 letras a) e i) LOPDGDD como infracciones muy graves. De igual modo, de haber datos especialmente protegidos o de terceros no parte en el proceso, se habría contravenido el régimen reforzado de categorías especiales (art. 9 RGPD), lo que también constituye infracción muy grave (art. 72.1.e LOPDGDD). En consecuencia, nos hallamos ante una vulneración gravísima del derecho a la protección de datos, que exige una respuesta a la altura de su gravedad. Cabe recordar que, tratándose de un responsable del tratamiento perteneciente al sector público (una oficina judicial), el art. 77 LOPDGDD establece que la Agencia de Protección de Datos u órgano de control competente deben instar la actuación disciplinaria interna cuando se aprecien indicios suficientes de infracción.

Dicho de otro modo, en el sector público español las sanciones económicas del RGPD suelen sustituirse por medidas disciplinarias a los responsables individuales de la infracción. Esto enlaza con la normativa específica del ámbito judicial: la conducta descrita podría constituir una falta disciplinaria muy grave en los términos de la Ley Orgánica del Poder Judicial (LOPJ). En particular, el art. 41.12 LOPJ califica como falta muy grave de las autoridades judiciales "la revelación de hechos o datos conocidos en el ejercicio de su función... cuando cause algún perjuicio a la tramitación de un proceso o a cualquier persona". Es evidente que la revelación aquí denunciada, realizada por una Letrada de la Administración de Justicia en ejercicio de sus funciones, ha causado perjuicio tanto al proceso (al introducir elementos ajenos y potencialmente impugnables) como, especialmente, a la persona afectada por la difusión de sus datos. Por analogía y por los principios generales aplicables al

personal al servicio de la Administración de Justicia, dicha conducta debería ser objeto de expediente disciplinario y sanción proporcional a su extrema gravedad. No solo ha existido un incumplimiento de la normativa de protección de datos, sino también una quiebra del deber de custodia y reserva de las actuaciones judiciales. La STS de 8 de febrero de 2012 (Sala 3ª) ya subrayó la importancia de ceñirse a la legalidad en el tratamiento de datos personales, llegando a invalidar preceptos que la desbordaban. Por tanto, corresponde ahora actuar con la misma firmeza: los responsables de esta infracción deben ser investigados y sancionados en el marco disciplinario que corresponda, a fin de restablecer la legalidad y prevenir que hechos similares vuelvan a ocurrir.

En resumen, existe una clara Infracción de los principios de licitud y minimización de datos (proporcionalidad) – arts. 5.1.a) y 5.1.c) RGPD. En este sentido, el principio de licitud exige que todo tratamiento de datos personales se ampare en una base jurídica legítima (art. 6 RGPD). A su vez, el principio de minimización de datos obliga a que únicamente se traten los datos adecuados, pertinentes y limitados a lo necesario en relación con los fines legítimos del tratamiento (art. 5.1.c RGPD). En este asunto, la comunicación del documento patrimonial completo al litigante contrario no cumple con ninguno de estos principios: no era necesaria para la finalidad procesal (resolver el litigio) y abarcó datos excesivos y ajenos al objeto del pleito. Según criterio de la Agencia Española de Protección de Datos (AEPD), si un tratamiento de datos por una Administración no es "necesario" para el cumplimiento de su misión de interés público o ejercicio de potestades, dicho tratamiento carece de base jurídica y además infringe el principio de minimización del art. 5.1.c RGPD. En este caso, al no ser necesario volcar la integridad de la información patrimonial del reclamante en el procedimiento, la Letrada actuó sin cobertura en una base de licitud válida y contravino el deber de minimizar los datos tratados. Debe recordarse que el artículo 6.1.e) RGPD (tratamiento necesario por interés público o ejercicio de poderes públicos) solo legitima el tratamiento cuando este es estrictamente necesario para la misión pública encomendada; fuera de ese supuesto, el tratamiento deviene ilícito. Además, la propia LOPDGDD enfatiza que el tratamiento por autoridades públicas solo podrá fundarse en el ejercicio de funciones públicas cuando derive de una norma con rango de ley que lo ampare (art. 8.2 LOPDGDD), condición que aquí no concurría en absoluto. No existe en nuestro ordenamiento jurídico ninguna disposición legal ni mandato judicial específico que habilitara a la Letrada para compartir la totalidad de los datos patrimoniales del reclamante con terceros en este procedimiento; por tanto, la comunicación efectuada carece de licitud y vulnera gravemente el artículo 6 del RGPD.

En apoyo de lo anterior, cabe mencionar que la Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial (CGPJ) – autoridad competente en materia de ficheros jurisdiccionales– ha reiterado la obligatoriedad de respetar el principio de proporcionalidad/minimización en el contexto de la Administración de Justicia. Por ejemplo, en diversas resoluciones se ha ordenado a los órganos judiciales "actuar con diligencia debida para consultar los

datos patrimoniales solo previa resolución judicial, o minimizar los datos del ciudadano, que deben ser adecuados, pertinentes y no excesivos en relación con los fines". Justamente lo contrario ocurrió en el presente caso, donde se realizó una consulta y difusión de datos patrimoniales sin resolución judicial previa y sin filtro alguno de relevancia o necesidad, excediendo con creces lo permitido y requerido para la finalidad procesal.

Existe una clara vulneración de los principios de integridad y confidencialidad – art. 5.1.f) RGPD, art. 5 LOPDGDD. Y es que el RGPD impone que los datos personales sean tratados garantizando su seguridad y confidencialidad, protegiéndolos contra accesos o comunicaciones no autorizadas (principio de integridad y confidencialidad, art. 5.1.f RGPD). Este principio se ve reforzado en el derecho interno por el artículo 5 de la LOPDGDD, que consagra el deber de confidencialidad: todas las personas que intervengan en cualquier fase del tratamiento de datos personales (especialmente los empleados públicos en sus funciones) están sujetas al deber de secreto y confidencialidad respecto de los datos a los que acceden o tratan. Dicho deber implica que la información personal obtenida en el ejercicio de sus funciones no puede ser divulgada a terceros salvo autorización legal expresa o cumplimiento estricto de las finalidades para las que fue recabada.

En el caso que nos ocupa, la Letrada de la Administración de Justicia incumplió de forma grosera su deber de confidencialidad al divulgar íntegramente a la parte contraria datos personales del reclamante y de terceros QUE NO DEBIERON TRASCENDER EL ÁMBITO INTERNO DEL PROCEDIMIENTO DE LA ADMINISTRACION DE JUSTICIA. Esta comunicación no autorizada de datos constituye en sí misma una violación de la seguridad/confidencialidad de los datos personales, equiparable a una brecha de datos en términos del RGPD (art. 4.1.12 RGPD: acceso o divulgación no autorizada de datos personales). El resultado fue que datos sensibles quedaron expuestos a personas ajenas sin control ni justificación, comprometiendo la integridad de la información (pues pasó a un ámbito no previsto) y la confidencialidad debida.

En suma, la actuación denunciada ha vulnerado los principios fundamentales del tratamiento de datos (art. 5 RGPD) y carece de toda base de licitud (art. 6 RGPD), constituyendo una infracción muy grave de la normativa de protección de datos. Así lo tipifica expresamente el artículo 72.1 de la LOPDGDD, al calificar como infracciones muy graves tanto "el tratamiento de datos personales vulnerando los principios establecidos en el artículo 5 del RGPD" (letra a) como "el tratamiento de datos sin concurrir alguna de las condiciones de licitud del artículo 6 RGPD" (letra b)[8].

Igualmente, se considera muy grave "la vulneración del deber de confidencialidad" (art. 72.1.i LOPDGDD), precepto plenamente aplicable a los hechos, dada la quiebra del secreto que debía guardarse sobre los datos difundidos.

5. Jurisprudencia y precedentes aplicables. La gravedad de las conductas descritas halla reflejo en la jurisprudencia y en pronunciamientos de las autoridades de control. El Tribunal Constitucional, en su sentencia 292/2000, ya afirmó que el contenido esencial del derecho fundamental del art. 18.4 CE impide la difusión de datos personales sin consentimiento ni habilitación legal, destacando que debe existir

"nítida conexión [...] entre la información personal recogida y el legítimo objetivo" que la justifica, así como observancia de los principios de congruencia, necesidad y racionalidad en la utilización de los datos. En el ámbito específico de la justicia, como se ha indicado, el órgano de gobierno de los jueces (CGPJ) a través de su Dirección de Protección de Datos ha venido estimando reclamaciones de ciudadanos en supuestos similares de tratamiento irregular de datos por juzgados, llegando incluso a promover acciones disciplinarias contra los responsables.

Cabe citar, a título ilustrativo, un expediente resuelto en diciembre de 2021 en el que un magistrado accedió a datos fiscales de un familiar sin resolución judicial: dicho proceder fue considerado contrario a la normativa y el órgano de supervisión ordenó el traslado de las actuaciones al Promotor de la Acción Disciplinaria para la depuración de responsabilidades. Este precedente guarda clara analogía con el presente caso (acceso/comunicación de datos sin respaldo judicial ni legal), evidenciando la necesidad de adoptar igualmente medidas sancionadoras y disciplinarias frente a la Letrada aquí reclamada.

Asimismo, el Reglamento General de Protección de Datos prevé en su artículo 83 sanciones severas para infracciones graves de este tipo, y aunque el ordenamiento español –en uso de la habilitación del art. 83.7 RGPD– exime de multas económicas a las Administraciones Públicas, no por ello las conductas quedan impunes. Al contrario, el artículo 77 LOPDGDD establece un régimen sancionador específico para responsables públicos, disponiendo que en caso de infracciones la autoridad de control (AEPD o, en su caso, el órgano competente del CGPJ) imponga SANCIONES DISCIPLINARIAS y adopte las medidas necesarias para asegurar el cese de la infracción, pudiendo además instar el inicio de actuaciones disciplinarias contra los funcionarios responsables. Este "régimen blando" sancionador para el sector público no resta importancia a la infracción cometida, sino que traslada la respuesta punitiva al terreno disciplinario interno, a fin de exigir responsabilidades al infractor sin menoscabo del erario público. En consecuencia, resulta procedente que, verificada la vulneración denunciada, se dicte apercibimiento o sanción no pecuniaria contra el órgano responsable y, especialmente, se dé traslado al órgano competente para la instrucción de un expediente disciplinario a D.ª Estrella por posible falta muy grave en el ejercicio de sus funciones.

6. Infracción de derechos de terceros afectados. No puede obviarse que la acción reclamada no solo lesiona el derecho del aquí reclamante, sino también los derechos de terceras personas cuyos datos fueron indebidamente comunicados. El RGPD y la LOPDGDD tutelan los datos personales de todas las personas físicas, de modo que la difusión no autorizada de datos de terceros (por ejemplo, familiares o cotitulares mencionados en el informe patrimonial) configura igualmente una vulneración del derecho fundamental a la protección de datos de esos terceros. Si bien dichos afectados podrían plantear sus propias reclamaciones, se deja expresamente constancia en este escrito de la infracción cometida respecto de los datos de terceros, en cuanto agrava la conducta y evidencia un alcance mayor del perjuicio. El principio de lealtad y transparencia (art. 5.1.a RGPD) también se ve quebrantado, puesto que esas personas no fueron informadas ni consintieron que su

información personal fuese revelada en el marco de este proceso. Este aspecto debería ser valorado en la presente reclamación, ya que subraya la necesidad de adoptar medidas no solo para reparar el daño al reclamante, sino para prevenir que datos de personas ajenas al procedimiento sean expuestos indebidamente, evitando así la multiplicación de víctimas de la vulneración.

Por todo lo expuesto, el reclamante considera acreditada una presunta infracción de la normativa de protección de datos de carácter personal, imputable a la Letrada de la Administración de Justicia D.ª Estrella, en el contexto de un tratamiento de datos realizado en el ámbito judicial sin cobertura legal, vulnerando los principios de proporcionalidad, minimización, integridad y confidencialidad, y afectando tanto a sus datos personales como a los de terceros. En base a ello, y al amparo de los artículos 77 y 79 del RGPD (derecho a presentar reclamación ante la autoridad de control y a la tutela efectiva), así como de los artículos 63 y 64 de la LOPDGDD (legitimación y procedimientos ante la AEPD), formula la siguiente:

PETICIÓN:

Por todo lo expuesto, solicito respetuosamente a esa Subdirección General de Inspección de Datos del Consejo General del Poder Judicial que adopte las siguientes medidas:

Primero: Inicio de actuación investigadora: Que se admita a trámite la presente reclamación y se proceda a investigar exhaustivamente los hechos denunciados, recabando la información necesaria del Juzgado de Primera Instancia n.º 1 de DIRECCION000 y de cualquier otro organismo competente, a fin de verificar la efectiva vulneración del derecho fundamental a la protección de datos personales del reclamante. Se solicita que, tras la oportuna investigación, se emita por ese órgano un informe o resolución concluyendo sobre las infracciones cometidas.

Segundo: Incoación de expediente disciplinario y medidas correctivas: Que, a la vista de la gravedad de los hechos (infracciones muy graves conforme a el art. 72 LOPDGDD), se proceda a la incoación formal de un expediente disciplinario contra D.ª Estrella (Letrada de la Administración de Justicia del JPI 1 de DIRECCION000) u otros responsables que se determinen, conforme a lo previsto en el art. 77 LOPDGDD y al régimen sancionador de la LOPJ (en particular, el art. 41.12 antes citado). Dicho expediente deberá dilucidar las responsabilidades individuales y podría conllevar las sanciones disciplinarias que procedan (por ejemplo, sanción de suspensión, traslado forzoso u otra prevista legalmente para faltas muy graves), con el objetivo de sancionar la conducta y disuadir futuras vulneraciones. Asimismo, se solicita que se adopten las medidas necesarias para corregir las deficiencias que hayan facilitado esta violación de datos garantizando el pleno cumplimiento de la normativa de protección de datos en el ámbito de la Administración de Justicia.

Tercero: Que se adopten medidas preventivas y correctivas necesarias para evitar la repetición de infracciones similares en el ámbito de los órganos judiciales. En concreto, se solicita que la Agencia Española de Protección de Datos, en coordinación con el órgano de gobierno de la Justicia, emita directrices o instrucciones dirigidas a los Juzgados y Tribunales recordando la obligación de respetar escrupulosamente los principios de protección de datos (especialmente, la

minimización y confidencialidad) en la tramitación de procedimientos. Estas medidas podrían incluir la formación específica del personal judicial en materia de protección de datos, la implementación de protocolos de anonimización o pseudonimización de datos sensibles en los expedientes judiciales, y la exigencia de que cualquier acceso o comunicación de datos patrimoniales o sensibles cuente con previa autorización judicial motivada, tal como ya se apuntó en resoluciones anteriores. De esta manera, se pretende garantizar la no repetición de hechos como los aquí denunciados y reforzar la seguridad de los datos personales en sede judicial, en beneficio de todos los ciudadanos.

Por lo expuesto, solicito de esa Subdirección General que tenga por presentado este escrito, con sus copias y anexos (incluyendo la documentación acreditativa del expediente NUM000 y del documento patrimonial divulgado), lo admita y, en su virtud, inicie el procedimiento de tutela correspondiente, adoptando las decisiones y medidas solicitadas en defensa del derecho fundamental del reclamante y de los terceros afectados».

Adjunta a dicha reclamación copia de la Consulta Integral de Patrimonio efectuada por el Juzgado de Primera Instancia núm. 1 de DIRECCION000 a nombre del reclamante.

SEGUNDO.- Mediante comunicación de la Directora de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial de 20 de octubre de 2025 se acusó recibo al reclamante, solicitándose al órgano judicial en esa misma fecha información sobre los hechos a que se refiere la reclamación.

TERCERO.- En fecha 3 de noviembre de 2025 tiene entrada en el Registro general del Consejo General del Poder Judicial el expediente remitido por la Agencia Española de Protección de Datos, en el que figura una reclamación de D. Luis Angel, con idénticas pretensiones a la presentada ante este Órgano Constitucional. Por acuerdo del Presidente de la Agencia Española de Protección de Datos, fechado el 20 de octubre de 2025 se traslada al denunciante que *"[d]el análisis de la documentación aportada no se desprende que, en el presente caso, el conocimiento de la cuestión planteada corresponda a la Agencia Española de Protección de Datos, sin perjuicio de la valoración que pueda realizar la mencionada Autoridad de control".* Tras citar el artículo 236 nonies, apartado 1, de la Ley Orgánica del Poder Judicial, se señala que *"de acuerdo con lo previsto en el Convenio suscrito, en fecha 6 de julio de 201, sobre colaboración en el ejercicio de las funciones propias de las Autoridades de control en materia de protección de datos, se procede a remitir su escrito a la Dirección de Supervisión y Control*

de Protección de Datos del Consejo General del Poder Judicial, a la que podrá dirigirse para todas las cuestiones relacionadas con el mismo".

CUARTO.- En fecha 10 de diciembre de 2025, tiene entrada en el Registro general del Consejo el informe del órgano judicial, en el que se señala lo siguiente:

«Dña. Estrella, Letrada del Juzgado de 1ª Instancia N. 1 de DIRECCION000, en relación a la información solicitada Expediente NUM001, en el que se da traslado de la reclamación planteada por D. Dámaso y referida al procedimiento Ejecución de Títulos Judiciales NUM000 que se tramita en este Juzgado, paso a informar de la misma.

Con carácter previo quisiera informar que esa letrada ya emitió un informe sobre estos mismos hechos con motivo de una queja presentada ante el cgpj, por el mismo reclamante en fecha 28 de julio de 2025 a través de la unidad de atención ciudadana con numero de referencia NUM002y que fue archivada por acuerdo de la secretaria coordinadora provincial en fecha 28 de Agosto de 2025.

Presenta la parte queja contra la Letrada que suscribe Juzgado de Primera Instancia n°. 1 de DIRECCION 000 por el traslado de información patrimonial que se realizó en este procedimiento de Ejecución de Títulos Judiciales N° NUM000, negociado 5, en fecha 28 de Junio del año 2023, al entender que constituye una intromisión en su esfera privada.

Examinadas actuaciones se observa que dicho procedimiento ha seguido el cauce procesal establecido sin que se hayan producido las irregularidades que denuncia la parte.

A continuación emito informe sobre los acontecimientos mas relevantes que pudieran tener relación con su queja.

La ejecución de: Títulos Judiciales NUM000 se despachó por auto de fecha 28/06/2023, siendo;

· Parte ejecutante: Dña. Constanza

· Parte ejecutada: D. Dámaso

La ejecución se despachó a instancia de Dña Constanza que presentó demanda ejecutiva en fecha 16 de Junio de 2023, manifestando en la misma que desconocía bienes y derechos de la parte ejecutada y solicitando al letrado, en base al art 590 de la _LEC que acuerde librar oficio a la oficina de averiguación patrimonial, Punto Neutro adscrita al juzgado a fin de localizar bienes y derechos de la misma

En fecha 28 de Junio de 2023, tras el análisis del título, S.Sa dictó auto autorizando el despacho de ejecución con arreglo al libro III de la LEC.

Tal y como establece el art 551.3 de la Lec "Dictado el auto, en el mismo día o al día siguiente el secretario dictara decreto conteniendo:

1. *las medidas ejecutivas concretas*

2. *Las medidas de localización y averiguación de los bienes del ejecutado que procedan, conforme a lo previsto en los art 589 y 590 de la Lec*

Dispone el art 590 que a instancia del ejecutante que no pudiere designar bienes del ejecutado suficientes para el fin de la ejecución el secretario judicial acordará dirigirse a las entidades financieras organismos y registros públicos para que faciliten dicha relación de bienes y derechos.

Por todo ello y en la misma fecha 28 de Junio de 2023, se dictó el Decreto de medidas ejecutivas acordando averiguación patrimonial y embargo de saldos bancarios, con el siguiente contenido:

"De conformidad con lo dispuesto en el art. 590 de la L.E.C., así como en el Convenio de Colaboración entre el C.G.P.J., el Ministerio de Justicia, la T.G.S.S. y el I.S. de la Marina, sobre Cesión de Datos a los Jueces y Tribunales y demás normas concordantes, como se interesa y se accede, se autoriza AVERIGUACIÓN PATRIMONIAL actualizada, mediante consulta telemática, respecto de los bienes y derechos de los que pudiera ser titular el/la ejecutado/a, de los que se tenga constancia en las Bases de Datos de la T.G.S.S, Agencia Tributaria, I.N.S.S y demás organismos respecto de los cuales se tiene Convenio por los Juzgados y Tribunales, practicándose la misma por medio del Punto Neutro Judicial, autorizándose a dichos efectos a funcionario habilitado"

Una vez obtenido el documento que contiene la información que a estos efectos proporcionan las plataformas correspondientes a tal fin y que únicamente se refieren a datos patrimoniales cuya titularidad corresponde al ejecutado, el mismo se unió al expediente por lo que únicamente las partes tuvieron acceso al mismo.

Alega la parte que se trata de una información confidencial, que no es solicitada por la ejecutante y que difunde datos irrelevantes, pero como puede observarse, la solicitud es efectuada por la ejecutante en su escrito de demanda, es autorizada por la autoridad judicial, y los datos reflejados son necesarios para conocer el patrimonio del ejecutado a fin de realizar los embargos necesarios para satisfacer la deuda reclamada.

Como puede observarse de la relación de acontecimientos expuesta las resoluciones respetan el cauce procesal establecido por ley. Quedo a su disposición para ampliar la información aportada si fuera necesario».

CUARTO.- Mediante comunicación de la Directora de Supervisión y Control de Protección de Datos de fecha 22 de diciembre de 2025, se solicitó ampliación de información relativa al informe emitido, en concreto la remisión del auto de ejecución de fecha 28 de junio de 2023 en el procedimiento de Ejecución de Títulos Judiciales núm. NUM000 que justifique el acceso a la averiguación patrimonial a través del PNJ. En fecha 13 de enero de 2026 ha tenido entrada en el Registro general del Consejo General del Poder Judicial copia del auto de fecha 28 de junio de 2023 dictado en el Procedimiento Ejecución Títulos Judiciales NUM000 dictado por el Juzgado de Primera Instancia núm. 1 de DIRECCION 000 (Familia) en el que se acuerda despachar ejecución frente a D. Dámaso y, copia del Decreto dictado por el referido órgano judicial en las actuaciones indicadas de fecha 28 de junio de

2023 en el que se autoriza la Averiguación patrimonial actualizada respecto del ejecutado D. Dámaso.

FUNDAMENTOS DE DERECHO

PRIMERO.- Objeto de la reclamación

Los hechos objeto del presente expediente se refieren a la posible vulneración de la normativa de protección de datos por parte del Juzgado de Primera Instancia núm. 1 de DIRECCION000, al acceder por dicho órgano judicial al Punto Neutro Judicial para su Consulta Integral Patrimonial y dar traslado de dicha documentación a la parte ejecutante del procedimiento Ejecución de Títulos Judiciales NUM000.

SEGUNDO.- Motivos alegados por el reclamante

El reclamante alega que se ha accedido a dicha consulta de manera irregular, sin su autorización ni resolución judicial y, que se ha dado traslado de la información patrimonial recabada a la otra parte del procedimiento sin proceder a la minimización de los datos sensibles e innecesarios para la ejecución, haciendo entrega íntegra da toda la información de manera desproporcionada.

TERCERO.- Normativa aplicable

El tratamiento de datos personales en el ámbito de los órganos judiciales se rige por un marco normativo multinivel, cuyo fundamento último se encuentra en la Constitución Española. En particular, el artículo 18.4 reconoce el derecho fundamental a la intimidad personal y familiar y a la protección de datos personales, exigiendo que cualquier injerencia en la vida privada sea legítima, necesaria y proporcionada.

Este marco constitucional se ve reforzado por el artículo 8 del Convenio Europeo de Derechos Humanos, que garantiza el derecho al respeto de la vida privada y familiar. La interpretación de este precepto por el Tribunal Europeo de Derechos Humanos impone a los poderes públicos, y por ende, a los órganos judiciales, no solo una obligación de abstención frente a injerencias indebidas, sino también obligaciones positivas de protección del derecho frente a posibles vulneraciones.

En el ámbito del Derecho de la Unión Europea, el Reglamento (UE) 2016/679, General de Protección de Datos (RGPD), establece los principios generales aplicables al tratamiento de datos personales, de aplicación directa también en el ámbito judicial, especialmente en lo relativo a los principios de licitud, minimización, exactitud, integridad, confidencialidad, seguridad y responsabilidad proactiva.

El RGPD, a través de su considerando 20, precisa dos cuestiones de especial relevancia para la Administración de Justicia. En primer lugar, confirma que el Reglamento resulta aplicable al tratamiento de datos personales realizado por los tribunales y otras autoridades judiciales. En segundo lugar, establece que el control del cumplimiento de la normativa de protección de datos en aquellos tratamientos efectuados con ocasión del ejercicio de la función jurisdiccional no debe corresponder a las autoridades de control "tradicionales" —como la Agencia Española de Protección de Datos—, sino a una autoridad de control independiente integrada en el propio poder judicial, con el fin de salvaguardar su independencia.

En coherencia con este planteamiento, el artículo 55.3 del RGPD, relativo a la competencia de las autoridades de control, establece que estas no serán competentes para controlar las operaciones de tratamiento efectuadas por los tribunales en el ejercicio de su función judicial, sin perjuicio de la existencia de una autoridad de control específica en el ámbito judicial, función que en España corresponde a esta Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial (DSYCPD).

No obstante, la aplicación del RGPD a los tratamientos realizados en el ámbito jurisdiccional debe matizarse en relación con el ámbito penal. El propio Reglamento excluye expresamente de su ámbito de aplicación el tratamiento de datos personales llevado a cabo por las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, así como de ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención, conforme a lo dispuesto en su artículo 2.2.d).

Estos tratamientos se regulan por la Directiva (UE) 2016/680, del Parlamento Europeo y del Consejo, transpuesta al ordenamiento jurídico español mediante 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 consecuencia, los tratamientos de datos personales realizados por juzgados y tribunales cuya finalidad se inscriba en el ámbito penal se rigen por esta Ley Orgánica 7/2021.

Sin perjuicio de lo anterior, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), resulta igualmente aplicable a los tratamientos de datos en el ámbito de la Administración de Justicia. Así lo establece expresamente su artículo 2.4, al disponer que el tratamiento de datos llevado a cabo con ocasión de la tramitación de los procesos judiciales, así como el realizado en el marco de la gestión de la Oficina Judicial, se regirá por lo dispuesto en el RGPD y en la propia Ley Orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, que resulten aplicables.

Finalmente, resulta imprescindible tener en cuenta las previsiones específicas contenidas en la Ley Orgánica del Poder Judicial, en particular los artículos 236 bis a 236 decies, incluidos en el Título III, "Actuaciones judiciales", Capítulo I bis, dedicado expresamente a la protección de datos de carácter personal en el ámbito de la Administración de Justicia, que introducen importantes precisiones en esta materia.

En particular, el artículo 236 bis de la Ley Orgánica 1/1986, de 1 de julio, del Poder Judicial (en adelante LOPJ), establece en su apartado 1 que "*[el] tratamiento de los datos personales podrá realizarse con fines jurisdiccionales o no jurisdiccionales. Tendrá fines jurisdiccionales el tratamiento de los datos que se encuentren incorporados a los procesos que tengan por finalidad el ejercicio de la actividad jurisdiccional".*

En consonancia con ese precepto, y siguiendo la LOPJ, su artículo 236 apartado 1 precisa que *"[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".*

Y el apartado 2 del mismo precepto dispone que *"[e]n 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, por la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal".

Estos artículos deben ponerse en relación con el artículo 236 octies de la LOPJ que atribuye a la Dirección de Supervisión y Control del Consejo General del Poder Judicial, respecto a las operaciones de tratamiento de datos con fines jurisdiccionales que realicen los Juzgados y Tribunales y las Oficinas Judiciales, diversas funciones, entre las que se encuentran la supervisión del cumplimiento de la normativa de protección de datos personales mediante el ejercicio de la labor inspectora (letra a) y la tramitación de las reclamaciones interpuestas por los interesados, informándose al reclamante sobre el curso y resultado de la reclamación en un plazo razonable, previa realización de la investigación oportuna si se considera necesario (letra e).

Estas funciones del artículo 236 octies de la LOPJ, se complementan, a su vez, con aquellas que sean aplicables de las recogidas tanto en el artículo 57 del Reglamento General de Protección de Datos, y en el artículo 48 de 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 este contexto, por tanto, la competencia de la Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial se ejerce respecto de los tratamientos de datos personales efectuados con fines jurisdiccionales, cuya caracterización se recoge en el apartado primero del artículo 236 bis de la Ley Orgánica del Poder Judicial, a cuyo tenor *"[t]endrá fines jurisdiccionales el tratamiento de los datos que se encuentren incorporados a los procesos que tengan por finalidad el ejercicio de la actividad jurisdiccional".*

En conclusión, los tratamientos de datos personales efectuados con fines jurisdiccionales se rigen por el Reglamento General de Protección de Datos (RGPD), la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines prevención, detección, investigación y

enjuiciamiento de infracciones penales y de ejecución de sanciones penales, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales, así como por la LOPJ y demás normas procesales que resulten de aplicación.

CUARTO.- Sobre la necesidad de respetar la normativa en materia de Protección de Datos Personales

La protección de los datos personales constituye un derecho fundamental reconocido en el artículo 18.4 de la Constitución Española y en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, conforme al cual:

"1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.
3. El respeto de estas normas estará sujeto al control de una autoridad independiente."

Este mandato se desarrolla mediante el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD), y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). Asimismo, la Ley Orgánica 7/2021, de 26 de mayo, relativa a la protección de datos personales tratados con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales, resulta de aplicación complementaria en este ámbito.

Los órganos judiciales en el ejercicio de su función jurisdiccional deben garantizar el cumplimiento íntegro de los principios y obligaciones establecidos por la normativa de protección de datos, garantizando en todo caso que los datos personales se traten conforme a los principios de licitud, lealtad, transparencia, minimización de datos, limitación de la finalidad, exactitud, integridad y confidencialidad, y todo ello, de acuerdo con el principio de responsabilidad proactiva (art. 5 RGPD).

En el ámbito judicial, la necesidad de conjugar la publicidad de las actuaciones (art. 120 CE y 232 LOPJ) con el derecho a la protección de los datos personales impone un deber reforzado de diligencia. Debe recordarse

que el tratamiento de datos por los órganos judiciales ha de limitarse a los estrictamente necesarios para la finalidad legítima del proceso, observando los principios mencionados.

Por ello, esta Dirección de Supervisión y Protección de Datos considera necesario recordar que los órganos judiciales, sus oficinas y el personal al servicio de la Administración de Justicia deben extremar el cuidado en el uso, acceso, tratamiento y difusión de datos personales obrantes en los expedientes, evitando la exposición innecesaria de información relativa a las partes, testigos u otros intervinientes, tanto en documentos de trabajo interno como en actuaciones públicas o resoluciones susceptibles de difusión.

En definitiva, la observancia de la normativa sobre protección de datos personales en el ámbito judicial no constituye una opción organizativa, sino un mandato jurídico derivado de la Constitución y de la normativa europea y nacional aplicable, cuya inobservancia puede comprometer el derecho fundamental reconocido en el artículo 18.4 CE y afectar a la confianza de la ciudadanía en la Administración de Justicia.

QUINTO.- Resolución de la reclamación

La reclamación objeto del presente expediente se fundamenta en la vulneración por el Juzgado de Primera Instancia núm. 1 de DIRECCION000 de la normativa en materia de protección de datos personales, y ello con base, en esencia, a dos motivos:

Por una parte, en la indebida incorporación al procedimiento de ejecución NUM000 tramitado ante el citado juzgado, de la información patrimonial recabada por el Letrado de la Administración de Justicia relativa al ejecutado (el reclamante), respecto de la cual, sostiene que contenía datos sensibles y no había resolución judicial habilitante ni petición de parte que justificase tal aportación y,

Por otra, en el traslado de dicha información a la parte contraria (parte ejecutante) sin solicitud de ésta, sin habilitación judicial específica y sin aplicar anonimización, disociación ni restricción alguna sobre los datos transmitidos.

En primer lugar, por lo que se refiere el primer motivo de reclamación, cabe señalar que, de la documentación obrante en el expediente y en particular, del informe emitido por el Juzgado de Primera Instancia núm. 1 de DIRECCION000 (actualmente Sección de Familia, Infancia y Capacidad del Tribunal de Instancia de DIRECCION000, Plaza núm. 3) y de las resoluciones aportadas por el mismo ha quedado acreditado que la averiguación patrimonial ha sido debidamente acordada en un procedimiento judicial.

La facultad del Letrado de la Administración de Justicia para llevar a cabo actuaciones de localización y averiguación de bienes del ejecutado encuentra su fundamento jurídico en diversos preceptos de la Ley de Enjuiciamiento Civil (LEC).

El artículo 589 LEC establece el deber del ejecutado de facilitar una relación detallada de sus bienes y derechos suficientes para satisfacer la deuda objeto de ejecución. El precepto faculta al órgano judicial, a través del LAJ, para requerir al ejecutado la presentación de dicha relación, así como para acordar la imposición de multas coercitivas en caso de falta de colaboración o resistencia injustificada.

Por su parte el artículo 590 LEC habilita al LAJ para proceder a la investigación judicial del patrimonio del ejecutado cuando éste no cumpla con el requerimiento previsto en el artículo anterior o cuando la información aportada resulte insuficiente. Esta averiguación puede incluir el libramiento de oficios y solicitudes de información a entidades financieras, registros públicos, administraciones tributarias, organismos de Seguridad Social y, en general, a cualquier entidad pública o privada que pueda disponer de datos relevantes sobre la titularidad o disponibilidad de viene y derechos del ejecutado.

Asimismo, el artículo 551.3.2º prevé que, dictado el auto de despacho de ejecución por el juez, el Letrado de la Administración de Justicia dictará decreto que contendrá, entre otras, las medidas necesarias para la localización y averiguación de los bienes del ejecutado, remitiéndose expresamente a lo dispuesto en los artículos 589 y 590 LEC. Esta previsión permite que el LAJ impulse de oficio actuaciones de averiguación de bienes sin necesidad de requerimientos adicionales cuando así se derive del título ejecutivo y de las circunstancias del caso.

En conjunto, estos preceptos configuran un marco normativo que atribuye al LAJ un papel esencial en la identificación de bienes embargables del ejecutado garantizando la efectividad de la ejecución. Es por ello que, el primer motivo de reclamación ha de ser rechazado por cuanto la actuación del Juzgado en la averiguación patrimonial se ha llevado a cabo con pleno sometimiento a derecho.

En segundo lugar, el motivo de reclamación se refiere al traslado íntegro de la información sobre averiguación patrimonial a la parte ejecutante. El análisis de este motivo exige hacer una serie de consideraciones.

Como hemos expuesto en la fundamentación precedente, el tratamiento de datos personales en el ámbito jurisdiccional, incluido el traslado de actuaciones o documentos a las partes, se encuentra plenamente sometido a los principios de limitación de la finalidad, minimización de datos, exactitud, integridad y confidencialidad, así como al principio de responsabilidad proactiva.

Estos principios son de aplicación directa y obligatoria para todas las actividades públicas, incluidos los órganos judiciales, sin perjuicio de las especialidades propias del proceso.

En este sentido, el Reglamento General de Protección Datos en lo que se refiere a los tratamientos de datos con fines jurisdiccionales, regula en su artículo 5 estos principios. Entre ellos, se encuentran los de "minimización de datos" e "integridad y confidencialidad" de los datos, los cuales son contemplados en los siguientes términos: *"1. Los datos personales serán: ... c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (´minimización de datos´) ... f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas y organizativas apropiadas (´integridad y confidencialidad´)".*

En el caso que nos ocupa, el traslado de la información patrimonial a las partes del procedimiento de ejecución constituye un tratamiento de datos personales en los términos del RGPD, al implicar comunicación o difusión relativa a personas físicas identificadas o identificables.

La finalidad del traslado de documentos es permitir el ejercicio de defensa y contradicción, lo que no ampara, en ningún caso, el conocimiento indiscriminado de datos personales no necesarios para resolver la cuestión controvertida (en este caso la ejecución). Por tanto, dicho traslado debe cumplir los principios que rigen el tratamiento lícito de datos, siendo especialmente relevante que, solo se trasladen datos adecuados, pertinentes y estrictamente necesarios para la finalidad procesal concreta, debiendo, en consecuencia, excluir aquellos datos accesorios o irrelevantes para la resolución del litigio.

En el caso de averiguaciones patrimoniales, la finalidad procesal se limita a acreditar la existencia, suficiencia o localización de bienes con el fin de posibilitar, en su caso, la ejecución o adopción de medidas procesales.

Sin embargo, dicha finalidad no justifica el traslado de números de cuentas bancarias (IBAN), datos identificativos de entidades financieras concretas si ello no es imprescindible, datos personales adicionales del titular de las cuentas o de terceros, entre otros. El conocimiento de estos datos por la parte contraria no aporta valor jurídico alguno a la efectividad de la ejecución y, por el contrario, supone un riesgo grave para la privacidad, la seguridad patrimonial y confidencialidad del reclamante.

El apartado 2 del artículo 5 del Reglamento General de Protección de Datos, preceptúa que *"[e]l responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)".* Con arreglo a lo dispuesto en el artículo 24.1 del mencionado Reglamento, y en virtud de las obligaciones que comporta el principio de responsabilidad proactiva del responsable del tratamiento, *"[t]eniendo 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".*

Por tanto, el principio de responsabilidad proactiva impone a la autoridad que trata los datos, en este caso el órgano judicial competente, el deber de anticiparse a los riesgos para los derechos de los interesados y adoptar las medidas técnicas y organizativas adecuadas. Ello implica, en relación con el traslado de datos, revisar previamente la información que se

va a comunicar, anonimizar, seudonimizar, disociar o suprimir los datos innecesarios, limitar el contenido del traslado a lo imprescindible para la finalidad (en este caso, la ejecución) y optar por las fórmulas menos invasivas.

En anteriores resoluciones adoptadas por esta Dirección de Supervisión y Protección de Datos del CGPJ se ha señalado reiteradamente que no le corresponde, en su condición de autoridad de control, pronunciarse sobre la adecuación de las actuaciones procesales a la normativa procesal por las que se rigen, salvo que por las circunstancias en que dichas actuaciones tengan lugar se desprenda algún indicio de posible vulneración de la normativa de protección de datos.

Siendo claro que en la actuación procesal de que se trata resultan de aplicación los correspondientes preceptos procesales, lo cierto es que sobre dicha actuación se proyecta también la normativa de protección de datos, incluida la necesaria observancia del principio de minimización de datos y confidencialidad, cuyo contenido se ha transcrito anteriormente.

En ejercicio de la responsabilidad asignada a esta Dirección de Supervisión y Control de Protección de Datos del CGPJ sobre el cumplimiento de la normativa de protección de datos y de la función de 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 (letras a y b del apartado 1 del artículo 236 octies LOPJ), debe subrayarse la necesidad de evitar tratamientos de datos que favorezcan el riesgo de que no se atiendan debidamente los principios por los que estos se rigen.

Es por ello que, el respeto de la normativa sobre protección de datos exige que por ese órgano judicial se adopten todas las medidas que sean necesarias, revisiones y comprobaciones del traslado que se realiza a las partes sobre la documentación aportada por las mismas o, que se encuentran dentro de los procedimientos, encaminadas a asegurar que los datos tratados sean en todo caso los adecuados, pertinentes y limitados a lo necesario en relación con los fines del tratamiento, que en todo caso debe incluir la garantía de la tutela judicial efectiva.

El propio artículo 236 LOPJ, en relación con el artículo 2.4 LOPDGDD, confirma que los tratamientos realizados en el marco de procedimientos

judiciales se someten al RGPD y a la legislación nacional en materia de protección de datos. La exigencia de cumplir con la normativa de protección de datos es, por tanto, de carácter imperativo en aras a garantizar una protección efectiva y no meramente formal de un derecho fundamental como es la protección de datos.

En el presente caso, por el Juzgado de primera instancia núm. 1 de Sevilla, se trasladó íntegramente la información patrimonial del reclamante a la parte ejecutante, sin respetar los principios de minimización, limitación a la finalidad, confidencialidad y responsabilidad proactiva consagrados en el artículo 5 del RGPD.

Habiendo quedado delimitados los hechos denunciados en la reclamación presentada y en el informe del Juzgado de Primera Instancia núm. 1 de DIRECCION000, no procede llevar a cabo ulteriores actuaciones de investigación en relación con los mismos. Por lo expuesto, la Directora de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial, por el presente

ACUERDA

1.- Declarar que, por el Juzgado de Primera Instancia núm. 1 de DIRECCION000, no se ha respetado la normativa de protección de datos.

2.- Que por el por el Juzgado de Primera Instancia núm. 1 de DIRECCION000 (actualmente Sección de Familia, Infancia y Capacidad del Tribunal de Instancia de DIRECCION000, Plaza núm. 3) se adopten las siguientes medidas:

- Que se compruebe que el traslado que se hace a las partes de los procedimientos contiene los datos personales adecuados, pertinentes y limitados a lo necesario en relación con los fines del tratamiento, teniendo en cuenta el principio de minimización de datos.
- Que se adopten las medidas de anonimización, seudonimización, disociación o supresión de datos necesarias para cumplir con los principios de minimización, limitación de la finalidad y confidencialidad.
- Que por el Juzgado de Primera Instancia núm. 1 de DIRECCION000 (actualmente Sección de Familia, Infancia y Capacidad del Tribunal de Instancia de DIRECCION000, Plaza núm. 3) en el plazo de quince días se dé traslado a esta Dirección de Supervisión y Control de Protección de datos de las referidas medidas adoptadas.

3.- Notificar la presente resolución a D. Dámaso y al Juzgado de Primera Instancia núm. 1 de DIRECCION000 (actualmente Sección de Familia, Infancia y Capacidad del Tribunal de Instancia de DIRECCION000, Plaza núm. 3)

Contra la presente resolución, que agota la vía administrativa, y de conformidad con lo dispuesto en el artículo 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, cabrá interponer recurso potestativo de reposición ante esta Dirección de Supervisión y Control de Protección de Datos, en el plazo de un mes a contar desde el día siguiente a la notificación de este acto, o directamente recurso contencioso-administrativo ante la Sala de lo Contencioso-Administrativo del Tribunal Supremo, de acuerdo con lo dispuesto en el artículo 25.1 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación del presente acto, conforme a lo dispuesto en el artículo 46.1 del referido texto legal.

Firmado digitalmente
Paloma Santiago y Antuña
Directora de Supervisión y Control de
Protección de Datos