RESOLUCIÓN

Exp.: 178/2026
Archivo
Fecha Inicio: 30/06/2026

ANTECEDENTES

PRIMERO.- Con fecha 30 de junio de 2026 se remite requerimiento de información a la Sección de Instrucción del Tribunal Central de Instancia Plaza núm. 2, sobre una posible vulneración de normativa de protección de datos en el siguiente sentido:

«Por la presente se comunica a ese órgano judicial que se ha tenido conocimiento por medios de comunicación de numerosas filtraciones de contenidos de la investigación (incluidos WhatsApp), que se está llevando a cabo por ese Tribunal en las Diligencias Previas 77/2024, y que pudieran afectar al derecho de protección de datos personales.

Por este motivo, y en ejercicio de las competencias asignadas a la Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial en el Capítulo I bis del Título III del Libro III de la Ley Orgánica del Poder Judicial, en materia de protección de datos de carácter personal en el ámbito de la Administración de Justicia, se ha procedido a iniciar actuaciones previas informativas relativas a los referidos hechos (número de expediente 178/2026), a cuyo fin se solicita de ese órgano judicial que informe sobre las medidas que se están adoptando para evitar las filtraciones de los datos personales contenidos en las diligencias de investigación».

SEGUNDO.- En fecha 6 de julio de 2026 tuvo entrada en el Registro general del Consejo el informe del órgano judicial, en el que se señala lo siguiente:

«Mediante oficio de fecha 30.06.2026 se pone en conocimiento de este órgano judicial, en relación con las Diligencias Previas número 77/2024, que esa Dirección de Supervisión y Control de Protección de Datos ha tenido conocimiento, a través de los medios de comunicación, de numerosas filtraciones de contenidos de la investigación (incluidos WhatsApp), que se está llevando a cabo por este Tribunal en las referidas actuaciones, y que pudieran afectar al derecho de protección de datos personales.

Por ese motivo, interesan información sobre "las medidas que se están adoptando para evitar las filtraciones de los datos personales contenidos en las diligencias de investigación"

A tales efectos, les participo los siguientes extremos:

1. En el órgano judicial a mi cargo nunca se facilitan resoluciones judiciales ni ningún otro tipo de documentos a los medios de comunicación.

2. Lamentablemente, en los procedimientos de alto impacto mediático, son frecuentes las filtraciones a los medios de comunicación, a través de alguna de las partes personadas, siendo extremadamente difícil determinar la responsabilidad de estos hechos.

3. Con fecha 22.06.2026 se presenta en este órgano judicial en la causa de referencia informe número 2910/26 UDEF-BBCA, acompañado de 19 anexos documentales.

4. Mediante resolución de fecha 24.06.2026 se acuerda tener "por recibido el anterior informe nº 2910/26, de fecha 22 de junio de 2026, procedente de la Unidad Central de Delincuencia Económica y Fiscal -Brigada Central de Investigación de Blanqueo de Capitales y Anticorrupción- de la Dirección General de la Policía, así como anexo documental, intégrense en el expediente judicial electrónico de su razón (Acont. 1754 y 1762) y no siendo técnicamente posible la transmisión telemática de los anexos indicados al Ministerio Fiscal y partes, en razón a su volumen, se procederá a su inclusión en la sede electrónica "Cloud Justicia".

5. Tras dicha puesta a disposición de las partes este órgano judicial tuvo conocimiento de que se había producido una filtración de su contenido a los medios de comunicación. De forma inmediata se dictó resolución de fecha 25.06.2025, acordando:

1) ***Deducir testimonio de los particulares oportunos en orden a la averiguación del origen de las filtraciones****, su eventual carácter delictivo y la identificación de las personas responsables, dada la gravedad de los hechos y su potencial encaje en tipos penales de revelación de actuaciones declaradas secretas; y su remisión a la Sección de Instrucción del Tribunal de Instancia de Madrid.*

2) *La adopción de las siguientes medidas adicionales de protección del secreto externo:*

a) ***La formación de una pieza de "información sensible"*** *que se integrará por las grabaciones audiovisuales de cuantas declaraciones personales se reciban, tanto a testigos como a investigados, en la presente causa.*

Esta pieza será accesible únicamente para este órgano jurisdiccional y el Ministerio Fiscal.

b) Una vez practicadas las referidas declaraciones, se facilitará a la acusación popular agrupada y a las defensas la trascripción de su contenido proporcionada automáticamente por el programa de grabación. No obstante, si alguno de los abogados de acusación o defensas precisara consultar algún extremo en concreto de las declaraciones referidas, para el que no le fuera bastante con la trascripción facilitada, podrá comparecer a consultar aquella en la sede de la Secretaría de este órgano judicial, sin que, sin embargo, se les facilite copia de la grabación hasta tanto, en su caso, se declare abierto el juicio oral.

c) La limitación del acceso al Cloud de las acusaciones populares personadas únicamente a través de la representación procesal y abogado bajo los que han sido agrupados.

6. Tras la notificación de esta resolución, se dictó otra complementaria de fecha 3 de julio, en la que se acordaba: (i) oficiar a la UDEF para que los anexos que incorporen a sus informes se limiten estrictamente a los hechos a los que estos hagan referencia, evitando la inclusión de información innecesaria o irrelevante para el objeto del procedimiento; y (ii) oficiar a la Subdirección General de Impulso e Innovación de los Servicios Digitales se emita informe técnico sobre la viabilidad de las medidas adicionales que, desde la perspectiva de seguridad digital, puedan incrementar la protección de los documentos insertados en el Cloud y evitar que su contenido pueda ser extendido a terceros sin autorización judicial».

FUNDAMENTOS DE DERECHO

PRIMERO.- Objeto del expediente

El presente expediente tiene por objeto comprobar la conformidad de las actuaciones llevadas a cabo por parte de la Sección de Instrucción del Tribunal Central de Instancia. Plaza núm. 2, en relación con la divulgación en prensa del contenido de actuaciones procesales, con la normativa sobre protección de datos.

SEGUNDO.- 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.

TERCERO.- 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.

CUARTO.- Resolución de la reclamación

En el presente expediente, iniciado a raíz de la publicación en determinados medios de comunicación de contenidos de la investigación que se está llevando a cabo por la Sección de Instrucción del Tribunal Central de Instancia. Plaza núm. 2, en las Diligencias Previas 77/2024, (incluidos WatsApp), se procedió a realizar por esta Dirección las investigaciones necesarias para comprobar la posible vulneración de la normativa de protección de datos por parte de ese órgano judicial.

La cesión del contenido de actuaciones judiciales a los medios de comunicación y el posterior acceso al mismo constituyen tratamientos de datos con arreglo a la definición que de estos se realiza en el artículo 4 del Reglamento general de protección de datos (entre otras, las operaciones de comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión).

En anteriores resoluciones adoptadas en ejercicio de las competencias asignadas como autoridad de protección de datos personales, el Consejo General del Poder Judicial se ha hecho eco de la doctrina del Tribunal

Constitucional relativa a los límites de los derechos fundamentales. En el fundamento jurídico 11 de la STC 292/2000, reiterado después en el fundamento jurídico 4 de la STC 17/2013, de 31 de enero, se indica que: *"[E]l derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los poderes públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución"*.

En esta misma línea, el propio Reglamento general de protección de datos reconoce en su considerando (4) que *"… [e]l derecho a la protección de datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales con arreglo al principio de proporcionalidad. El presente Reglamento respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto a la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo y la diversidad cultural, religiosa y lingüística".*

En definitiva, el derecho de protección de datos personales debe coexistir, entre otros, con los de tutela judicial efectiva y a comunicar o recibir libremente información veraz por cualquier medio de difusión. La plasmación del principio de proporcionalidad al que se refiere el considerando transcrito se realiza mediante la ponderación de los distintos derechos fundamentales y restantes bienes jurídicos constitucionalmente protegidos en juego. Poca duda puede caber de que, en los procedimientos judiciales, la realización del juicio de ponderación, en orden a determinar la prevalencia de cualquiera de los que pudieran entrar en posible conflicto, corresponde a quienes, en el órgano judicial, y en ejercicio de las competencias que a tal fin tienen atribuidas, desarrollan la actividad jurisdiccional que tienen atribuida en el régimen de plena independencia constitucionalmente reconocido (artículo 117 CE). Para llegar a dicha conclusión basta con recordar lo dispuesto en el artículo 7.1 de la Ley Orgánica del Poder Judicial: *"Los derechos y libertades reconocidos en el Capítulo Segundo del Título I de la Constitución vinculan,*

en su integridad, a todos los Jueces y Tribunales y están garantizados bajo la tutela efectiva de los mismos".

En el plano del derecho de tutela judicial efectiva, las partes personadas tienen acceso a todas las actuaciones del expediente judicial.

Situados en este punto, resulta obligado recordar que, con arreglo a lo prevenido en el artículo 236 quinquies, apartado 3, la normativa de protección de datos, respecto de los tratamientos de los datos que obran en los procedimientos judiciales, no solo vincula a los órganos judiciales, sino que igualmente compromete a todos aquellos que hayan tenido acceso a tales datos en el desarrollo del procedimiento: " *[l]os datos personales que las partes conocen a través del proceso deben ser tratados por éstas de conformidad con la normativa general de protección de datos. Esta obligación también incumbe a los profesionales que representan y asisten a las partes, así como a cualquier otro que intervenga en el procedimiento".*

En el presente caso, del contenido del informe emitido por el órgano judicial, resulta acreditado que las filtraciones de la información contenida en las actuaciones de investigación a los medios de comunicación no proceden del órgano judicial. Así se afirma categóricamente en el referido informe al señalar que "*1. En el órgano judicial a mi cargo nunca se facilitan resoluciones judiciales ni ningún otro tipo de documentos a los medios de comunicación".*

Por otra parte, con el referido informe se constata que, el órgano judicial, tras tener conocimiento de que se había producido una filtración del contenido del informe procedente de la Unidad Central de Delincuencia Económica y Fiscal -Brigada Central de Investigación de Blanqueo de Capitales y Anticorrupción- de la Dirección General de la Policía y sus anexos, de manera inmediata, adoptó cuantas medidas se estiman por esta Dirección necesarias y suficientes, teniendo en cuenta los medios disponibles, para evitar nuevas filtraciones, entre ellas: deducir testimonio de los particulares oportunos en orden a la averiguación del origen de las filtraciones, la formación de una pieza de "información sensible" a integrar por las grabaciones audiovisuales de cuantas declaraciones personales se reciban que será accesible únicamente para ese órgano jurisdiccional y el Ministerio Fiscal, adoptándose medidas restrictivas respecto de las acusaciones y defensas para garantizar su confidencialidad.

A mayor abundamiento, el órgano judicial, adoptó medidas adicionales consistentes en oficiar a la UDEF para que los anexos que incorporen a sus informes se limiten estrictamente a los hechos a los que estos hagan referencia y asimismo, oficiar a la Subdirección General de Impulso e Innovación de los Servicios Digitales para que emita informe técnico sobre la viabilidad de las medidas adicionales que, desde la perspectiva de seguridad digital, puedan incrementar la protección de los documentos insertados en el Cloud y evitar que su contenido pueda ser extendido a terceros sin autorización judicial.

Sin perjuicio de lo anterior, es preciso señalar que, la difusión de actuaciones procesales por cualquiera que haya tenido acceso a las mismas no constituye un tratamiento de datos con fines jurisdiccionales en sentido propio. En efecto, que los datos en cuestión obren en un procedimiento judicial y que se haya accedido al mismo no supone que cualquier tratamiento que se haga de éstos revista carácter jurisdiccional. Para ello es preciso, según se desprende del artículo 236 ter de la Ley Orgánica del Poder Judicial, no sólo que los datos estén incorporados a los procesos de que conozcan los tribunales, sino que la finalidad del tratamiento sea el ejercicio de la actividad jurisdiccional, condición esta última que claramente falta en el presente caso, ya que el tratamiento cuestionado se realiza en un contexto de relación entre las partes del procedimiento con los medios de comunicación en el que, cualquiera que fuera la finalidad perseguida, ésta se encuentra desconectada del ejercicio de la función jurisdiccional.

Tales tratamientos, por tanto, se encuentran al margen del ámbito competencial de la Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial como autoridad de control, que se ciñe a los tratamientos de datos con fines jurisdiccionales.

En conclusión, del informe emitido por el órgano judicial, ha quedado debidamente acreditado que, en las Diligencias Previas 77/2024, el órgano judicial cumplió adecuadamente las obligaciones derivadas de la normativa de protección de datos y ha adoptado aquellas que se consideran pertinentes para evitar futuras filtraciones de datos.

A la vista del informe emitido por la Sección de Instrucción del Tribunal Central de Instancia. Plaza núm. 2, y toda vez que el presente se ha iniciado de oficio por esta Dirección de Supervisión y Control de Protección de Datos.

ACUERDA

1.- Archivar el expediente registrado con el número 178/2026, por una posible vulneración de la normativa de protección de Datos por la Sección de Instrucción del Tribunal Central de Instancia. Plaza núm. 2.

2.- Notificar la presente resolución a la Sección de Instrucción del Tribunal Central de Instancia. Plaza núm. 2.

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