



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

RESOLUCIÓN

Exp.: 142/2026

Inadmisión

Fecha entrada: 28/05/2026

ANTECEDENTES

PRIMERO.- Con fecha 2 de abril de 2026 tiene entrada en el Registro general de la Agencia Española de Protección de Datos una reclamación de D. Casiano referente al Juzgado Togado Militar Central Nº 1, cuyo contenido es el siguiente:

« El presente escrito tiene por objeto poner en conocimiento de la Agencia Española de Protección de Datos la posible existencia de una brecha de seguridad supuestamente cometida el 4 de julio de 2022 consistente en accesos, comunicaciones o difusión indebida de datos personales especialmente protegidos en el marco de las Diligencias Previas nº 1/04/22 del Juzgado Togado Militar Central nº 1.

Desde el inicio del procedimiento se incorporaron datos de máxima sensibilidad, incluyendo datos de salud del reclamante y de la madre de sus tres hijos, así como información relativa a dichos menores de edad, afectando al menos a cuatro personas, de las cuales dos son menores. Ello determina la aplicación del régimen reforzado de protección previsto en el artículo 9 del Reglamento (UE) 2016/679.

De la documentación analizada se desprenden indicios racionales de que dichos datos pudieron haber sido accedidos por personas sin posición procesal claramente definida, comunicados a terceros sin base jurídica suficientemente acreditada, remitidos mediante canales electrónicos carentes de garantías adecuadas y puestos a disposición sin control efectivo de acceso ni trazabilidad.

Especial relevancia presenta la remisión de documentación desde el propio órgano judicial a direcciones de correo electrónico de terceros, incluyendo archivos adjuntos susceptibles de contener la totalidad de la documentación del procedimiento, entre ellos datos de salud y datos relativos a menores, sin que consten medidas de protección adecuadas como cifrado o control de accesos.

Asimismo, se identifican posibles irregularidades en la fase inicial del procedimiento, en la que una persona ajena a la condición procesal correspondiente habría tenido acceso e intervención en la tramitación de notificaciones, lo que comprometería el principio de confidencialidad desde el origen del tratamiento.

Del conjunto de hechos descritos se infiere la posible existencia de una vulneración de los principios de integridad y confidencialidad (art. 5.1.f RGPD), tratamiento de datos sin base jurídica adecuada (art. 6 RGPD), tratamiento indebido de categorías especiales de datos (art. 9 RGPD) y falta de adopción de medidas de seguridad apropiadas (art. 32 RGPD), constituyendo todo ello indicios de una brecha



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

de seguridad no documentada ni notificada a la autoridad de control ni a las personas afectadas.

Se desconoce el alcance exacto de la difusión, así como el número de accesos realizados, lo que incrementa el riesgo para los derechos y libertades de las personas afectadas, especialmente por tratarse de datos de salud y de menores de edad.

En consecuencia, se solicita la intervención de la Agencia Española de Protección de Datos a fin de investigar los hechos descritos, determinar las posibles responsabilidades y, en su caso, adoptar las medidas correctoras o sancionadoras que procedan».

Adjunta a la reclamación diversa documentación entre la que se encuentra la reclamación efectuada ante este órgano constitucional en fecha 20 de diciembre de 2022 tramitado con el núm. de expediente NUM000, junto con comunicaciones de dicho expediente remitidas por esta Dirección de Supervisión y Control y escrito dirigido a la Agencia Española de Protección de Datos en fecha 2 de abril de 2026, que contiene los siguientes particulares:

« PRIMERO. – Incorporación al procedimiento de datos especialmente protegidos (Art. 9 RGPD)

En fecha 7 de marzo de 2022, el compareciente formuló denuncia ante el Cuerpo Nacional de Policía, dando lugar al Atestado nº NUM001 y, posteriormente, a las Diligencias Previas nº 1/04/22 del Juzgado Togado Militar Central Nº 1. En dicha denuncia consta expresamente identificada Dª María Dolores como persona afectada, así como la afectación del entorno familiar. Igualmente, se hizo constar la aportación de varios tomos documentales, incluyendo un Tomo IV:

Informes médicos de los denunciantes, además de referencias expresas a la incidencia del problema sobre los hijos menores.

Por tanto, desde el inicio del procedimiento quedaron incorporados datos de salud del compareciente y de la madre de sus tres hijos, así como datos concernientes al entorno familiar y a los menores de edad, todo ello perteneciente al ámbito de máxima sensibilidad y protección reforzada.

SEGUNDO. – Filtración inicial del Auto 32/22 y quiebra del deber de confidencialidad desde el inicio del procedimiento

Con carácter previo a los hechos descritos en el apartado siguiente, y tal y como se acredita mediante la documentación aportada como ANEXO correspondiente (queja registrada ante el Delegado de Protección de Datos de la Guardia Civil en fecha 23 de mayo de 2023, registro REGAGE23e00032889775), ya se habría producido una primera comunicación irregular de datos personales en el propio acto inicial de notificación del procedimiento.

En concreto, el Auto nº 32/22, de fecha 18 de abril de 2022, por el que se acuerda la incoación de las Diligencias Previas nº 1/04/22, fue remitido desde el Juzgado Togado Militar Central nº 1 al Servicio de Régimen Disciplinario de la Guardia Civil, siendo posteriormente conocido y gestionado por uno de los oficiales



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

denunciados, el coronel D. Modesto, con carácter previo a su efectiva notificación al denunciante.

Tal y como se desprende de la documentación aportada, dicho oficial no solo tuvo acceso al contenido del Auto, sino que intervino directamente en la tramitación de la notificación dirigida al propio denunciante, llegando incluso a remitir al órgano judicial la cédula de notificación firmada, sin que conste la adopción de medidas que garantizaran la confidencialidad de la información ni la existencia de una base jurídica que legitimara dicho acceso.

Debe destacarse que, en el momento de los hechos, respecto del referido oficial denunciado no constaba formalmente su personación procesal ni la existencia de una habilitación expresa que legitimara el acceso a dicha documentación en el procedimiento, ni tampoco que contara con representación letrada en ese momento.

Asimismo, consta que los documentos fueron remitidos mediante canales electrónicos sin cifrado ni protección, permitiendo el acceso a archivos susceptibles de contener información especialmente sensible, lo que resulta incompatible con las exigencias de seguridad establecidas en el artículo 5.1.f del Reglamento (UE) 2016/679.

Este hecho resulta especialmente relevante, en la medida en que evidencia una quiebra del deber de confidencialidad desde el mismo inicio del tratamiento de datos personales en el procedimiento, configurando un antecedente directo de las posteriores comunicaciones descritas en los apartados siguientes y permitiendo apreciar la existencia de un patrón de actuación carente de las garantías exigidas por la normativa de protección de datos.

TERCERO. – Indicios de acceso o conocimiento del procedimiento por terceros sin posición procesal claramente definida

Del expediente NUM002 seguido ante la Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial resulta que el Tribunal Militar Central afirmó que el Auto nº 186/2022, de fecha 10 de octubre, fue notificado, además de a la procuradora, a los tres oficiales denunciados mediante sus correos profesionales, añadiendo que dichos oficiales "ya habían tenido conocimiento puntual del procedimiento" y que "como investigados" tenían derecho a conocer la totalidad del proceso conforme al artículo 118 de la Ley de Enjuiciamiento Criminal, extremo cuya cobertura jurídica efectiva en ese concreto momento procesal se cuestiona expresamente en la presente reclamación.

Sin embargo, los hechos que se someten a la consideración de esa Agencia no se limitan a dicha actuación, sino que encuentran un antecedente directo, previo y documentado en actuaciones del propio procedimiento.

Tal y como se acredita de forma directa en el ANEXO 3 que se acompaña, consistente en documentación relativa al Auto nº 48/22, de fecha 1 de julio de 2022, la Secretaria Relator del Juzgado Togado Militar Central nº 1 procedió a remitir por correo electrónico documentación del procedimiento desde el propio órgano judicial a varios destinatarios identificados como los tres oficiales denunciados.

En dicho ANEXO 3 se documenta de forma directa el origen del envío, el canal utilizado, los destinatarios y la existencia de archivos adjuntos, constando que la



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

remisión se realiza desde el propio órgano judicial a direcciones de correo electrónico individualizadas correspondientes a los tres oficiales denunciados. Asimismo, se identifica la inclusión de varios documentos adjuntos, entre los que figuran resoluciones del procedimiento y un archivo denominado "DENUNCIA", susceptible de contener el conjunto de los tomos documentales aportados en la causa, incluyendo datos de salud y datos relativos a menores de edad.

Este extremo resulta especialmente relevante desde la perspectiva de protección de datos, en la medida en que permite inferir la efectiva comunicación o, al menos, la puesta a disposición de información especialmente protegida a destinatarios sin posición procesal claramente definida ni cobertura jurídica suficientemente acreditada.

Debe señalarse que dichos destinatarios no constaban formalmente personados en el procedimiento ni contaban con representación letrada en el momento de los hechos, lo que determina, al menos indiciariamente, la ausencia de una base jurídica clara para el acceso a dicha información.

Asimismo, resulta especialmente relevante, desde la perspectiva de protección de datos, que a lo largo de toda la fase de instrucción de las Diligencias Previas nº 1/04/22 no consta comunicación formal alguna con los denunciados ni intervención procesal por su parte, lo que convierte en un hecho no explicado ni justificado que la Secretaria Relator dispusiera de los correos electrónicos individuales de cada uno de ellos.

Dicha circunstancia plantea serias dudas sobre el origen y la forma de obtención de dichos datos de contacto, pudiendo resultar contraria a los principios de licitud, minimización y limitación del acceso establecidos en el Reglamento (UE) 2016/679.

CUARTO. – Indicios de comunicación irregular y de utilización de canales no garantistas

En el citado recurso de reposición del expediente NUM002 seguido ante la Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial se denunció que el medio empleado para notificar el Auto 32/22 no respetó los principios de integridad y confidencialidad, al haberse canalizado la notificación con intervención del coronel Mora y del Negociado de Régimen Disciplinario de la Guardia Civil, utilizándose un cauce que, según se expone en dicho escrito, dejaba los archivos sin encriptar y permitía una circulación impropia de información sensible. También se expuso que esos hechos se habrían repetido con posterioridad mediante nuevas notificaciones tramitadas y devueltas por conducto del Negociado de Expedientes perteneciente a la Zona de la Guardia Civil de DIRECCION000.

QUINTO. – Posible remisión de documentación adicional no reflejada formalmente

En el mismo recurso de reposición del expediente NUM002 seguido ante la Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial se hizo constar que, además del Auto 48/22, la Secretaria Relator habría adjuntado más documentos sin que el acuerdo de la resolución lo reflejase



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

expresamente, indicándose que el archivo "Denuncia.pdf" podía contener los tomos I, II, III y IV, incluyendo datos médicos del compareciente y de la madre de sus tres hijos, así como de los menores de edad. El propio escrito formula este extremo como una cuestión que debe ser esclarecida e investigada.

Resulta especialmente relevante la denominación de los archivos adjuntos remitidos en fecha 4 de julio de 2022 a los correos electrónicos de los denunciados.

Mientras que en la comunicación dirigida a la representación letrada del denunciante se emplea una nomenclatura neutra y coherente con su condición procesal (por ejemplo, "C.E. LDO. ..." junto con el Auto correspondiente), en los correos remitidos a los denunciados se observa una denominación individualizada de los archivos, incorporando expresamente sus nombres y empleando fórmulas propias de actos procesales de comunicación (por ejemplo, "C.E." o "CED. NOT." seguidas del nombre del destinatario).

Tal y como se refleja gráficamente a continuación:

Dicha denominación de los datos adjuntos no resulta irrelevante, pues:

– Introduce una apariencia formal de acto de comunicación procesal dirigido a un destinatario concreto.

– Sugiere una posible legitimación de acceso vinculada a una condición procesal no claramente acreditada en ese momento.

– Podría haber servido como soporte documental para justificar, en el ámbito interno o externo del procedimiento, el acceso y tratamiento de la información contenida en los archivos adjuntos, generando una apariencia de licitud en relación con dichos accesos.

Todo ello adquiere especial relevancia si se tiene en cuenta que los destinatarios de dichos correos no constaban formalmente personados ni asistidos de letrado, y que los envíos incluían documentación adicional no mencionada expresamente en la resolución notificada.

En consecuencia, se interesa que por esa Agencia se valore si la forma de construcción, denominación y remisión de dichos archivos pudo constituir un mecanismo que facilitara o encubriera accesos no plenamente justificados a datos personales, incluidos datos especialmente protegidos.

Los hechos descritos en el presente apartado resultan directamente relevantes a efectos de valorar la posible existencia de una brecha de seguridad en los términos desarrollados en el apartado OCTAVO del presente escrito.

SEXTO. – Falta de garantías suficientes respecto de las personas afectadas

Mientras existen indicios de acceso, conocimiento o comunicación del procedimiento a personas con una posición procesal controvertida, D^a María de los Ángeles Mata Vidal, identificada desde la denuncia inicial y cuyos datos personales y de salud forman parte del material incorporado a la causa, no fue citada, informada de sus derechos, llamada a ratificarse ni invitada a personarse, según constará en el incidente de nulidad que será promovido ante la jurisdicción militar.

SÉPTIMO. – Alcance de la presente reclamación y competencia de esa Agencia

La presente reclamación no se limita a cuestionar el tratamiento de datos dentro del estricto ejercicio de la función jurisdiccional, sino que se refiere



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

específicamente a posibles accesos, comunicaciones o difusión de datos personales especialmente protegidos fuera de los límites estrictamente necesarios, con utilización de canales no suficientemente garantistas y sin trazabilidad clara sobre quién accedió, qué documentos se remitieron y con qué cobertura jurídica.

Por ello, se interesa la intervención de esa Agencia a fin de determinar si se ha producido una vulneración de los principios de integridad, confidencialidad, minimización y limitación del acceso, especialmente relevante al afectar a datos de salud y a menores de edad.

OCTAVO.– Posible existencia de brecha de seguridad no gestionada conforme a los criterios del CGPJ

El "Procedimiento para la notificación y gestión de brechas de seguridad que puedan sufrir los datos personales tratados con fines jurisdiccionales", publicado por el Consejo General del Poder Judicial en marzo de 2026, define como brecha de seguridad, de conformidad con el artículo 4.12 del Reglamento (UE) 2016/679, cualquier incidente que ocasione la comunicación o acceso no autorizados a datos personales, incluyendo, entre otros supuestos:

- El acceso no autorizado a datos personales.*
- La comunicación indebida de datos.*
- El envío de información a destinatarios no legitimados.*
- El uso inadecuado de canales electrónicos.*

Asimismo, establece la obligación de documentar internamente la brecha, evaluar el riesgo para los derechos de los afectados, notificarla a la autoridad de control y comunicarla a los interesados cuando exista riesgo elevado.

Si bien dicho procedimiento es posterior a los hechos aquí descritos, y por tanto no resulta directamente aplicable de forma retroactiva, los criterios en él recogidos permiten identificar y calificar conductas que, en esencia, ya se encontraban prohibidas y reguladas en el momento de los hechos por el propio Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018.

En el presente caso y en particular en relación con los hechos descritos en el apartado QUINTO, concurren indicios racionales de que personas sin posición procesal claramente definida pudieron acceder a documentación del procedimiento; que se utilizaron canales de comunicación no suficientemente garantistas; y que pudieron haberse remitido documentos con datos especialmente protegidos.

Debe destacarse, además, que parte de las actuaciones se encontraban pendientes de resolución en el momento en que se produjeron determinadas comunicaciones, lo que implica que el procedimiento no había adquirido firmeza ni delimitación definitiva de las partes intervinientes, incrementando el riesgo de accesos indebidos o prematuros a información sensible.

Especialmente relevante resulta el hecho de que dichos accesos y comunicaciones habrían afectado a datos de salud (art. 9 RGPD) y a información relativa a tres menores de edad, lo que determina la existencia de un alto riesgo para los derechos y libertades de los afectados.

Sin que conste:

- Documentación de la incidencia.*



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

- Notificación de la brecha.
- Comunicación a los afectados.

Por todo ello, se interesa que por esa Agencia se investigue si los hechos descritos constituyen una vulneración de las obligaciones ya vigentes en el momento de los hechos en materia de protección de datos personales, con independencia de la posterior formalización de procedimientos internos por parte del Consejo General del Poder Judicial.

NOVENO. – Insuficiencia de la actuación del órgano de control del Consejo General del Poder Judicial y necesidad de investigación material de los hechos

Con carácter previo a la presente reclamación, el compareciente acudió inicialmente al Delegado de Protección de Datos del Consejo General del Poder Judicial, dando lugar posteriormente a actuaciones tramitadas por la Dirección de Supervisión y Control de Protección de Datos del propio CGPJ en los expedientes 069/2022 y 045/2023, en los que se pusieron en conocimiento de dicho órgano los hechos sustancialmente coincidentes con los que ahora se someten a la consideración de esta Agencia.

Las resoluciones dictadas en dichos expedientes procedieron al archivo o inadmisión de las actuaciones, fundamentando dicha decisión, esencialmente, en la consideración de que las actuaciones descritas se enmarcarían en el ámbito de la legalidad procesal, así como en la remisión de determinadas comunicaciones por conducto jerárquico.

Sin embargo, dichas resoluciones no efectuaron un análisis material de los elementos nucleares desde la perspectiva de protección de datos personales, omitiendo pronunciamiento específico sobre extremos relevantes tales como:

- *El acceso previo a resoluciones judiciales por parte de personas sin posición procesal claramente definida.*
- *La eventual intervención de uno de los oficiales denunciados en la tramitación material de actos de notificación dirigidos al propio denunciante.*
- *La remisión de documentación a direcciones de correo electrónico individualizadas con inclusión de archivos adjuntos susceptibles de contener datos especialmente protegidos.*
- *La ausencia de medidas técnicas y organizativas que garantizaran la confidencialidad, integridad y control de acceso a la información.*

Debe destacarse, en particular, que de la documentación obrante se desprende que uno de los oficiales denunciados habría tenido acceso previo al contenido del procedimiento y habría intervenido en la práctica de la notificación, llegando a remitir al órgano judicial la cédula firmada. Dicha circunstancia, de confirmarse, supondría una quiebra sustancial del principio de confidencialidad del tratamiento, al permitir que una persona potencialmente afectada por el procedimiento acceda, gestione y participe en actos de comunicación de datos personales especialmente protegidos sin habilitación procesal acreditada.

Asimismo, resulta relevante que las resoluciones del Consejo General del Poder Judicial no aborden las contradicciones existentes entre las manifestaciones del órgano judicial respecto a la condición procesal de los denunciados, ni la efectiva



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

cobertura jurídica del acceso a la totalidad de la documentación del procedimiento en el momento en que se produjeron los hechos.

Debe ponerse de manifiesto que, con independencia del contexto más amplio en el que fueron inicialmente expuestos, los hechos que sustentan aquellas reclamaciones permanecen inalterados y deben ser analizados desde la perspectiva específica de la normativa de protección de datos personales.

En este sentido, resulta especialmente significativo que el propio Consejo General del Poder Judicial haya publicado en marzo de 2026 el "Procedimiento para la notificación y gestión de brechas de seguridad que puedan sufrir los datos personales tratados con fines jurisdiccionales", en el que se identifican como supuestos de brecha de seguridad, entre otros, el acceso no autorizado, la comunicación indebida de datos o el uso inadecuado de canales electrónicos, supuestos que coinciden sustancialmente con los hechos denunciados en 2023.

Por todo ello, se considera que las actuaciones desarrolladas por el órgano de control del Consejo General del Poder Judicial no han agotado el análisis de los hechos desde la perspectiva propia de la protección de datos personales, resultando necesaria una investigación material y completa por parte de esa Agencia, a fin de determinar la existencia de accesos, comunicaciones o difusión indebida de datos especialmente protegidos y, en su caso, las responsabilidades que pudieran derivarse

FUNDAMENTOS DE DERECHO

I. Artículos 5, 6 y 9 del Reglamento (UE) 2016/679, en cuanto a los principios de licitud, minimización, integridad, confidencialidad y al tratamiento de categorías especiales de datos.

II. Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales.

III. Artículo 236 de la Ley Orgánica del Poder Judicial, en cuanto al tratamiento de datos personales en el ámbito judicial.

IV. Demás preceptos de general y pertinente aplicación.

SOLICITA

Que teniendo por presentado este escrito, con la documentación que se acompaña, se sirva admitirlo y, en su virtud:

PRIMERO. Se admita la presente reclamación en materia de protección de datos.

SEGUNDO. Se investigue si en relación con las Diligencias Previas nº 1/04/22 del Juzgado Togado Militar Central se produjeron accesos, comunicaciones o difusión de datos personales, especialmente de datos de salud y datos relativos a menores, fuera de los límites estrictamente necesarios y sin garantías suficientes.

TERCERO. Se requiera, en su caso, la información necesaria para esclarecer:

- a) Qué personas accedieron a la documentación*
- b) Qué documentos fueron efectivamente remitidos en cada acto de comunicación*
- c) Qué canales se utilizaron*
- d) Si existía registro de trazabilidad y control de acceso*



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

e) Si se adoptaron medidas suficientes para garantizar la integridad y confidencialidad de los datos.

CUARTO. Se determine si se han vulnerado los principios y obligaciones establecidos en la normativa de protección de datos.

QUINTO. En su caso, se adopten las medidas correctoras, de investigación o sancionadoras que procedan.

OTROSÍ DIGO

Que esta parte interesa expresamente que se valore la especial gravedad de los hechos descritos por afectar a datos médicos y a menores de edad, así como por la posible concurrencia de una brecha de seguridad no gestionada conforme a los criterios establecidos por el Consejo General del Poder Judicial».

Adjunta a la reclamación particulares del procedimiento seguido en el Juzgado Togado Militar Central núm. 01, Exp. 00/0002 y resoluciones dictadas por esta Dirección de Supervisión y Control en los Expedientes 069/2022 y 045/2023.

SEGUNDO.- Por acuerdo del Presidente de la Agencia Española de Protección de Datos, fechado el 27 de mayo de 2026 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 2017, 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". El expediente remitido por la Agencia Española de Protección de Datos tiene entrada en el Registro general de este órgano constitucional el día 28 de mayo de 2026.

FUNDAMENTOS DE DERECHO

PRIMERO.- Objeto de la reclamación

Los hechos objeto del presente expediente se refieren a una posible vulneración de la normativa de protección de datos por parte del Juzgado Togado Militar Territorial Central núm. 1, al remitir comunicaciones por medio de correo electrónico sin las debidas medidas de control.



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

SEGUNDO.- Motivos alegados por el reclamante

El reclamante alega que las comunicaciones remitidas por el Juzgado Togado Militar Territorial Central núm. 1 no se realizaron por medio de canales electrónicos con cifrado y protección, por lo que no se utilizaron canales garantistas lo que habría producido una brecha de seguridad al poder acceder a los mismos personas ajenas al proceso.

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



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

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.



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

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



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

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."



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

- 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, siendo responsables de garantizar que los datos personales se traten de manera lícita, leal y transparente, de acuerdo con el principio de responsabilidad proactiva del artículo 5.2 del 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 de minimización, limitación de la finalidad y confidencialidad (artículos 5.1.c) y f) RGPD.

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 y difusión de datos personales obrantes en los expedientes, evitando la exposición innecesaria de información identificativa de 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



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

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

En el caso que nos ocupa, se trata de una nueva reclamación sobre unos extremos que el Sr. Casiano no manifestó en sus anteriores escritos que fueron tramitados en esta Dirección de Supervisión y Control de Protección de Datos con los números de expediente 069/2022 y 045/2023, todos ellos referentes a las D. PV. 1/04/22 seguido ante el Juzgado Togado Militar Central núm. 1, por lo que versan sobre el mismo fondo de la cuestión en su día reclamada.

En el presente expediente alega el Sr. Casiano, que las notificaciones remitidas por correo electrónico no se realizaron por medio de canales electrónicos con cifrado y protección, por lo que no se utilizaron canales garantistas. Pues bien, examinado el informe emitido por el Secretario Relator del Juzgado Togado Militar Central núm. 1, de fecha 16 de enero de 2023 unido al Exp. 069/2022 de esta Dirección consta que: "ha de ponerse aquí de manifiesto que la Jurisdicción Militar no tiene, hasta la fecha, acceso al sistema de notificaciones LEXNET. Motivo por el que, al objeto de poder mantener ágiles notificaciones con los letrados y en su caso procuradores, se les solicita, cuando se acepta su personación, la designación de un correo electrónico al que remitirle la documentación y las notificaciones."

También consta en el Expediente NUM002 de esta Dirección de Supervisión y Control informe del Secretario Relator del Tribunal Militar Central de fecha 8 de febrero de 2023 que: "Este auto fue notificado a través de los correos profesionales tanto de la Procuradora (el que consta en el Ilustre Colegio de Procuradores de DIRECCION001) como de los tres Oficiales denunciados, quienes ya habían tenido conocimiento puntual del procedimiento al notificárseles el auto de archivo de las actuaciones y que como investigados tenían, asimismo, derecho a conocer la totalidad del procedimiento como consecuencia del derecho de acceso que le reconoce el artículo 118 de la Ley de Enjuiciamiento Criminal".

Con arreglo a lo establecido en el artículo 65.2 de la Ley Orgánica 3/2018, la Agencia Española de Protección de Datos *"inadmitirá las*



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

reclamaciones presentadas cuando no versen sobre cuestiones de protección de datos de carácter personal, carezcan manifiestamente de fundamento, sean abusivas o no aporten indicios racionales de la existencia de una infracción”.

En el marco de las funciones que, con arreglo a lo dispuesto en el citado artículo 236 nonies, apartado primero, de la Ley Orgánica del Poder Judicial, el Consejo General del Poder Judicial tiene atribuidas como autoridad de control, le corresponde pronunciarse sobre la admisibilidad a trámite de la reclamación formulada.

Con estos antecedentes, cabe concluir que la reclamación reproduce sustancialmente los mismos hechos que ya fueron objeto de examen y resolución por esta Dirección de Supervisión y Control de Protección de Datos, limitándose a incorporar nuevos motivos o argumentos jurídicos respecto de una controversia previamente decidida. Tal circunstancia impide la apertura de un nuevo procedimiento, en la medida en que las resoluciones dictadas por las autoridades de protección de datos ponen fin a la vía administrativa, sin perjuicio de los recursos legalmente previstos.

En efecto, los artículos 63 y siguientes de la Ley Orgánica 3/2018, de 5 de diciembre de Protección de datos personales y garantía de los Derechos Digitales, regulan el procedimiento de tramitación de reclamaciones ante las autoridades de protección de datos, mientras que el artículo 48.6 de la misma norma establece que las resoluciones de la AEPD, aplicable a esta autoridad de Control, ponen fin a la vía administrativa. Por su parte, los artículos 112 y siguientes de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, articulan los cauces ordinarios de impugnación de tales resoluciones, reservando los artículos 106 y siguientes y 125 y siguientes de la misma ley a los supuestos excepcionales de revisión de actos firmes.

De conformidad con el principio de seguridad jurídica consagrado en el artículo 9.3 de la Constitución Española, la firmeza de los actos administrativos impide reabrir de forma sucesiva e indefinida cuestiones ya decididas mediante la mera alegación de nuevos fundamentos jurídicos que pudieron haber sido invocados en el procedimiento originario. Admitir lo contrario supondría desconocer el efecto preclusivo inherente a los actos administrativos firmes y vaciar de contenido las limitadas vías extraordinarias de revisión previstas por el ordenamiento.



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

En consecuencia, existiendo identidad sustancial entre los hechos objeto de la presente reclamación y los ya examinados en el procedimiento anteriormente resuelto, y no concurriendo hechos nuevos, circunstancias sobrevenidas ni ninguna de las causas excepcionales que permiten la revisión de actos firmes, procede declarar la improcedencia de una nueva reclamación, sin que la invocación de distintos motivos de impugnación permita reabrir una cuestión ya definitivamente resuelta.

Por lo expuesto, la Directora de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial, por el presente

ACUERDA

1.- Inadmitir la reclamación formulada por D. Casiano frente al Juzgado Togado Militar Central núm. 1.

2.- Notificar la presente resolución a D. Casiano.

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