



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

SOLICITUD DE INFORMACIÓN

Asunto: Consulta-020/2026

Por la presente se comunica que ha tenido entrada en esta Dirección de Supervisión y Control de Protección de Datos, sus consultas referentes a:

La primera, versa sobre "Conforme al art 129 bis de la LEC las intervenciones telemáticas deben hacerse siempre desde punto de acceso seguro. El problema que se me plantea es asegurar que se hace desde ese tipo de acceso. No tengo inconveniente- salvo que por la materia o la duración previsible del interrogatorio o la actuación sea conveniente la asistencia presencial - que la intervención se realice desde lugar seguro (juzgado del domicilio, IML, comisaria...) que además garantizan la identidad del interviniente y se acomoda más a la solemnidad del acto, pero normalmente pretenden conectarse desde cualquier lugar y dispositivo, cuyas condiciones desconozco; se han dado el caso acceso de un testigo sin decir nada y detectar su "presencia" el auxilio judicial por percibir una respiración o un ruido; al desconocimiento de las condiciones de dispositivo, se añade que no puedes saber con certeza si hay alguien más en la estancia con la parte, testigo o perito o si la identificación que proporciona es correcta."

En cuanto a la segunda, se refiere "al acceso que se ha dado a los funcionarios a todas las plazas judiciales a raíz de los TI. Al ser servicios comunes y trabajar para todas o varias plazas o ser movibles, pueden acceder a los procedimientos de alguna, algunas o todas ellas. Tal acceso es mayor que el de los jueces y magistrados porque nosotros tenemos acceso a la plaza propia y mantenemos el acceso a las plazas del partido en los que por algún motivo (vg.r abstención) hayamos tenido que intervenir en un asunto, pero no a las plazas en las que nunca hemos trabajado.

Antes en el juzgado podía haber más control sobre el acceso a los datos pues la distribución del trabajo era clara, había posibilidad de controlar más el horario de trabajo y pautas claras por ejemplo sobre cadencia de las consultas domiciliarias, averiguaciones patrimoniales. Trabajábamos magistrado, letrado y funcionarios en la misma estancia o en estancias próximas, normalmente sin puertas o con puertas abiertas, con lo que era



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

más sencillo tener cierta supervisión en esta materia. Además, el acceso de los funcionarios se limitaba a los asuntos del propio juzgado.

Ahora, por lo menos en lo que se refiere a Cartagena, concretamente a la Sección Civil, los funcionarios, están distribuidos en dos plantas (en la 5ª los declarativos por así decirlo y en la 6ª los de ejecución) y en cada una de las plantas están en departamentos cerrados y cuyo interior no es visible desde el pasillo. Aunque en principio tengan asignado un tipo de procedimiento (desahucios y precarios; verbales, ordinarios, jurisdicción voluntaria, ejecución no judicial, etc) o una fase concreta (incoación, tramitación) y plaza o varias plazas, nada impide que se les asignen sobre la marcha otros por necesidades del servicio (más ahora porque los ajustes para distribución del trabajo son continuos). Quizá por esto se les ha dado ese acceso generalizado, pero ello supone un riesgo mayor de acceso indebido a datos personales que en una oficina dispersa y cambiante es más difícil de controlar y detectar. En el caso de los auxilios judiciales el acceso es amplio a todas las plazas al rotar en las salas

Planteo esto no por desconfianza hacia el funcionario pues parto de su profesionalidad y del cumplimiento del deber de sigilo y reserva que nos concierne, como también del deber de abstención en asuntos con los que haya algún vínculo que a ello obligue, sino porque la normativa en protección de datos es cada vez más rigurosa en el nivel de protección y en la exigencia de responsabilidades y en una oficina abierta y "fluida" no puede dejarse esta materia a la buena voluntad o recomendaciones genéricas y seguir funcionando en esta materia como si siguiéramos siendo juzgados. Veo difícil el papel de jueces y magistrados en esta materia orillados en la oficina judicial."

En relación a las consultas planteadas se procede a informar en los siguientes términos:

PRIMERO.- Como punto de partida de ambas preguntas, y a los efectos de que se produzca un tratamiento de datos personales, el Reglamento General de Protección de Datos, en su artículo 5 regula los principios del tratamiento, entre los que se encuentra el principio de integridad y confidencial que supone que los datos personales sean 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 u organizativas apropiadas".

En aplicación de este principio, el artículo 32 del RGPD denominado "Seguridad del tratamiento" contienen un mandato para que los responsables



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

y encargados del tratamiento, *“teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:*

- a) la seudonimización y el cifrado de datos personales;*
- b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
- c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;*
- d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.”*

SEGUNDO.- Los puntos de acceso seguros y lugares seguros se regulan en el artículo 62 Real Decreto-ley 6/2023, de 19 de diciembre, siendo aquellos que *“cumplan los requisitos que se determinen por la normativa del Comité técnico estatal de la Administración judicial electrónica, que en todo caso deberán reunir, al menos, los siguientes:*

- a) Permitir la transmisión segura de las comunicaciones y la protección de la información.*
- b) Permitir y garantizar la identificación de los intervinientes.*
- c) Cumplir los requisitos de integridad, interoperabilidad, confidencialidad y disponibilidad de lo actuado.”*

Además, deberán también:

- “a) Disponer de dispositivos y sistemas que tengan la condición de punto de acceso seguro, conforme al apartado anterior.*
- b) Garantizar la comprobación de la identidad de los intervinientes y la autonomía de su intervención.*
- c) Asegurar todas las garantías del derecho de defensa, inclusive la facultad de entrevistarse reservadamente con el Abogado o Abogada.*
- d) Disponer de medios que permitan la digitalización de documentos para su visualización por videoconferencia.”*



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

Asimismo, el citado precepto contiene una serie de supuesto que, sin perjuicio de lo anterior, determina como lugares seguros, siendo:

- a) La oficina judicial correspondiente al tribunal competente, o cualquier otra oficina judicial o fiscal, y las oficinas de justicia en el municipio.*
- b) Los Registros Civiles, para actuaciones relacionadas con su ámbito.*
- c) El Instituto Nacional de Toxicología y Ciencias Forenses y los Institutos de Medicina Legal, para la intervención de los Médicos Forenses, Facultativos, Técnicos y Ayudantes de Laboratorio.*
- d) Las sedes de las Fuerzas y Cuerpos de Seguridad del Estado, para la intervención de sus miembros.*
- e) Las sedes oficiales de la Abogacía del Estado, del Servicio Jurídico de la Administración de la Seguridad Social y de los Servicios Jurídicos de las Comunidades Autónomas, para la intervención de los miembros de tales servicios.*
- f) Los Centros penitenciarios, órganos dependientes de Instituciones Penitenciarias, centros de internamiento de extranjeros y centros de internamiento de menores, para las personas internas y funcionarios públicos.*
- g) Cualesquiera otros lugares que se establezcan por Reglamento de aplicación en todo el territorio del Estado, previo informe favorable del Comité técnico estatal de la Administración judicial electrónica.*

TERCERO.- A los efectos de cumplir los requisitos descritos anteriormente para ser considerado como punto seguro, el Comité técnico estatal de la Administración judicial electrónica ha elaborado un documento de manera que la entidad o persona física que se conecte de forma telemática garantice a través de una declaración responsable que los dispositivos, sistemas y lugares desde los que se accede a los sistemas de la Administración de Justicia cumple con los requisitos mínimos funcionales, técnicos y de seguridad establecidos para los puntos de acceso seguro y lugares seguros en la Guía Técnica de Interoperabilidad y Seguridad de Requisitos de puntos de acceso seguro y lugares seguros del CTEAJE.

Se facilita dicha declaración responsable como Anexo a esta consulta.

De esta forma, lo que puede realizar en el caso planteado es solicitar a quien vaya a participar es que firme esta declaración responsable, en caso de que cumpla los requisitos que figuran en la misma.

CUARTO.- Por lo que respecta, al posible acceso generalizado consecuencia de la nueva organización judicial de la Ley Orgánica 1/2025, de



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

2 de enero, de medidas en materia de eficiencia del Servicio Público de Justicia, como bien indica en su consulta supone un mayor riesgo.

No obstante, el personal sólo debe consultar la documentación judicial en el ejercicio de sus funciones y cuando deba realizar el correspondiente trámite, pudiendo incurrir en responsabilidades en caso contrario.

Además, como buena parte de la implementación de las medidas de seguridad, le corresponde a su Administración prestacional, sobre todo las de carácter técnico. Por ello, debería existir un registro de accesos, de manera que, cada vez que se acceda a un documento judicial por el personal debe quedar registrado quien ha accedido, a qué ha accedido y durante cuánto tiempo.

En consecuencia, sería recomendable que desde ese Tribunal de Instancia se recordase al personal que sólo pueden acceder a la documentación judicial para el ejercicio de sus funciones y cuando corresponda.

QUINTO.- No obstante lo anterior, procede precisar lo siguiente:

- De su consulta se desprende el acceso a documentación, y no al posible uso de cuentas de correo electrónico compartidas que, de existir, no debería ser utilizadas para el envío entre el personal de documentos judiciales puesto que para esta finalidad se puede utilizar las propias funcionalidades del sistema de gestión procesal.
- Dado que no es la primera consulta de este tipo que esta Dirección ha recibido, durante el segundo semestre de este año está previsto que se inspeccione un Tribunal de Instancia para obtener más información sobre la situación descrita, y poder valorar si se puede adoptar algún tipo de alternativa que permita reducir el riesgo, más allá de lo descrito anteriormente.

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