INFORME

SOBRE EL POSIBLE ACCESO DE LA POLICÍA JUDICIAL AL SISTEMA DE GESTIÓN PROCESAL "ADRIANO"**.**

I. ANTECEDENTES

1.Se ha recibido solicitud de informe presentada por la Presidencia de la Sección de Instrucción del Tribunal de Instancia relativa al posible acceso de la Policía Judicial a determinada información obrante en el sistema de gestión procesal "Adriano".

Según el contenido de la consulta, en la sede de la Ciudad de la Justicia se encuentra ubicada la Unidad de Policía Judicial, que según el Real Decreto 769/1987, de 19 de junio, en su artículo 26 quedan asignadas a los respectivos Decanatos, hoy Tribunales de Instancia, sin perjuicio de su dependencia funcional directa en la relación de cometidos específicos de investigación establecido por cada órgano jurisdiccional.

La gran mayoría de procedimientos que se incoan en los Juzgados de Instrucción de se hace en virtud de atestados remitidos previamente por la Policía Nacional, los cuales en su mayoría requieren una ampliación posterior de las investigaciones. Surge la problemática de que la policía, pese a tener el contenido de la denuncia inicial en sus archivos y el justificante de la presentación por Lexnet, no posee el número de diligencias previas que se asigna al atestado presentado, por lo que el atestado con ampliaciones tiene que presentarse de forma aislada en el juzgado de guardia si conocer a quien fue turnado.

Este hecho supone que el citado Juzgado de Guardia tiene que realizar una indagación previa para localizar y buscar el juzgado competente a quien se le ha atribuido el atestado inicial, dedicando tiempo para ello, e incluso a veces se dificulta eta labor por existir algún error en la identificación del atestado ampliado. Con la nueva Ley Orgánica 1/2025, de 2 de enero, de medidas en materia de Eficiencia del Servicio Público de Justica, se hace más necesario la identificación con el atestado inicial con el número de previas asignado a fin de conocer el destino.

A este respecto, la propia Policía Judicial ya dispone desde hace años un acceso a los archivos judiciales que constan en el SIRAJ a los efectos de dar cumplimiento a las medidas que pueda instar cualquier juzgado.

Ante todo esto, y puesto que con anterioridad ya se hizo esta solicitud a la Comisión Lexnet, se ha solicitado a los servicios informáticos de la Junta de Andalucía que se facilite a la Unidad de la Policía Judicial adscrita a los juzgados y tribunales ubicada en la primera planta del edificio judicial, mediante el uso y contraseña o bien tarjetas criptográficas en sus ordenadores, un punto de conexión sólo de consulta al sistema informático Adriano para cada uno de los integrantes de la citada Unidad, con idéntico contenido al punto de acceso que existe en la Oficina de Información al Público, de tal forma que el citado acceso limitado comprenda:

- Fecha de entrada del asunto.
- Número de atestado.
- Número de asunto.
- Nombre de la persona y DNI.
- Y otros extremos que constan en el listado de consulta de intervinientes cuyo modelo anonimizado se adjunta.

A día de hoy, incluso, se tiene que acudir a esa Oficina de Información al Público para solicitar los datos para poder asociar los atestados ampliatorios.

Asimismo, este sistema de acceso que se plantea ya existiría desde hace años en los Juzgados de Madrid.

Por otra parte, desde la Consejería de Justicia de la Comunidad Autónoma de Andalucía, han planteado dudas de forma verbal sobre esta posible solución aduciendo que afectaría a la protección de datos personales. No obstante, a juicio del consultante carece de sentido debido a que:

La policía ya tiene esta información en sus propias bases de datos; en segundo lugar, no se facilita el contenido de las actuaciones judiciales sino únicamente el número de previas o verificar la existencia de denuncias anteriores; y en tercer lugar, la propia policía ya puede consultar datos más sensibles en SIRAJ.

En definitiva, se solicita si esta solución de acceso a determinada información obrante en el sistema de gestión procesal "Adriano" con la finalidad descrita

resulta factible, ya que desde el punto de vista del consultante no afecta a lo dispuesto en la normativa de protección de datos personales.

2. Una vez recibida esta petición, por la Dirección de Supervisión y Control de Protección de Datos del CGPJ se han realizado diferentes actuaciones a los efectos de aclarar los términos de la consulta así como si en alguna Comunidad Autónoma existía en el sistema de gestión procesal un acceso similar al planteado.

II. CONSIDERACIONES

3. Analizado el contenido de la petición, procede indicar que la solución planteada debería tener un carácter provisional y nunca definitivo, puesto que se debería arbitrar como solución que se recibiese por el órgano policial un oficio, escrito o similar, el cual además se puede automatizar por la Administración prestacional, en el que se indicase el órgano receptor del atestado inicial.

4. En todo caso, y a los efectos de permitir un acceso al sistema de gestión procesal para consultar la información que se describe en la petición de informe, y valorar su procedencia, debe tenerse en cuenta lo siguiente:

-Se trata de información a la cual pueden acceder las Fuerzas y Cuerpos de Seguridad en el ejercicio de sus funciones como policía judicial atendiendo a lo dispuesto en la Ley de Enjuiciamiento Criminal.

- En la práctica, y según el contenido de la petición de informe, ya se estaría accediendo mediante la información que facilita la Unidad de Atención al Ciudadano. No obstante, facilitar la misma de manera verbal impide la trazabilidad, además de que la finalidad de dicha Unidad no es precisamente esta sino como su nombre indica atender a los ciudadanos.

-En cambio, el hecho de permitir un acceso como el propuesto permitiría esa trazabilidad que en la actualidad no existe.

5. No obstante, y respecto al acceso propuesto debe matizarse lo siguiente:

El artículo 32 del Reglamento General de Protección de Datos Personales regula la "Seguridad del tratamiento". Según su apartado primero:

"1. 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."

A su vez, 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, dispone en su artículo 37 titulado "Seguridad del tratamiento":

"1. El responsable y el encargado del tratamiento, teniendo en cuenta el estado de la técnica y los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los niveles de riesgo para los derechos y libertades de las personas físicas, aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado, especialmente en lo relativo al tratamiento de las categorías de datos personales a las que se refiere el artículo 13. En particular, deberán aplicar a los tratamientos de datos personales las medidas incluidas en el Esquema Nacional de Seguridad.

2. Por lo que respecta al tratamiento automatizado, el responsable o encargado del tratamiento, a raíz de una evaluación de los riesgos, pondrá en práctica medidas de control con el siguiente propósito:

a) En el control de acceso a los equipamientos, denegar el acceso a personas no autorizadas a los equipamientos utilizados para el tratamiento.

b) En el control de los soportes de datos, impedir que estos puedan ser leídos, copiados, modificados o cancelados por personas no autorizadas.

c) En el control del almacenamiento, impedir que se introduzcan sin autorización datos personales, o que estos puedan inspeccionarse, modificarse o suprimirse sin autorización.

d) En el control de los usuarios, impedir que los sistemas de tratamiento automatizado puedan ser utilizados por personas no autorizadas por medio de instalaciones de transmisión de datos.

e) En el control del acceso a los datos, garantizar que las personas autorizadas a utilizar un sistema de tratamiento automatizado, sólo puedan tener acceso a los datos personales para los que han sido autorizados.

f) En el control de la transmisión, garantizar que sea posible verificar y establecer a qué organismos se han transmitido o pueden transmitirse, o a cuya disposición pueden ponerse los datos personales mediante equipamientos de comunicación de datos.

g) En el control de la introducción, garantizar que pueda verificarse y constatarse, a posteriori, qué datos personales se han introducido en los sistemas de tratamiento automatizado, en qué momento y quién los ha introducido.

h) En el control del transporte, impedir que durante las transferencias de datos personales o durante el transporte de soportes de datos, los datos personales puedan ser leídos, copiados, modificados o suprimidos sin autorización.

i) En el control de restablecimiento, garantizar que los sistemas instalados puedan restablecerse en caso de interrupción.

j) En el control de fiabilidad e integridad, garantizar que las funciones del sistema no presenten defectos, que los errores de funcionamiento sean señalados y que los datos personales almacenados no se degraden por fallos de funcionamiento del sistema."

En este sentido, y conforme al Real Decreto-ley 6/2023, de 19 de diciembre, el artículo 88 configura el Esquema Judicial de Interoperabilidad y Seguridad constituido, según su apartado primero, "*por el conjunto de instrucciones técnicas de interoperabilidad y seguridad aprobadas por el Comité técnico estatal de la Administración judicial electrónica y que permitan el cumplimiento del Esquema Nacional de Interoperabilidad y del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, recogiendo las particularidades de la Administración de Justicia que requieran una concreta regulación*".

En la práctica, con alguna precisión al tener en cuenta la compleja organización judicial, se sigue lo dispuesto en el Esquema Nacional de Seguridad regulado por el Real Decreto 311/2022, de 3 de mayo.

En todo caso, a los efectos de proceder al acceso se debería:

- Sobre el acceso planteado, se debería realizar un análisis de riesgos, que podría elaborarse conjuntamente por la Administración prestacional y por las Fuerzas y Cuerpos de Seguridad.
- Además, de acceder con un certificado electrónico de tarjeta criptográfica, o mediante usuario y contraseña, como se propone en la consulta, sería conveniente añadir por razones de seguridad un segundo factor de autenticación.
- Y como ya se ha señalado, esta solución debe ser meramente provisional, mientras no exista el procedimiento descrito en el punto 3.

III. CONCLUSIONES.

PRIMERO.- Debería existir un sistema por el cual, una vez que se remitiese el primer atestado, la policía judicial tuviese conocimiento del órgano judicial destinatario. Incluso, como se ha puesto de manifiesto, dicho sistema se podría automatizar.

SEGUNDO.- Se puede realizar el acceso solicitado en los términos descritos en la consulta, mientras no exista el sistema referido en la conclusión primera.

En todo caso, se deberá dar cumplimiento a los requisitos contemplados en el punto 5 del presente informe.

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