INFORME

SOBRE EL USO DEL CORREO ELECTRÓNICO PARA LA DACIÓN DE CUENTA PUDIENDO VULNERAR LA NORMATIVA DE PROTECCIÓN DE DATOS PERSONALES**.**

I. ANTECEDENTES

1.Se ha recibido informe del Tribunal Superior de Justicia mediante el cual pone de manifiesto determinadas disfunciones detectadas en los mecanismos de comunicación en los tribunales de ese territorio en relación con la dación de cuenta y el recurso del correo electrónico valorando su posible incidencia en la protección de datos personales.

En su escrito señala que la dación de cuenta constituye el instrumento estructurado esencial para la comunicación entre el personal tramitador y los órganos judiciales, al permitir trasladar de forma ordenada el estado procesal del procedimiento y la concreta actuación sometida a decisión judicial.

Sin embargo, se han advertido diferentes disfunciones que están generando la utilización como medio alternativo de comunicación del correo electrónico, usándolo para transmitir indicaciones, documentación procesal e incluso resoluciones, tanto entre magistrados del mismo Tribunal como los servicios comunes.

A este respecto, el correo electrónico, sin embargo, no constituye un canal integrado en el expediente judicial electrónico ni en los sistemas de gestión procesal, careciendo de funcionalidades esenciales desde la perspectiva de control del tratamiento de la información, como son la trazabilidad de accesos, el registro de actuaciones y la adecuada delimitación de perfiles de acceso. Además, su utilización puede permitir el acceso a información judicial por parte de personal no directamente vinculado al procedimiento, especialmente en el ámbito de los servicios comunes e incluso suponer una brecha en la seguridad de la información ya que no se trata de un canal seguro.

Desde su punto de vista, esta forma de actuar supone una afectación al principio de integridad y confidencialidad de datos, al no existir garantías de acceso y difusión de la información, así como de minimización, en la medida de acceder a datos que no sean estrictamente necesarios.

A modo de conclusión, el uso del correo electrónico resulta incompatible con el modelo de justicia digital implantada no garantizado los niveles de seguridad, confidencialidad y trazabilidad de la información, debiendo sensibilizar desde el CGPJ a la carrera judicial de los peligros para la seguridad de los datos de la utilización del correo electrónico como cauce de comunicación.

II. CONSIDERACIONES

2. Con carácter previo, procede manifestar que esta Dirección de Supervisión y Protección de Datos Personales del Consejo General del Poder Judicial es la autoridad de protección de datos personales sobre los tratamientos de datos personales que realicen los órganos juridiciales con fines jurisdiccionales, es decir, en el marco del procedimiento judicial.

Este tratamiento con fines jurisdiccionales se regula por el Reglamento General de Protección de Datos (RGPD), 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, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales, Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (principalmente, los artículos 236 bis a 236 decies, y demás normativa que fuese de aplicación.

3. El RGPD configura una serie de principios en su artículo 5, entre los que se encuentra el principio de "integridad y confidencialidad", según el cual, los datos personales serán "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".

4. Este principio se completa con lo dispuesto en el artículo 32 del RGPD 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."

5. Por su parte, 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, aplicable al tratamiento de datos personales en el ámbito penal, también contempla en su artículo 6 los principios del tratamiento.

A imagen y semejanza del RGPD, se recoge que los datos personales serán "Tratados de manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental. Para ello, se utilizarán las medidas técnicas u organizativas adecuadas".

6. En consonancia con este principio, dispone el artículo 37 titulado "Seguridad del tratamiento" de la Ley Orgánica 7/2021, de 26 de mayio:

"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.

7. En definitiva, el tratamiento de datos personales derivado de los procedimientos judiciales a través de los sistemas de gestión procesal debe cumplir la normativa de protección de datos personales, incluyendo lo referente a la seguridad, tanto los principios como los preceptos anteriormente descritos.

8. Del texto del informe remitido por el Tribunal Superior de Justicia n se desprende que, en ocasiones, no se estaría utilizando para la dación de cuenta el procedimiento habilitado en el sistema de gestión procesal sino el correo electrónico.

Este hecho podría suponer la vulneración de los principios referidos así como las medidas de seguridad puesto que:

- Pueden estar accediendo a la documentación y resoluciones judiciales personal que no tenga que acceder;
- No se garantiza la trazabilidad de los documentos judiciales.
- No se envían de manera cifrada.
- Al salir del sistema de gestión procesal, quedan expuestos a que terceros ajenos a la organización judicial puedan acceder a los mismos (por ejemplo mediante suplantaciones de correos electrónicos).

III. CONCLUSIONES.

PRIMERO.- La utilización del correo electrónico, en vez del sistema de dación de cuenta habilitado en el sistema de gestión procesal, para el envío de documentación y resoluciones judiciales puede suponer un incumplimiento de los principios y medidas de seguridad de protección de datos personales.

SEGUNDO.- En consecuencia, no debería utilizarse el correo electrónico para tal fin.

TERCERO.- La Presidenta del Tribunal Superior de Justicia de Castilla León puede difundir el presente informe con la finalidad de concienciar al personal de los órganos judiciales de ese ámbito territorial.

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