ECIJA
Torre de Cristal Pº de la Castellana, 259C
28046 Madrid · Tel: +34 917 816 160
www.ecija.com

Nota informativa STS 543/2022: La adopción de medidas para garantizar la seguridad de los datos de carácter personal no es una obligación de resultado, sino de medios

7/03/2022

Sobre la diligencia de la persona jurídica en las medidas de seguridad en materia de protección de datos

RESUMEN: "La obligación de adoptar las medidas necesarias para garantizar la seguridad de los datos personales no puede considerarse una obligación de resultado, que implique que, producida una filtración de datos personales a un tercero exista responsabilidad, con independencia de las medidas adoptadas y de la actividad desplegada por el responsable del fichero o del tratamiento".

La reciente Sentencia del Tribunal Supremo 543/2022 de 15 de febrero resuelve sobre la **cuestión de interés casacional**, para la formación de la jurisprudencia, relativa a si las **infracciones de la Ley de Protección de Datos por fallos de las medidas de seguridad** que puedan cometer los empleados de una persona jurídica **deben examinarse en atención al resultado y, por lo tanto, imputarse a la persona jurídica, con independencia de los medios y medidas de prevención que hubiera podido adoptar**.

Los hechos analizados están relacionados con la gestión de solicitudes de financiación en las que una empleada registró una dirección de correo electrónico que no correspondía a los solicitantes para que el sistema le permitiese continuar con la tramitación. Como consecuencia, se produjo un acceso no autorizado por parte de terceros a 14 solicitudes de financiación en las que obraban datos personales (nombre y apellidos, datos económicos, de domiciliación bancaria y firma).

Resolviendo la cuestión objeto de casación, el TS interpreta que estamos una obligación de medios, en la que: *"el compromiso que se adquiere es el de adoptar los medios técnicos y organizativos, así como desplegar una actividad diligente en su implantación y utilización que tienda a conseguir el resultado esperado con medios que razonablemente puedan calificarse de idóneos y suficientes para su consecución, por ello se las denomina obligaciones "de diligencia " o "de comportamiento"*. A diferencia de una obligación de resultado, en la que *"se responde ante un resultado lesivo por el fallo del sistema de seguridad, cualquiera que sea su causa y la diligencia utilizada"*.

Esta interpretación es la más acorde con la redacción del artículo 31 del Reglamento General de Protección de Datos (en adelante, RGPD), por el que **la suficiencia de las medidas de seguridad ha de ponerse en relación con el estado de la tecnología y técnica en cada momento, así como el nivel de protección requerido por los datos tratados, pero no se garantiza un resultado.**

Sin embargo, no basta con diseñar los medios técnicos y organizativos necesarios, sino también su correcta implantación, de modo que **también se responderá por la falta de la diligencia en su utilización**, entendida como una diligencia razonable acorde a las circunstancias del caso.

A esta distinción responde el Artículo 73 d), e) y f) del RGPD, que recogen la infracción de falta de adopción de medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado y el Artículo 73 g) del RGPD, que estipula la infracción por falta de debida diligencia en la utilización de dichas medidas técnicas y organizativas implantadas.

Por tanto, **sin que sea exigible la infalibilidad de las medidas adoptadas, resulta exigible la adopción e implantación de medidas técnicas y organizativas, que conforme al estado de la tecnología y en relación con la naturaleza del tratamiento realizado y los datos personales en cuestión, permitan razonablemente evitar su alteración, pérdida o tratamiento no autorizado.**

En el caso analizado, se constata que el programa utilizado para la recogida de los datos no contenía ninguna medida de seguridad que permitiese comprobar si la dirección de correo electrónico introducida por la empleada pertenecía realmente a la persona cuyos datos estaban siendo tratados. La Sala concluye que "*el estado de la técnica en el momento en el que se produjeron estos hechos permitía establecer medidas destinadas a comprobar la veracidad de la dirección de email, condicionando la continuación del proceso a que el usuario recibiese el contrato en la dirección proporcionada…*".

En este sentido, la propia entidad sancionada indicaba que el programa no disponía de un sistema de verificación del correo electrónico, pero que habría sido posible un sistema basado en el **doble "opt-in"**, si bien este debería haber sido implantado por la entidad responsable del tratamiento. Por ello, **la Sentencia identifica, que era factible en este caso implementar un control de doble opt-in para comprobar que la información recogida es correcta y veraz, y el hecho de no hacerlo supone falta de diligencia en la comprobación de los datos**.

Entiende la Sala que el hecho de que la herramienta que carecía de las medidas de comprobación fuese diseñada por el Responsable **no exime al Encargado de responsabilidad, dado que "*implantó y utilizó dicho programa siendo conocedora, o hubiera debido serlo, de que éste carecía de las medidas de seguridad necesarias*".**

Por último, el TS reafirma que: "*las **personas jurídicas responden por la actuación de sus empleados** o trabajadores. **No se establece por ello una responsabilidad objetiva, pero si es trasladable a la persona jurídica la falta de diligencia de sus empleados**, en tal sentido Sentencia del Tribunal Constitucional 246/1991, de 19 de diciembre*".

Por este motivo, en el supuesto analizado**, el hecho de que la actuación fuese cometida por una empleada negligente no exime a la mercantil de su responsabilidad** en la correcta utilización de las medidas de seguridad, ya que se entiende que las medidas implementadas no eran suficientes para mitigar el riesgo de esta actuación inadecuada por parte de esta y, en consecuencia, garantizar un adecuado funcionamiento del sistema (en este caso, el del registro de clientes).

En consecuencia, del contenido de la Sentencia pueden extraerse **tres conclusiones principales**, de gran relevancia en relación con el tratamiento de los datos personales:

- No se exige la infalibilidad de las medidas de seguridad (existe una obligación de medios, no de resultado), pero su implantación ha ser diligente para permitir los resultados esperables.
- Existe una obligación de adoptar medidas para confirmar que los datos de contacto recabados son correctos (como un sistema de doble opt-in).

- El encargado del tratamiento puede resultar responsable por la adopción de medidas de seguridad inadecuadas o insuficientes, aunque estas sean diseñadas por el responsable del tratamiento.

Área de Privacidad de ECIJA

info@ecija.com

Telf: + 34 91.781.61.60