

MULTA DE 300.000 € POR ABANDONO DE HISTORIAS CLÍNICAS CONFIRMADA POR EL TRIBUNAL SUPREMO

Recientemente se ha publicado Sentencia de la Sala de lo Contencioso Administrativo del Tribunal Supremo por la que se confirma la sanción impuesta por la Agencia Española de Protección de Datos de 300.506,05 euros a una clínica por tirar historiales clínicos a la basura.



El hecho que ha dado lugar a la imposición de esta multa y a su posterior confirmación tanto por la Audiencia Nacional como por el Tribunal Supremo fue la publicación en prensa del hallazgo en un contenedor de Sevilla de expedientes de pacientes que habían acudido a la consulta ginecológica de una Clínica. Al parecer estos historiales médicos, que contenían datos tales como el motivo de la consulta, antecedentes, alergias, medicación, resultado de la exploración física, juicio clínico y tratamiento, habrían sido depositados en la basura por un administrativo de la sociedad que presta en la Clínica los servicios ginecológicos. Esta conducta fue calificada por la Agencia como una vulneración del deber de guardar secreto sobre los datos de carácter personal al que hacen referencia el apartado 3 del artículo 7 de Ley Orgánica de Protección de Datos, entre los que se encuentra la información referente a la salud.

De esta Sentencia se deben extraer dos conclusiones. Por un lado, la importancia de las medidas de seguridad aplicables al soporte papel y por otro lado el deber de implicar a todos los trabajadores que tengan acceso a datos de carácter personal en las políticas de protección de datos que se adopten.

Como sabemos, desde abril de 2010 es obligatorio el cumplimiento de las medidas de seguridad en soporte papel exigidas para los ficheros de nivel alto, como los que contienen datos de salud, establecidas en el Real Decreto 1720/2007, que aprueba el Reglamento de desarrollo de la LOPD. Sin embargo, el cumplimiento de estas medidas no puede limitarse al establecimiento de una serie de protocolos y de recursos, sino que se debe involucrar al personal que tenga acceso a los datos, ya sean profesionales sanitarios o de administración, incluyendo contabilidad, recepción, atención al paciente, etc. Se deben establecer políticas de formación para los empleados y procedimientos mediante los que puedan conocer cuáles son sus obligaciones y responsabilidades en protección de datos.

Uno de los aspectos que la sociedad condenada recurría era precisamente que la documentación fue depositada en un contenedor de la vía pública por un tercero, identificado por la propia sociedad como un administrativo, lo que, manifiesta la Sentencia, comporta la atribución de responsabilidad para la sociedad médica.

Es decir, cuando un trabajador incumple la normativa protección de datos, el responsable será la empresa para la que trabaje (como responsable del fichero), sin perjuicio de que posteriormente la sociedad pueda, en su caso, tomar las acciones legales correspondientes contra dicho trabajador. Por este motivo es importante concienciar a todos los trabajadores de las políticas adoptadas por sus empresas en esta materia, siendo asimismo, muy recomendable la contratación de un seguro que cubra los riesgos que las empresas deban soportar a pesar del cumplimiento de la normativa de protección de datos.

Por último, recordar que la normativa de protección de datos no debe cumplirla sólo el Hospital o el centro sanitario, sino también será exigible a las sociedades médicas que presten sus servicios dentro de un hospital o clínica, debiendo analizarse en este caso las relaciones creadas con los hospitales o clínicas en lo que respecta a la información de los pacientes.