¿DEBE RESPONDER LA EMPRESA EN CASO DE BRECHA DE SEGURIDAD CUANDO CUMPLE CON LA NORMATIVA?

21 de marzo de 2022

Si una empresa aplica de forma exhaustiva todas las obligaciones que establece la normativa, así como las medidas de seguridad según la tipología de datos que trata y basándose en un análisis de riesgos, y, aun así, tiene una brecha de seguridad, ¿la pueden sancionar?

Analizamos esta reciente sentencia STS 543/2022 de 15 de febrero de 2022 relevante en el ámbito de la protección de datos sobre la obligación de medios vs obligación de resultado.

En concreto, el Tribunal Supremo se ha pronunciado sobre si los errores de las medidas de seguridad cometidos por los trabajadores deben ser imputados a la persona jurídica por el resultado lesivo que producen o, si, por el contrario, se deben valorar las medidas de prevención adoptadas. En las siguientes líneas analizaremos la resolución del TS y determinaremos la responsabilidad de la empresa.

Antecedentes de hecho

Esta sentencia gira en torno a una **infracción de seguridad cometida por una trabajadora, que permitió el acceso por parte de terceros no autorizados a al menos 14 solicitudes de financiación**. Estos documentos contenían **datos personales de los clientes** (nombre y apellido, datos económicos, domiciliación bancaria y firma). Este acceso se produjo porque, para poder realizar el contrato de financiación, es necesario rellenar un formulario, que entre otros datos solicita el correo electrónico para enviar una copia de dicho contrato. La trabajadora para poder rellenar el formulario usaba una cuenta de correo electrónico que creía inexistente. El resultado fue que mandó a dicho correo los contratos de financiación de los clientes.

¿Qué obligación tiene el empresario respecto a las medidas de seguridad?

Las obligaciones pueden ser de resultado o de medios. En el primer supuesto se obliga a obtener un resultado concreto, en el segundo, en cambio, se obliga a adoptar una serie de medios técnicos y organizativos que tiendan a obtener el fin que se persigue. La diferencia principal radica en la responsabilidad, en el primer supuesto se es responsable en caso de producción de un resultado lesivo, mientras que, en el segundo supuesto, para no responder basta con establecer e implementar de manera diligente medidas técnicas adecuadas.

En relación con la protección de datos se debe establecer una obligación de medios, esto implica, implantar una serie de medidas técnicas y organizativas conforme a la tecnología actual y al tratamiento realizado. La **sentencia en cuestión considera**

que no se cumple con la implantación de las medidas conforme a la tecnología actual **por no tener instaurado el sistema** de verificación de correo electrónico "**doble *opt-in***".

¿Qué es el "doble *opt-in*"?

Doble *opt-in* es un sistema que permite comprobar la veracidad de la información subministrada a partir de un sistema de doble verificación. Para hacerlo, se manda un correo electrónico de confirmación a la dirección facilitada para asegurarse de este modo que el usuario acepta el tratamiento de sus datos.

Esta medida existía en el momento en el que se produjeron los hechos, y por eso el TS considera que no se han implementado todas las medidas posibles.

¿Responde el empresario por fallos cometidos por sus trabajadores?

Sí, se traslada a las personas jurídicas la falta de diligencia de sus empleados. En el presente supuesto, el programa utilizado por la empresa no implementaba todas las medidas disponibles en el momento en el que sucedieron los hechos. La implementación de todas las medidas disponibles hubiese evitado la filtración de datos personales.

En conclusión

Lo fundamental para poder **evitar las brechas de seguridad** son unas **medidas de seguridad adecuadas en base a los datos gestionados** y de acuerdo con los procesos técnicos actuales y, una correcta **formación a los trabajadores** que les permita saber qué riesgos entrañan sus acciones y estar concienciados con lo que puede pasar.

Aun así, habiendo aplicado las medidas correctas, podemos sufrir un ataque de día cero, por ejemplo, ante el que no podemos reaccionar porque aprovecha una nueva vulnerabilidad. En un caso así, si nos basamos solo en resultado, no lo podremos evitar

Fuente: www.economistjurist.es