EL TRIBUNAL SUPREMO DELIMITA LA RESPONSABILIDAD DE LAS EMPRESAS ANTE LA EXISTENCIA DE BRECHAS DE SEGUIDAD

El alto Tribunal establece y acota el deber de diligencia, y el control de la efectividad de las políticas de seguridad.

La Sala en su Fundamentación Jurídica (Tercera, Cuarta y Quinta), establece una serie de consideraciones y pronunciamientos de gran transcendencia práctica y jurídica. A destacar:

La obligación que recae sobre el responsable del tratamiento y sobre el encargado, respecto a la adopción de medidas necesarias para garantizar la seguridad de los datos no es una obligación de resultado sino **una obligación de medios, 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 y los datos, que permitan razonablemente evitar su alteración pérdida, y tratamiento no autorizado.

No basta con diseñar los medios técnicos y organizativos necesarios, también **es imprescindible su correcta implantación y utilización de forma apropiada**, de modo que también responderá (la empresa) por la falta de la diligencia en su utilización, entendida como una **diligencia razonable atendiendo a las circunstancias del caso y a la tecnología al alcance en cada momento.**

La clave es conseguir el resultado esperado con aquellos medios que razonable y tecnologicamente puedan calificarse en cada momento de idóneos y suficientes para garantizar la seguridad de los datos. Estamos ante una obligación de diligencia y comportamiento proactivo.

EL TRIBUNAL SUPREMO DELIMITA LA RESPONSABILIDAD DE LAS EMPRESAS ANTE LA EXISTENCIA DE BRECHAS DE SEGUIDAD

La Sala también insiste en otras interesantes cuestiones trascendentes de índole práctica:

1. Las personas jurídicas responden en cuestiones de seguridad por la actuación de sus empleados o trabajadores. Se traslada a la persona jurídica la falta de diligencia de sus empleados. De ahí la importancia de instaurar programas de control periódico, así como planes de formación continua dirigida a los trabajadores.

2. **El encargado del tratamiento** -la persona física o jurídica que solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento -, **también deberá adoptar las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos en los términos anteriormente enunciados.**

Como conclusión:

- El Tribunal no considera las medidas de seguridad como medidas de resultado, razón por la cual no es exigida la infalibilidad de las medidas instrumentadas. Son obligaciones de medios.

- Es exigible implantar medidas de seguridad y desplegar las mismas **diligentemente, con medios idóneos y suficientes** en concordancia con el estado de la tecnología en cada momento.

  Por ejemplo, la Sala confirma en su fallo la sentencia recurrida por entender *que en el momento en el que se produjeron los hechos existían medidas técnicas referidas al proceso de registro de datos personales que hubieran evitado la brecha de seguridad y que ni el responsable ni el encargado tenían implantadas*. En este caso la implementación de un mecanismo de doble verificación que asegura que los usuarios han aceptado la política de privacidad y tratamiento de datos antes de recibir cualquier tipo de comunicación, garantizando así que la información recogida es correcta, y veraz, que de estar implementados hubieran evitado la sanción.

- Se recomienda entonces, la **utilización de sistemas de verificación del correo electrónico**, sistemas conocidos como "*doble op-in*", que permiten establecer un proceso de aceptación de normas o condiciones de uso, cuyo principal objetivo es verificar que los usuarios son quienes dicen ser y no robots o terceras personas, que generen suscripciones fraudulentas utilizando correos electrónicos que nos son de su propiedad.

- Se recomienda igualmente, (i) **establecer controles de seguridad periódicos** que analicen si los sistemas de seguridad responden a la tecnología que está al alcance del responsable del tratamiento; (ii) proceder a **instrumentar programas de formación continua** en materia de seguridad dirigido a trabajadores; (iii) así como establecer **programas de control periódico** por parte del responsable sobre el cumplimiento del estándar de seguridad exigido a cada encargado del tratamiento.

Área Tecnologías de la Información