



Ataques cibernéticos, protección de datos y deber de diligencia



José Antonio Muñoz
Socio director de Muñoz Arribas
Abogados

De todos es conocido la importancia del deber de diligencia del profesional, empresario, directivo, etc., a la hora de dilucidar su responsabilidad, pero lo que no esta tan claro es hasta dónde alcanza dicho deber en supuestos tales como los daños a terceros derivados de ataques informáticos.

El Tribunal Supremo (STS 1456/2021, de 13 de diciembre) recientemente ha abordado el caso de una suplantación de la personalidad para la obtención de un microcrédito que conllevó que los datos de la persona suplantada acabasen inscritos en un listado de morosos.

Lo interesante de la sentencia es la fijación del deber de diligencia de las empresas, pues considera que aún existiendo, y aplicándose, las medidas previstas por la empresa (registro en la plataforma; validación del DNI, con verificación de doble factor de 2 algoritmos que garantizan tanto la veracidad del número y la letra del documento como que el solicitante tiene en su poder el DNI. por original o copia: validación del número de teléfono móvil a través de un código PIN. validación de datos bancarios y validación de la tarjeta de crédito/débito aportada por el solicitante; y pese a la adopción de tales medidas) se podría haber cometido el delito de suplantación de identidad, de estafa y/o de uso indebido de documento verdadero.

En síntesis, las medidas de verificación aplicadas por la empresa afectada parecen enteramente encaminadas asegurar el buen fin del préstamo, pero, en cambio, se desentienden enteramente del objetivo de verificar la veracidad y exactitud de los datos, y, en particular, de comprobar que quien solicita el crédito es precisamente quien dice ser.

El Supremo concluye que no puede recaer sobre la empresa contratante la responsabilidad de impedir que se produzca un hecho ilícito o delictivo como es la utilización fraudulenta de un DNI por parte de quien no es su titular. Pero sí es exigible a dicha empresa contratante, como diligencia necesaria para que no se le pueda reprochar el incumplimiento de sus obligaciones en materia de protección de datos de carácter personal -tanto en lo que se refiere a la exigencia de consentimiento del interesado como en lo relativo al principio de veracidad y exactitud de los datos- la implantación de medidas de control tendentes a verificar que la persona que pretende contratar es quien dice ser, esto es, que coincide con el titular del DNI aportado.

