Recuadro 2.5

## EL NUEVO REGLAMENTO DE RESILIENCIA OPERATIVA DIGITAL

Como parte de su estrategia de finanzas digitales, y con el fin de mitigar los riesgos asociados a la digitalización y mejorar la resiliencia del sistema financiero europeo, la Comisión Europea publicó en septiembre de 2020 su propuesta legislativa de un nuevo reglamento sobre resiliencia operativa digital, conocido como DORA por sus siglas en inglés.

Tras un proceso de negociación que duró dos años, el texto final de DORA se publicó en diciembre de 2023, siendo su fecha de aplicación enero de 2025.

El hecho de que el instrumento legislativo elegido sea un reglamento garantiza que la misma norma se aplicará en todos los países de la Unión Europea, logrando de esa forma una armonización sin precedentes en la regulación sobre resiliencia tecnológica para el sistema financiero europeo.

El alcance de DORA es sorprendentemente amplio, ya que será de aplicación a todo tipo de instituciones financieras, de todo tamaño, con la debida proporcionalidad. La Comisión reconoce así que, dado el elevado nivel de interconexiones e interdependencias entre las distintas entidades que forman parte del sistema financiero, es imprescindible garantizar unos niveles mínimos de resiliencia comunes a todas ellas para conseguir que el sector sea resiliente en su conjunto.

La resiliencia no es, en ningún caso, un mero ejercicio de cumplimiento. En una auténtica declaración de principios, el capítulo sobre gestión de los riesgos asociados a la tecnología empieza con un artículo dedicado a la gobernanza y la organización, en el que se establecen las responsabilidades y obligaciones del órgano de dirección de las entidades, que necesitará entender estos riesgos e implicarse directamente en su gestión. En muchas entidades esto supondrá un punto de inflexión que obligará a revisar la composición de sus órganos de dirección, sus funciones y su nivel de implicación en la resiliencia operativa de la institución.

Si bien podría argumentarse que los requerimientos de DORA sobre gestión de los riesgos asociados a la tecnología, gestión y notificación de incidentes tecnológicos, realización de pruebas sobre la resiliencia de los sistemas y gestión de los riesgos con terceras partes no son completamente novedosos, sí lo es el haberlos elevado a la categoría de un reglamento aplicable a todo el sector. En la actualidad, los niveles de resiliencia de las entidades financieras no son homogéneos, por lo que el esfuerzo que deberán hacer para cumplir con los requerimientos de DORA será también diferente en cada caso. Esto preocupa especialmente a las entidades más pequeñas, para las que puede ser un reto importante dotarse de los recursos técnicos y humanos necesarios.

Otra de las novedades con mayor impacto sobre los supervisores son las provisiones de DORA sobre la realización de pruebas avanzadas de ciberseguridad *(Threat Led Penetration Tests),* similares a las que ya existen en algunos países, entre ellos España, bajo el marco TIBER. Estas pruebas deberán realizarse con una frecuencia determinada (en principio, cada tres años) y se exigirán a un número potencialmente elevado de entidades, lo que demandará recursos supervisores significativos. Si bien algunas entidades ya se someten a estas pruebas de modo voluntario, para otras supondrá elevar sustancialmente el nivel de exigencia.

Asimismo, DORA contiene provisiones animando a las entidades a compartir de modo voluntario información de amenazas y vulnerabilidades, ya que, si bien los beneficios de esta compartición son indiscutibles, a menudo existen reticencias al respecto.

Pero, sin duda, la característica de DORA que más ha dado que hablar, y que ha convertido el reglamento en un referente a escala mundial, es el establecimiento de un nuevo marco de vigilancia sobre aquellos proveedores tecnológicos externos que sean críticos para el sistema financiero europeo en su conjunto, un aspecto que está cobrando cada vez más relevancia dada la tendencia creciente a la externalización de algunas funciones esenciales. La Comisión es consciente de que para mejorar el nivel de resiliencia del sector es imprescindible tener en cuenta a los proveedores de servicios tecnológicos sobre los que se apoyan las funciones críticas del negocio de las entidades, especialmente aquellos que han alcanzado una dimensión sistémica. El nuevo esquema de vigilancia será liderado por agencias europeas de supervisión, si bien los supervisores nacionales deberán prestar apoyo en esta función.

La puesta en marcha de este mecanismo de vigilancia está requiriendo y va a requerir un esfuerzo significativo por parte de todas las autoridades del sector financiero europeo, entre ellas el Banco de España. En un principio, se deberán desarrollar procedimientos y metodologías para realizar una supervisión efectiva sobre compañías grandes y complejas, con modelos de negocio, organización y

estructuras de gobierno muy diferentes entre sí, con las que los supervisores financieros no están familiarizados. Además, las autoridades tendrán que dotarse de los recursos adicionales necesarios, lo que implicará incorporar un número significativo de profesionales con un nivel de especialización técnica elevado. Este tipo de perfiles son escasos y muy demandados por todo tipo de compañías, por lo que su captación y retención supondrá un reto para los supervisores.

Más allá de los aspectos anteriormente mencionados, también cabe destacar que el reglamento establece numerosas obligaciones adicionales para las autoridades competentes, con lo que reconoce que son piezas fundamentales en el ecosistema. Tendremos que hacer un esfuerzo de coordinación sin precedentes, y asumir un rol activo, más allá de nuestro papel como vigilantes del cumplimiento de la norma, por ejemplo, promoviendo la realización de ejercicios de resiliencia sectoriales.