



### Javier Puyol

Magistrado y letrado del Tribunal Constitucional en excedencia. Socio director de Puyol Abogados

## DORA o el reglamento comunitario sobre resiliencia operativa digital

**E**l escenario actual de la ciberseguridad se caracteriza por las constantes oleadas de ciberataques de alta persistencia y sofisticación tecnológica, originados por atacantes que están explotando el crecimiento exponencial de la superficie de exposición que comportan una pluralidad de circunstancias, que oscilan entre todas las manifestaciones derivadas de la ciberdelincuencia, hasta los riesgos vinculados con el trabajo a distancia.

Estos hechos han determinado que finalmente el Consejo de la UE recientemente haya aprobado el Reglamento sobre la Resiliencia Operativa Digital (DORA), el cual tienen como finalidad el asegurar que el sector financiero en Europa siga funcionando de forma resiliente en el caso de la existencia de una grave perturbación operativa, que comprometa su continuidad en el negocio. El término resiliencia, tan utilizado en la actualidad, hace referencia a la necesidad de que las entidades de carácter financiero asuman con flexibilidad la situación que está atravesando y al mismo tiempo sean capaces de sobreponerse a ella, saliendo favorecidas por el hecho de enfrentarse y superar dichas circunstancias.

El Reglamento DORA establece nuevos requisitos uniformes para la seguridad de las redes y los sistemas de información de las empresas y organizaciones que operan en el sector financiero, así como de terceros esenciales, que les presen servicios relacionados con las TIC (tecnologías de la información y la comunicación), como plataformas en la nube o servicios de análisis de datos, dibujando con relación a estos últimos una nueva estrategia, consistente en someterlos y vincularlos a esta nueva regulación. Como consecuencia de todo ello, el objetivo de DORA es fundamentalmente el hecho de crear un marco regulador sobre la resiliencia operativa digital conforme al cual todas las empresas deban asegurarse de que pueden resistir y responder a cualquier tipo de perturbación y amenaza relacionada con las TIC y recuperarse de ellas.

Una de las funciones específicas del Reglamento DORA consiste en que el establecimiento de este conjunto de requisitos tengan el carácter de homogéneo en todos los Estados miembros de la UE. Debe tenerse presente que el principal objetivo es prevenir y mitigar las ciberamenazas.



En este sentido el Reglamento DORA parte de una premisa inicial consistente en la constatación de una realidad en la que actualmente nos encontramos, basada en que en la era digital las tecnologías de la información y la comunicación (TIC) constituyen el soporte de los sistemas complejos utilizados en actividades cotidianas ya que a través de los mismos, se mantienen de manera principal, las economías de la zona euro, especialmente en sectores claves como puede ser el sector financiero, con el propósito colateral de llevar a cabo una mejora del mercado interior.

En este sentido, hay factores que deben tenerse en cuenta, y que hacen referencia al aumento más que evidente de la digitalización y de la interconexión entre toda clase de dispositivos, lo que lleva consigo un aumento más que relevante derivado del uso de las TIC.

Es evidente, que ante este panorama tanto la Sociedad en su conjunto, como de manera muy especial el sector financiero en particular, sean mucho más vulnerables a las ciberamenazas o a las perturbaciones que pueden llevar consigo el uso indiscriminado de las TIC, lo que evidencia la necesidad de proceder a reforzar la ciberseguridad en todas sus magnitudes. Consecuentemente con ello, en

los Considerandos del Reglamento DORA se pone de manifiesto que, si bien el uso generalizado de los sistemas de TIC y la alta digitalización y conectividad constituyen sin lugar a duda una de las características básicas y fundamentales de las actividades desarrolladas por las entidades financieras dentro de la Unión Europea, por dicha razón, se hace preciso abordar e integrar mejor su resiliencia digital en sus marcos operativos más sólidos y amplios.

Dicho Reglamento, parte del hecho consistente en que el uso de las TIC's ha adquirido en las últimas décadas un papel fundamental en la prestación de servicios financieros, hasta el punto de que ahora tiene una importancia fundamental en la ejecución de las funciones cotidianas típicas de todas las entidades. Por ello, puede afirmarse que la digitalización abarca ahora prácticamente la totalidad de la actividad de dichas entidades poniendo como ejemplo de ello algunas de las funcionalidades desarrolladas que son más típicas y recurrentes, entre las que cabe citar las que se indican a continuación: los pagos, para los que se utilizan, cada vez más, soluciones digitales; la actividad vinculada a la compensación y la liquidación de valores; la negociación electrónica y algorítmica las operaciones de préstamo y financiación; la financiación entre particulares; la calificación crediticia, la gestión de siniestros y las operaciones administrativas.

El uso de las TIC también ha transformado el sector de los seguros, desde la aparición de intermediarios de seguros que ofrecen sus servicios en línea y desarrollan su actividad con tecnología aplicada al sector de los seguros (*InsurTech*) hasta la suscripción de seguros por medios digitales. También debe resaltarse, que este auge producido en el uso de las TIC ha traído consigo, en términos del Reglamento, una profundización de las interconexiones y las dependencias existentes dentro del sector financiero, en relación con proveedores terceros de infraestructuras y servicios.

A modo de conclusión, es evidente que en este momento donde el escenario actual de la ciberseguridad se caracteriza por las constantes oleadas de ciberataques de alta persistencia y sofisticación tecnológica, originados por atacantes que, además de los escenarios tradicionales, están explotando el crecimiento exponencial de la superficie de exposición que comporta el uso de las TIC en todas sus manifestaciones, y por ello, la ciberseguridad en el sector financiero debe ser reforzada de manera efectiva y eficiente, de ahí las nuevas aportaciones y exigencias contenidas en el Reglamento DORA en aras de incrementar la misma en este ámbito tan estratégico de la actividad económica.



## La ciberseguridad en el sector financiero debe ser reforzada en un momento de ciberataques de alta persistencia