Entidades críticas y resiliencia en la UE: nueva propuesta de Directiva

Félix Arteaga | Investigador principal, Real Instituto Elcano.

La Comisión Europea ha multiplicado su actividad normativa en el campo de la ciberseguridad y entre las distintas iniciativas [1] se encuentra una nueva propuesta de Directiva para reforzar la ciberseguridad de las entidades que prestan servicios esenciales en la UE: la Directiva sobre la resiliencia de entidades críticas que se analiza en este comentario (la Propuesta de ahora en adelante). Con las nuevas directivas, la Comisión busca reforzar la capacidad de los Estados miembros para proteger y recuperar sus infraestructuras y servicios críticos nacionales y, progresivamente, avanzar en la armonización de la resiliencia europea. Para ello aumenta los deberes de los Estados miembros: elaborar estrategias, llevar a cabo análisis de riesgos e identificar y supervisar las entidades críticas, entre otros.

"Con las nuevas directivas, la Comisión busca reforzar la capacidad de los Estados miembros para proteger y recuperar sus infraestructuras y servicios críticos nacionales (…)"

La protección de las infraestructuras críticas en la UE se ha encuadrado tradicionalmente dentro de las estrategias y competencias de Interior de la UE (Estrategia de Seguridad de la Unión, DG Home, ENISA) al igual que lo ha sido en los Estados Miembros (Ministerio del Interior y Centro Nacional de Protección de Infraestructuras Críticas, CNPIC, en el caso español). La regulación comenzó mediante el Programa para la protección de las infraestructuras críticas europeas en 2006, seguido de la Directiva 2008/114 que se aplicó a los sectores de transporte y energía a la que sucede esta nueva propuesta de Directiva sobre la resiliencia de entidades críticas de diciembre de 2020. A ese periodo y marco corresponde la Ley 8/2011 para la protección de infraestructuras críticas en España.

Posteriormente, la ciberseguridad dejó de ser un componente más de ese enfoque de seguridad interior y adquirió un perfil propio, vinculado a la seguridad de la información y diferenciado respecto a los perfiles tradicionales asociados a la seguridad física. En este sentido, las medidas de la Directiva sobre la seguridad de las redes y sistemas de información, Directiva NIS de 2016, acentuó la importancia de los elementos digitales en la seguridad de las todas las entidades, estuvieran o no catalogadas como infraestructuras críticas y esta importancia no ha dejado de crecer. Esta diferenciación progresiva en la protección de las infraestructuras críticas ha creado conflictos de competencias y perfiles profesionales de sus responsables tanto en el ámbito público

[1] Entre otras, la Estrategia de Ciberseguridad de la UE, la estrategia Digital de la UE, la propuesta de Directiva sobre Seguridad de las redes y sistemas de información (Directiva NIS revisada o NIS2).

como el privado para integrar los nuevos componentes de seguridad digital en el marco tradicional de seguridad física.

Desde entonces, también ha crecido el número de infraestructuras que se han vuelto críticas para el funcionamiento de la economía digital, la interdependencia entre ellas y con otros bienes y servicios esenciales para las sociedades y su exposición a nuevos riesgos, por lo que se ha considerado necesario reforzar su protección y resiliencia. Como resultado, la Comisión puso en marcha una evaluación de la Directiva 2008/114 en 2012 que concluyó en 2019[2].

Entre sus conclusiones figura la constatación de que, a pesar de los progresos en la protección de las infraestructuras, no se puede concluir que la Directiva haya alcanzado sus objetivos de armonización en la UE debido, probablemente, a que el margen de interpretación que las directivas dan a los Estados miembros resta empuje a la armonización (unos países consideran sectores y operadores que otros no reconocen y viceversa). También a que los Estados y entidades han partido de un nivel de madurez diferente o a que los mecanismos de supervisión no han sido lo suficientemente eficaces para forzar la convergencia. Aunque no se han producido grandes incidentes, no se ha podido establecer hasta qué punto se debe a las medidas adoptadas y no se ha encontrado una correlación entre inversiones a cargo del sector privado y los resultados (también probablemente por la falta de trasparencia de Estados y entidades responsables) ni existe unanimidad entre las entidades reguladas sobre el sentido y proporcionalidad de esa correlación (no se han registrado grandes incidentes ni en las infraestructuras europeas que adoptaron las medidas de la Directiva ni entre las que no lo hicieron)[3].

En la evaluación se reconoció su efecto tractor, para impulsar cambios normativos y la toma de conciencia sobre la necesidad de proteger las infraestructuras críticas, especialmente en los sectores de energía y transportes, pero también se constató el agotamiento de su efecto. A la aparición de nuevas necesidades de protección (nuevos servicios esenciales según la terminología de la Directiva NIS) siguió la creciente interdependencia de las infraestructuras críticas, soporte de los servicios esenciales, con otros servicios no regulados por la Directiva y el solapamiento de ésta con otras regulaciones.

La Comisión descartó elaborar un reglamento porque la protección de las infraestructuras críticas entra dentro de las competencias de los Estados miembros y les corresponde a estos determinar el alcance de la revisión. Por ello la Comisión orientó sus consultas con Estados y entidades a elaborar una Directiva que añadiera valor a las medidas gubernamentales y a las que adoptaran las entidades responsables de las

[2] Las conclusiones se encuentran recogidas en el documento de la Comisión sobre Comprehensive Assessment of EU Security Policy, SWD(2017) 278 de 26 de julio y, más resumidas, en el preámbulo de la Propuesta o en los estudios de impacto que la acompañan.

[3] En España, la trasposición de la Directiva PIC incluyó a los operadores de infraestructuras críticas entre las entidades obligadas por las normas.

infraestructuras para mejorar su resiliencia. También, y debido a su impacto transfronterizo, la Comisión aprovecharía la actualización para reforzar la armonización de las obligaciones de las entidades cuya disrupción tiene alcance europeo y apoyar los mecanismos de protección y supervisión de los Estados miembros, cualquiera que fuera la amenaza o riesgo al que se enfrentan.

En líneas generales, se consideró que la capacidad de protección de los operadores de infraestructuras críticas no era la adecuada para hacer frente al nuevo contexto de riesgos[4]. Se amplió su ámbito a sectores distintos de los ya regulados, pero con un elevado nivel de interdependencia. También se consideró necesario ampliar el foco desde la protección, en unos niveles que se consideraban satisfactorios, hacia la resiliencia fomentando la mayor y más rápida recuperación de los sectores si la protección fallaba. Posteriormente, la revisión de la Estrategia de Seguridad [Interior] de la UE para el período 2020-2025 dedicó más atención a la ciberseguridad que su predecesora y reivindicó la necesidad de aproximar las dimensiones física y ciber de la seguridad, lo que dio origen a dos propuestas de directiva elaboradas en paralelo: la de la Directiva NIS2 y la de la Directiva sobre resiliencia de entidades críticas[5].

La nueva Directiva de resiliencia (RCE en sus siglas inglesas) amplía su ámbito de regulación a nuevos sectores distintos de los de transporte y energía haciéndolos coincidentes a los sectores de servicios esenciales establecidos en la propuesta de Directiva NIS2: administración pública, banca, finanzas, espacio, salud, aguas e infraestructuras digitales; y dedica especial atención a los que actúan en tres o más países de la UE (entidades de críticas de relevancia europea). Las entidades críticas deben ahora desarrollar análisis de riesgos, planes de respuesta y notificar los incidentes de importancia, unas obligaciones con las que ya están familiarizados los responsables de infraestructuras críticas de los países como España en los que la protección ha desarrollado una notable madurez. También mejora el procedimiento para identificar las entidades críticas armonizando los criterios nacionales en los análisis nacionales de riesgos que se actualizarán, como las estrategias, cada cuatro años.

> “La Propuesta entra ahora en una fase de refinamiento en la que gobiernos y entidades críticas pueden presentar modificaciones tras la cual acabará entrando en vigor la nueva Directiva”.

Al igual que en las directivas NIS, los Estados miembros deciden si existe una o varias puertas de entrada para las notificaciones de incidentes, lo que complica su gestión a pesar de la creación de un grupo de coordinación entre la Comisión y los Estados miembros (*Critical Entities Resilience Group*) que puede interactuar con las entidades críticas, aunque no se aclaran las condiciones de la participación en la propuesta. Los Estados miembros deberán elaborar estrategias de actuación incluyendo objetivos,

[4] Doc. COM (2020) 829 de 16 de diciembre sobre la evaluación de impacto de la propuesta sobre resiliencia de entidades críticas, p. 10.

[5] En ella se reitera la necesidad de afrontar los riesgos físicos y digitales que puedan aprovechar amenazas como el terrorismo, los desastres naturales, accidentes, actores mal intencionados o nuevas tecnologías, incluida la experiencia de la pandemia COVID-19.

medidas y modelo de gobernanza, además de reforzar sus capacidades de supervisión y cumplimiento. Estas incluyen, –al menos en el estado actual de la Propuesta–, la realización de inspecciones y auditorías sobre las entidades críticas, además de la posibilidad de imponer sanciones.

La Propuesta entra ahora en una fase de refinamiento en la que gobiernos y entidades críticas pueden presentar modificaciones tras la cual acabará entrando en vigor la nueva Directiva. La colaboración entre los anteriores, en las capitales o en Bruselas, será necesaria para mejorar la redacción actual y, sobre todo, para ponerla en práctica. Una tarea nada fácil por la superposición de normas afines, la diferente interpretación de cada Estado miembro y el coste de los mecanismos de supervisión en una época en la que todos los encargados de proteger las infraestructuras críticas se enfrentan a limitaciones de recursos.