DICTAMEN DEL BANCO CENTRAL EUROPEO

de 11 de abril de 2022

sobre una propuesta de directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148

(CON/2022/14)

(2022/C 233/03)

Introducción y fundamento jurídico

El 16 de diciembre de 2020 la Comisión Europea adoptó una propuesta de directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148 ([1]) (en lo sucesivo, la «directiva propuesta»). El 3 de diciembre de 2021 el Consejo de la Unión Europea acordó su orientación general sobre la directiva propuesta ([2]). La competencia consultiva del Banco Central Europeo (BCE) se basa en el artículo 127, apartado 4, del Tratado de Funcionamiento de la Unión Europea, pues la directiva propuesta contiene disposiciones que afectan a las competencias del BCE, en particular las de promover el buen funcionamiento de los sistemas de pago, contribuir a la buena gestión de las políticas que lleven a cabo las autoridades competentes con respecto a la estabilidad del sistema financiero, y supervisar prudencialmente las entidades de crédito, conforme al artículo 127, apartado 2, cuarto guion, y al artículo 127, apartados 5 y 6, del Tratado. De conformidad con la primera frase del artículo 17.5 del Reglamento interno del Banco Central Europeo, el presente dictamen ha sido adoptado por el Consejo de Gobierno.

Observaciones generales

El BCE respalda resueltamente los objetivos de la directiva propuesta de incrementar el nivel de ciberresiliencia en todos los sectores pertinentes, reducir incoherencias en el mercado interior, y mejorar el nivel de conciencia situacional y la capacidad colectiva de preparación y respuesta, garantizando una cooperación eficaz en la Unión.

El BCE reconoce la importancia de mantener vínculos estrechos entre la directiva propuesta y el sector financiero, que debe seguir formando parte del ecosistema de seguridad de las redes y sistemas de información (SRI) para promover una evaluación coherente de los riesgos relacionados con las tecnologías de la información y de las comunicaciones (TIC) en toda la Unión, así como un intercambio de información intersectorial y una colaboración eficaz al abordar las ciberamenazas. Con este fin, las autoridades competentes deben, conforme a la propuesta de reglamento del Parlamento Europeo y del Consejo sobre la resiliencia operativa digital del sector financiero ([3]) (en lo sucesivo, «DORA»), participar en los debates estratégicos y en los trabajos técnicos del Grupo de Cooperación SRI, así como intercambiar información y cooperar más con los puntos de contacto únicos y los equipos nacionales de respuesta a incidentes de seguridad informática a que se refiere la directiva propuesta ([4]).

1. Alcance de la directiva propuesta

1.1 El BCE entiende que, respecto de las entidades del sector financiero, DORA se considerará como legislación de carácter sectorial que introduce requisitos de gestión de riesgos y notificación de incidentes de ciberseguridad de efectos al menos equivalentes a los de los requisitos establecidos en la directiva propuesta ([5]). Por lo tanto, las disposiciones de la directiva propuesta relativas a gestión de riesgos, obligaciones de comunicación e intercambio de información, y medidas de supervisión y ejecución, en materia de ciberseguridad, no serán de aplicación a las entidades financieras sujetas a DORA ([6]). Como se aclara en los considerandos de la directiva propuesta, se les

([1]) COM(2020) 823 final.
([2]) Disponible en la dirección del Consejo en internet, www.consilium.europa.eu.
([3]) COM(2020) 595 final.
([4]) Véase el apartado 1.5 del Dictamen CON/2021/20 del Banco Central Europeo, de 4 de junio de 2021, acerca de una propuesta de reglamento del Parlamento Europeo y del Consejo sobre la resiliencia operativa digital del sector financiero (DO C 343 de 26.8.2021, p. 1). Todos los dictámenes del BCE se publican en EUR-Lex. Véanse el artículo 17, apartado 5, y el artículo 42, de DORA, así como el artículo 11 de la directiva propuesta.
([5]) Artículo 2, apartado 6, de la directiva propuesta.
([6]) Considerando 13, y artículo 2, apartado 6, de la directiva propuesta.

aplicarán las disposiciones de DORA sobre las medidas de gestión de riesgos de TIC, la gestión y comunicación de incidentes de TIC, las pruebas de resiliencia operativa digital, los mecanismos de intercambio de información, y el riesgo de terceros relacionado con TIC, y no las disposiciones de la directiva propuesta ([7]).

1.2 El BCE observa además que el Consejo, en su orientación general sobre la directiva propuesta, propone una modificación para excluir del ámbito de aplicación de la directiva propuesta a las «entidades que lleven a cabo actividades en los ámbitos del poder judicial, los parlamentos o los bancos centrales» ([8]). El BCE entiende que la modificación propuesta alcanzaría a todas las funciones y competencias básicas del Sistema Europeo de Bancos Centrales (SEBC) conforme al artículo 127, apartado 2, del Tratado, y al artículo 3.1 de los Estatutos del Sistema Europeo de Bancos Centrales y del Banco Central Europeo (en lo sucesivo, los «Estatutos del SEBC»), tales como la promoción del buen funcionamiento de los sistemas de pago. Sobre este punto, las infraestructuras del mercado financiero propiedad del Eurosistema y gestionadas por él, como TARGET2 y TARGET2-Securities, se consideran comprendidas en el ámbito de la exclusión de la aplicación de la directiva propuesta sugerida por el Consejo.

2. El SEBC y las competencias de vigilancia del Eurosistema

2.1 Junto al objetivo principal del SEBC de mantener la estabilidad de precios, y de acuerdo con el artículo 127, apartado 2, del Tratado, una de las funciones básicas que deben llevarse a cabo a través del SEBC es la de promover el buen funcionamiento de los sistemas de pago ([9]). En el desempeño de esta función básica, el BCE y los bancos centrales nacionales pueden proporcionar medios, y el BCE dictar reglamentos, destinados a garantizar unos sistemas de compensación y liquidación eficientes y solventes dentro de la Unión, así como con otros países ([10]). En el ejercicio de su función de vigilancia, el BCE adoptó el Reglamento (UE) n.º 795/2014 (BCE/2014/28) ([11]) (en lo sucesivo, el «Reglamento sobre los SIPS»), que transforma los principios para las infraestructuras del mercado financiero de CPSS-IOSCO ([12]) en derecho directamente aplicable. El Reglamento sobre los SIPS establece requisitos para los sistemas de grandes y pequeños pagos de importancia sistémica, sean de titularidad pública o privada. Entre los requisitos del Reglamento sobre los SIPS ya se incluyen la gestión del riesgo operativo y el establecimiento de un marco de ciberresiliencia ([13]).

2.2 Además de los sistemas de pago de importancia sistémica, la vigilancia del Eurosistema comprende los sistemas de pago sin importancia sistémica, los instrumentos electrónicos de pago, los regímenes y acuerdos de pago y otras infraestructuras y proveedores de servicios críticos, según se indica en el marco de la política de vigilancia del Eurosistema ([14]). Los sistemas y otros acuerdos de pago sujetos a la vigilancia del Eurosistema no se incluyen expresamente en el ámbito de aplicación de la directiva propuesta ([15]). Asimismo, puesto que la directiva propuesta es un instrumento de armonización mínima ([16]), la legislación de ejecución que aprueben los Estados miembros podría solaparse con las competencias de vigilancia del Eurosistema. Para evitarlo, en los considerandos de la directiva propuesta deberían reconocerse expresamente las competencias del SEBC conforme al Tratado y a los Estatutos del SEBC y las competencias del Eurosistema conforme al Reglamento sobre los SIPS y, en general, conforme al marco de la política de vigilancia del Eurosistema.

([7]) Considerando 13 de la directiva propuesta.
([8]) Artículo 2, apartado 3 *bis*, número 1, letra b), de la orientación general del Consejo sobre la directiva propuesta.
([9]) Artículo 127, apartado 2, del TFEU, reproducido en el artículo 3.1 de los Estatutos del SEBC.
([10]) Artículo 22 de los Estatutos del SEBC.
([11]) Reglamento (UE) n.º 795/2014 del Banco Central Europeo, de 3 de julio de 2014, sobre los requisitos de vigilancia de los sistemas de pago de importancia sistémica (BCE/2014/28) (DO L 217 de 23.7.2014, p. 16).
([12]) Véase Comité de sistemas de Pago y Liquidación (CPSS) y Comité Técnico de la Organización Internacional de Comisiones de Valores (IOSCO), *Principios aplicables a las infraestructuras del mercado financiero*, abril de 2012, disponible en la dirección del Banco de Pagos Internacionales en internet, www.bis.org. Según la responsabilidad D de dichos principios, «cabe esperar que todos los miembros del CPSS y la IOSCO apliquen dichos principios a las FMI pertinentes de sus jurisdicciones en la medida en que lo permita el marco legal de su jurisdicción».
([13]) Artículo 15 del Reglamento (UE) n.º 795/2014 (BCE/2014/28).
([14]) *Eurosystem oversight policy framework*, versión revisada (julio de 2016), disponible en inglés en la dirección del BCE en internet, www.ecb.europa.eu.
([15]) Artículo 2, y anexos I y II, de la directiva propuesta.
([16]) Artículo 3 de la directiva propuesta.

3. **Riesgo de terceros relacionado con TIC, gestión de incidentes y crisis a gran escala, intercambio de información y estrategia nacional de ciberseguridad**

3.1 *Gestión del riesgo de terceros relacionado con TIC*

3.1.1 La directiva propuesta faculta a las autoridades competentes, cuando ejerzan sus facultades de ejecución en relación con entidades esenciales, para emitir instrucciones vinculantes o una orden de requerimiento para que dichas entidades subsanen las deficiencias detectadas o las infracciones de las obligaciones establecidas en la directiva propuesta ([17]). Al mismo tiempo, el «supervisor principal» designado conforme a DORA puede dirigir recomendaciones a los proveedores terceros esenciales de servicios de TIC para la gestión de los riesgos potencialmente sistémicos derivados de las prácticas de externalización y de la concentración de TIC en terceros ([18]).

3.1.2 Puesto que una entidad esencial conforme a la directiva propuesta puede también ser designada como proveedor tercero esencial de servicios de TIC conforme a DORA, el BCE reitera ([19]) la necesidad de evitar recomendaciones e instrucciones vinculantes que se contradigan. En este punto, el BCE celebra la orientación general del Consejo sobre la directiva propuesta, conforme a la cual, las autoridades competentes deben informar al «Foro de Supervisión» establecido de conformidad con DORA cuando ejerzan sus facultades de supervisión y ejecución con objeto de garantizar el cumplimiento por parte de una entidad esencial identificada conforme a DORA como proveedor tercero esencial de servicios de TIC ([20]).

3.2 *Gestión de incidentes y crisis a gran escala*

3.2.1 Conforme a la directiva propuesta ([21]), cada Estado miembro debe designar una o varias autoridades competentes responsables de la gestión de incidentes y crisis a gran escala. Como aclaran los considerandos de la directiva propuesta, por incidente a gran escala debe entenderse un incidente que cause perturbaciones que superen la capacidad de un Estado miembro para responder a él o que afecte significativamente por lo menos a dos Estados miembros. Los incidentes a gran escala pueden convertirse en una crisis propiamente dicha que impida el correcto funcionamiento del mercado interior ([22]).

3.2.2 Aunque las autoridades competentes designadas conforme a DORA siguen siendo las responsables de gestionar los incidentes de ciberseguridad que afecten a las entidades financieras, será esencial para garantizar una respuesta coordinada en toda la Unión que cooperen con las estructuras y autoridades establecidas conforme a la directiva propuesta. Para ello, el BCE celebraría que las autoridades competentes designadas conforme a DORA, incluido el BCE, participasen en la red de funcionarios de enlace nacionales para la gestión de cibercrisis (EU-CyCLONe) ([23]) cuando se produjeran incidentes y crisis de ciberseguridad a gran escala que afectasen al sector financiero.

3.3 *Intercambio de información*

3.3.1 Como se acaba de exponer, el BCE es firme partidario de la cooperación entre las autoridades competentes designadas conforme a DORA y las estructuras y autoridades establecidas conforme a la directiva propuesta. Concretamente, el intercambio de información entre las autoridades puede permitir el conocimiento intersectorial, contribuir a la prevención de los ciberataques y a su gestión eficaz, y fomentar una evaluación coherente de los riesgos de TIC en toda la Unión. Sin embargo, el BCE subraya que el intercambio de información debe tener lugar cuando se hayan establecido mecanismos claros de clasificación y de intercambio de información y, al mismo tiempo, salvaguardias adecuadas que garanticen la confidencialidad ([24]). El BCE celebra la orientación general del

([17]) Artículo 29, apartado 4, letra b), de la directiva propuesta.
([18]) Artículo 31 de DORA.
([19]) Véase el apartado 1.2 del Dictamen CON/2021/20.
([20]) Artículo 29, apartado 10, de la orientación general del Consejo sobre la directiva propuesta.
([21]) Artículo 7, apartado 1, de la directiva propuesta.
([22]) Considerando 27 de la directiva propuesta.
([23]) Artículo 14 de la directiva propuesta.
([24]) Véase el apartado 1.5 del Dictamen CON/2021/20.

Consejo sobre la directiva propuesta, que propone el intercambio periódico de la información pertinente entre las autoridades ([25]), el establecimiento de acuerdos de cooperación que especifiquen un mecanismo de intercambio de información ([26]), y la transmisión automática y directa de las notificaciones de incidentes ([27]). Sobre este particular, debe velarse por que la información que sea confidencial conforme a las disposiciones sobre secreto profesional de DORA ([28]) o a la legislación sectorial pertinente ([29]) solo pueda intercambiarse con las autoridades competentes conforme a la directiva propuesta cuando estas la necesiten para aplicar lo previsto en la directiva propuesta ([30]).

3.4 *Estrategia nacional de ciberseguridad*

3.4.1 Conforme a la directiva propuesta, cada Estado miembro debe adoptar una estrategia nacional de ciberseguridad en la que se establezcan los objetivos estratégicos y las medidas políticas y normativas adecuadas con objeto de alcanzar y mantener un elevado nivel de ciberseguridad ([31]). Según aclaran los considerandos de la directiva propuesta, los Estados miembros deben seguir incluyendo al sector financiero en sus estrategias de ciberseguridad ([32]). A título orientativo, como parte de su estrategia nacional de ciberseguridad, los Estados miembros deben adoptar medidas que aborden la ciberseguridad en la cadena de suministro de los productos y servicios de TIC que utilicen las entidades para prestar sus servicios. Por lo que respecta al sector financiero, las estrategias nacionales de ciberseguridad deben ser coherentes con el marco regulador derivado de DORA. En este sentido, el BCE considera que se necesitan más aclaraciones para garantizar la coherencia entre las estrategias nacionales de ciberseguridad y la legislación sectorial.

En un documento técnico de trabajo separado, disponible en inglés en EUR-Lex, figuran las propuestas de redacción específicas, acompañadas de explicaciones, correspondientes a los puntos de la directiva propuesta que el BCE recomienda modificar.

Hecho en Fráncfort del Meno el 11 de abril de 2022.

La Presidenta del BCE
Christine LAGARDE

([25]) Artículo 11, apartado 5, de la orientación general del Consejo sobre la directiva propuesta.
([26]) Considerando 23 *bis* de la orientación general del Consejo sobre la directiva propuesta.
([27]) Considerando 13 de la orientación general del Consejo sobre la directiva propuesta.
([28]) Artículo 49 de DORA.
([29]) Artículos 53 a 62 de la Directiva 2013/36/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativa al acceso a la actividad de las entidades de crédito y a la supervisión prudencial de las entidades de crédito, por la que se modifica la Directiva 2002/87/CE y se derogan las Directivas 2006/48/CE y 2006/49/CE (DO L 176 de 27.6.2013, p. 338).
([30]) Artículo 2, apartado 5, y artículo 11, apartado 4, de la directiva propuesta.
([31]) Artículo 5 de la directiva propuesta.
([32]) Considerando 13 de la directiva propuesta.