BUTLLETÍ OFICIAL
DEL PARLAMENT DE CATALUNYA

X legislatura
Segon període

Número 28
18 de febrer de 2013

SUMARI

NOTES

Aquesta publicació és impresa en paper ecològic (definició europea ECF), en compliment del que estableix la Resolució 124/III del Parlament, sobre la utilització del paper reciclat en el Parlament i en els departaments de la Generalitat, adoptada el 30 d'abril de 1990.

Els documents publicats en el *Butlletí Oficial del Parlament de Catalunya* (BOPC) són una reproducció fidel dels documents originals entrats al Registre. La reproducció dels textos presentats per la Secretaria de la Comissió Mixta de la Unió Europea respecta també la compaginació de l'original.

La numeració del BOPC no està necessàriament vinculada a una sola data.

ISSN: 0213-7798 · Dipòsit legal: B-20.066-1980 · Imprès a Multitext, SL
www.parlament.cat

3. TRAMITACIONS EN CURS

3.40. PROCEDIMENTS AMB RELACIÓ A LES INSTITUCIONS DE LA UNIÓ EUROPEA

3.40.02. PROCEDIMENTS DE PARTICIPACIÓ EN L'APLICACIÓ DELS PRINCIPIS DE SUBSIDIARIETAT I PROPORCIONALITAT PER LA UNIÓ EUROPEA

——— **Control del principi de subsidiarietat amb relació a la Proposta de directiva del Parlament Europeu i del Consell sobre la prevenció de la utilització del sistema financer per al blanqueig de capitals i per al finançament del terrorisme**
Tram. 295-00014/10

Text presentat
Tramesa de la Secretaria de la Comissió Mixta de la Unió Europea de l'11.02.2013
Reg. 2333 / Admissió a tràmit: Mesa del Parlament, 12.02.2013

Asunto: Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo
(Texto pertinente a efectos del EEE)
[COM(2013) 45 final] [2013/0025 (COD)]
{SWD(2013) 21 final} {SWD(2013) 22 final}

En aplicación del artículo 6.1 de la Ley 8/1994, de 19 de mayo, la Comisión Mixta para la Unión Europea remite a su Parlamento, por medio del presente correo electrónico, la iniciativa legislativa de la Unión Europea que se acompaña, a efectos de su conocimiento y para que, en su caso, remita a las Cortes Generales un dictamen motivado que exponga las razones por las que considera que la referida iniciativa de la Unión Europea no se ajusta al principio de subsidiariedad.

Aprovecho la ocasión para recordarle que, de conformidad con el artículo 6.2 de la mencionada Ley 8/1994, el dictamen motivado que, en su caso, apruebe su Institución debería ser recibido por las Cortes Generales en el plazo de cuatro semanas a partir de la remisión de la iniciativa legislativa europea.

Con el fin de agilizar la transmisión de los documentos en relación con este procedimiento de control del principio de subsidiariedad, le informo que se ha habilitado el siguiente correo electrónico de la Comisión Mixta para la Unión Europea: cmue@congreso.es

Secretaría de la Comisión Mixta para la Unión Europea

Estrasburgo, 5.2.2013
COM(2013) 45 final
2013/0025 (COD)

Propuesta de

DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo

(Texto pertinente a efectos del EEE)

{SWD(2013) 21 final}
{SWD(2013) 22 final}

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

Motivación y objetivos de la propuesta

Los principales objetivos de las medidas propuestas son fortalecer el mercado interior, reduciendo la complejidad de las operaciones transfronterizas, proteger los intereses de la sociedad de la delincuencia y los actos terroristas, preservar la prosperidad económica de la Unión Europea, ofreciendo un entorno empresarial eficiente, y contribuir a la estabilidad financiera, protegiendo la solidez, el correcto funcionamiento y la integridad del sistema financiero.

Estos objetivos se lograrán garantizando la coherencia entre el enfoque adoptado por la UE y el enfoque internacional, garantizando la coherencia entre las normas nacionales, así como la flexibilidad a la hora de aplicarlas, y velando por que estas normas se centren en los riesgos y se adapten para responder a las nuevas amenazas que vayan surgiendo.

Por otro lado, la presente propuesta incorpora y deroga la Directiva 2006/70/CE de la Comisión, de 1 de agosto de 2006, por la que se establecen disposiciones de aplicación de la Directiva 2005/60/CE[1], lo que mejorará la comprensión y accesibilidad del marco legislativo relativo a la lucha contra el blanqueo de capitales para todas las partes interesadas.

Como complemento de la presente propuesta, la Comisión se propone reforzar las medidas represivas de la UE contra el blanqueo de capitales. En consecuencia, en 2013 se prevé proponer la armonización de las disposiciones de Derecho penal aplicables a este delito sobre la base del artículo 83, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE)[2].

Contexto general

La supresión de los obstáculos en el mercado interior no solo facilita el establecimiento o el desarrollo en toda la UE de empresas que operan lícitamente, sino que también puede ofrecer mayores oportunidades para el blanqueo de capitales y la financiación del terrorismo. Los delincuentes implicados en actividades de blanqueo de capitales pueden, por tanto, intentar ocultar o encubrir la verdadera naturaleza, origen o propiedad de estos activos y transformarlos en productos aparentemente legítimos. Por otra parte, el terrorismo puede financiarse mediante actividades tanto legítimas como delictivas, ya que las organizaciones terroristas desarrollan actividades generadoras de ingresos que, en sí mismas, pueden ser, o al menos parecer, legítimas. El blanqueo de capitales y la financiación del terrorismo representan así un riesgo importante para la integridad, el correcto funcionamiento, la reputación y la estabilidad del sistema financiero, con consecuencias potencialmente devastadoras para la sociedad en general.

Se ha adoptado legislación europea para proteger el funcionamiento adecuado del sistema financiero y del mercado interior. No obstante, la naturaleza variable de las amenazas que plantea el blanqueo de capitales y la financiación del terrorismo, propiciada por la evolución constante de la tecnología y de los medios a disposición de los delincuentes, exige una adaptación permanente del marco jurídico para responder a estas amenazas.

A nivel de la UE, la Directiva 2005/60/CE, de 26 de octubre de 2005, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo[3] (en lo sucesivo denominada «tercera Directiva contra el blanqueo de capitales»), establece el marco destinado a proteger la solidez, integridad y estabilidad de las entidades financieras y de crédito, así como la confianza en el sistema financiero en su conjunto, frente a estos riesgos. Las disposiciones de la UE se basan en gran medida en las normas internacionales adoptadas por el Grupo de Acción Financiera Internacional (GAFI). Además, como la Directiva no pretende ir más allá de una armonización mínima, esas disposiciones se completan con las adoptadas a nivel nacional.

A nivel internacional, el GAFI ha emprendido una revisión a fondo de sus normas y en febrero de 2012 adoptó un nuevo conjunto de Recomendaciones.

En paralelo al proceso internacional, la Comisión Europea ha acometido su propia revisión del marco normativo europeo. La revisión de la Directiva en este momento viene a complementar las Recomendaciones revisadas del GAFI, que, en sí mismas, representan un refuerzo sustancial del marco de la lucha contra el blanqueo de capitales y la financiación del terrorismo. La propia Directiva refuerza elementos de las Recomendaciones revisadas, en particular en lo que respecta al ámbito de aplicación (al incluir a los proveedores de servicios de juegos de azar y a las personas que negocian con bienes de un valor superior a 7 500 EUR), a la información sobre la titularidad real (que deberá facilitarse a las entidades obligadas y a las autoridades competentes) y a las sanciones. La revisión tiene en cuenta la necesidad de aumentar la eficacia de las medidas contra el blanqueo de capitales adaptando el marco jurídico, a fin de velar por que se realicen evaluaciones de riesgos al nivel adecuado y con el grado necesario de flexibilidad para adaptarse a las distintas situaciones y agentes. En consecuencia, al tiempo que fija un nivel elevado de normas comunes, la Directiva impone a los Estados miembros, a las autoridades de supervisión y a las entidades obligadas el deber de evaluar los riesgos y adoptar medidas de atenuación adecuadas y proporcionadas a los riesgos. La Directiva es, por tanto, menos detallada en cuanto a las medidas concretas que deben adoptarse.

Disposiciones vigentes en este ámbito

Se han adoptado diversos instrumentos jurídicos para garantizar un marco eficaz contra el blanqueo de capitales y la financiación del terrorismo a nivel de la UE. Los más importantes son los siguientes:

– la tercera Directiva contra el blanqueo de capitales, que abarca la mayoría de las cuarenta Recomendaciones del GAFI y algunas de las nueve Recomendaciones Especiales (RE) del GAFI;

1 DO L 214 de 4.8.2006, p. 29.
2 http://ec.europa.eu/governance/impact/planned_ia/docs/2013_home_006_money_laundering_en.pdf
3 DO L 309 de 25.11.2005, p. 15.

– el Reglamento (CE) nº 1781/2006, de 15 de noviembre de 2006, relativo a la información sobre los ordenantes que acompaña a las transferencias de fondos[4], que aplica la RE VII del GAFI sobre las transferencias electrónicas;

– el Reglamento (CE) nº 1889/2005, de 26 de octubre de 2005, relativo a los controles de la entrada o salida de dinero efectivo de la Comunidad[5], que aplica la RE IX del GAFI sobre transportes de fondos;

– la Directiva 2007/64/CE, de 13 de diciembre de 2007, sobre servicios de pago en el mercado interior[6] (Directiva sobre servicios de pago), que, en combinación con la tercera Directiva contra el blanqueo de capitales, aplica la RE VI del GAFI sobre sistemas alternativos de envíos de fondos;

– el Reglamento (CE) nº 2580/2001, de 27 de diciembre de 2001, sobre medidas restrictivas específicas dirigidas a determinadas personas y entidades con el fin de luchar contra el terrorismo[7], que, junto con el Reglamento (CE) nº 881/2002, de 27 de mayo de 2002[8], que impone las sanciones de las Naciones Unidas contra Al Qaida y los talibanes, aplica parte de la RE III del GAFI sobre congelación de activos terroristas.

Coherencia con otras políticas y objetivos de la Unión

La adaptación propuesta del marco normativo contra el blanqueo de capitales y la financiación del terrorismo es plenamente coherente con las políticas de la UE en otros ámbitos. En particular:

– El Programa de Estocolmo[9], que aspira a conseguir una Europa abierta y segura que sirva y proteja al ciudadano, insta a los Estados miembros y a la Comisión a fomentar el intercambio de información entre las unidades de información financiera (UIF) en su lucha contra el blanqueo de capitales.

– La Estrategia de Seguridad Interior de la UE[10], que señala los retos más urgentes para la seguridad de la UE en los próximos años y propone cinco objetivos estratégicos y medidas específicas para el período 2011-2014 que contribuirán a mejorar la seguridad de la UE, entre ellas la lucha contra el blanqueo de capitales y la prevención del terrorismo. Se reconoce expresamente la necesidad de actualizar el marco normativo de la UE contra el blanqueo de capitales y la financiación del terrorismo con objeto de aumentar la transparencia de las personas jurídicas y las estructuras jurídicas.

– Debido a la posibilidad de utilizar abusivamente las nuevas tecnologías para encubrir transacciones y ocultar la identidad, es importante que los Estados miembros estén al tanto de la evolución tecnológica y fomenten el uso de la identificación electrónica, la firma electrónica y los servicios de confianza para las transacciones electrónicas, de conformidad con la propuesta de Reglamento relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior[11], presentada por la Comisión.

– La propuesta sobre el embargo preventivo y el decomiso de los productos de la delincuencia en la Unión Europea[12], adoptada por la Comisión Europea en marzo de 2012 y cuyo objetivo es garantizar que los Estados miembros dispongan de un sistema eficaz para embargar preventivamente, administrar y decomisar los activos de origen delictivo, con el respaldo de la estructura institucional y los recursos financieros y humanos necesarios;

– En lo relativo a la protección de datos, las precisiones propuestas respecto a la tercera Directiva contra el blanqueo de capitales, que están plenamente en consonancia con el enfoque seguido por la Comisión en sus recientes propuestas en materia de protección de datos[13], en las que, en virtud de una disposición específica[14], el Derecho nacional o de la UE podrá limitar el ámbito de aplicación de las obligaciones y derechos previstos en el proyecto de Reglamento sobre la base de una serie de motivos específicos, entre ellos la prevención, la investigación, la detección y el enjuiciamiento de delitos penales.

4 DO L 345 de 8.12.2006, p. 1.
5 DO L 309 de 25.11.2005, p. 9.
6 DO L 319 de 5.12.2007, p. 1.
7 DO L 344 de 28.12.2001, p. 70.
8 DO L 139 de 29.5.2002, p. 9.
9 DO C 115 de 4.5.2010, p. 1.
10 Comunicación de la Comisión al Parlamento Europeo y al Consejo titulada «La Estrategia de Seguridad Interior de la UE en acción: cinco medidas para una Europa más segura» [COM(2010) 673 final].
11 COM(2012) 238/2.
12 Propuesta de Directiva del Parlamento Europeo y del Consejo sobre el embargo preventivo y el decomiso de los productos de la delincuencia en la Unión Europea [COM(2012) 85 final].
13 Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos [COM(2012) 10 final] y propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) [COM(2012) 11 final].
14 Artículo 21 del Reglamento general de protección de datos.

– En cuanto a las sanciones, la propuesta de introducir un conjunto de normas mínimas basadas en principios para reforzar las sanciones administrativas, que es plenamente coherente con la política de la Comisión expuesta en su Comunicación «Regímenes sancionadores más rigurosos en el sector de servicios financieros»[15].

– Con respecto a la inclusión financiera, se ha reconocido que la aplicación de un enfoque excesivamente prudente en la lucha contra el blanqueo de capitales y la financiación del terrorismo podría tener como consecuencia no deseada excluir del sistema financiero a empresas y consumidores legítimos. Se han realizado estudios sobre esta cuestión a nivel internacional[16] para asesorar a los países y sus entidades financieras a la hora de diseñar medidas de lucha contra el blanqueo de capitales y la financiación del terrorismo que cumplan el objetivo nacional de inclusión financiera, sin comprometer las medidas que existen a fin de combatir la delincuencia. A nivel de la UE, se está examinando actualmente la cuestión de la inclusión financiera en el marco de los trabajos sobre un paquete de medidas relativas a las cuentas bancarias.

– Con respecto a la cooperación con personas o autoridades (incluidos tribunales y organismos administrativos) que participen en labores de evaluación o recaudación de impuestos o cualquier otro gravamen público, en los procedimientos declarativos o ejecutivos relativos a dichos impuestos, o en la resolución de los recursos relativos a los mismos, la propuesta es coherente con el enfoque seguido a nivel internacional en la lucha contra el fraude y la evasión fiscal[17] al incluir una referencia específica a los delitos fiscales entre los delitos graves que pueden considerarse delitos principales de blanqueo de capitales. La mejora de los procedimientos de diligencia debida con respecto al cliente a efectos de la lucha contra el blanqueo de capitales contribuirá también a la lucha contra el fraude fiscal y la evasión fiscal.

2. RESULTADOS DE LAS CONSULTAS CON LAS PARTES INTERESADAS Y DE LAS EVALUACIONES DE IMPACTO

Consulta con las partes interesadas

En abril de 2012 la Comisión aprobó un informe sobre la aplicación de la tercera Directiva contra el blanqueo de capitales y solicitó comentarios de todas las partes interesadas. El informe se centraba en una serie de temas clave concretos (por ejemplo, la aplicación de un enfoque basado en el riesgo, la ampliación del ámbito de aplicación del marco vigente, la adaptación del enfoque en materia de diligencia debida con respecto al cliente, la aclaración de las obligaciones de información y las competencias de supervisión, el refuerzo de la cooperación entre las UIF, etc.), esenciales para la revisión de dicha Directiva.

La Comisión recibió 77 contribuciones de una amplia variedad de partes interesadas (autoridades públicas, sociedad civil, federaciones de empresas y empresas de varios ámbitos, entre ellos los servicios financieros, el sector de los juegos de azar, las profesiones liberales, el sector inmobiliario y los proveedores de servicios a sociedades y fideicomisos). Al margen de la consulta, se recibieron otras observaciones, documentos de opinión y contribuciones.

Los resultados globales de la consulta[18] vienen a confirmar en general las cuestiones y problemas señalados en el informe de la Comisión y muestran un amplio respaldo a la propuesta de adaptación a las normas revisadas del GAFI y la clarificación de determinados aspectos (por ejemplo, la protección de datos y las modalidades de aplicación de las normas en situaciones transfronterizas).

Utilización de asesoramiento técnico

Se han realizado esfuerzos sustanciales para obtener datos documentales en este ámbito y garantizar la plena participación de las distintas partes interesadas.

En particular, durante 2010, la consultoría externa Deloitte realizó un estudio[19] en nombre de la Comisión en el que analiza la aplicación de la tercera Directiva contra el blanqueo de capitales.

Evaluación de impacto

La Comisión ha llevado a cabo una evaluación de impacto[20], en la que ha analizado las posibles consecuencias del blanqueo de capitales y la financiación del terrorismo. En particular, la no intervención del sistema financiero para poner coto a las actividades de blanqueo de capitales y financiación del terrorismo puede tener repercusiones

15 COM(2010) 716 final.

16 *Anti-money laundering and terrorist financing measures and Financial Inclusion*, GAFI, junio de 2011.

17 Comunicación de la Comisión en la que se presenta un «Plan de acción para reforzar la lucha contra el fraude fiscal y la evasión fiscal», aprobado por la Comisión el 6 de diciembre de 2012 [COM(2012) 722 final].

18 El resumen de las respuestas puede consultarse en: http://ec.europa.eu/internal_market/company/financial-crime/index_en.htm

19 El estudio puede consultarse en: http://ec.europa.eu/internal_market/company/financial-crime/index_en.htm

20 La evaluación de impacto puede consultarse en: http://ec.europa.eu/internal_market/company/financial-crime/index_en.htm

económicas negativas (derivadas de las perturbaciones de los flujos de capitales internacionales, la disminución de la inversión y el menor crecimiento económico) y desestabilizar los mercados financieros (como consecuencia de la reticencia de otros intermediarios financieros a entablar relaciones comerciales, la pérdida de reputación, el deterioro de la confianza y riesgos prudenciales).

Se examinaron los siguientes problemas:

– la aplicación divergente de las actuales normas de la UE en los Estados miembros, lo que va en detrimento de la seguridad jurídica;

– las deficiencias y lagunas en las normas vigentes de la UE;

– la falta de coherencia de las normas vigentes con las normas internacionales recientemente revisadas.

Para solucionarlos, deben alcanzarse los siguientes objetivos operativos:

– garantizar la coherencia entre las normas nacionales y, en su caso, la flexibilidad en su aplicación, reforzando y aclarando los requisitos actuales;

– velar por que las normas se centren en los riesgos y se adapten para responder a las nuevas amenazas, reforzando y aclarando los requisitos actuales;

– garantizar la coherencia entre el enfoque de la UE y el aplicado a nivel internacional, ampliando el ámbito de aplicación y reforzando y aclarando los requisitos actuales.

–

Según las conclusiones de la evaluación de impacto, las opciones más idóneas para mejorar la situación actual serían las siguientes:

– *Ampliación del ámbito de aplicación para incluir los juegos de azar*: ampliar el ámbito de aplicación de la Directiva más allá de los casinos para incluir el sector de los juegos de azar.

– *Umbrales aplicables al comercio de bienes*: para las operaciones en efectivo, reducir de 15 000 EUR a 7 500 EUR los umbrales a partir de los cuales las personas que comercian con bienes de elevado valor quedan incluidas en el ámbito de aplicación de la Directiva y están obligadas a aplicar procedimientos de diligencia debida con respecto al cliente.

– *Regímenes sancionadores*: introducir un conjunto de normas mínimas basadas en principios para endurecer las sanciones administrativas.

– *Comparabilidad de los datos estadísticos:* reforzar y precisar el requisito relativo a la recogida y comunicación de datos estadísticos.

– *Protección de datos:* introducir en la Directiva disposiciones para aclarar la interacción entre los requisitos aplicables a la lucha contra el blanqueo de capitales y la financiación del terrorismo y los relativos a la protección de datos.

– *Inclusión de los delitos fiscales en el ámbito de aplicación*: incluir una referencia explícita a los delitos fiscales como delito principal.

– *Disponibilidad de información sobre el titular real:* obligar a todas las sociedades a disponer de información sobre sus titulares reales.

– *Identificación del titular real:* mantener el enfoque que contempla la exigencia de identificar al titular real a partir de un umbral de propiedad del 25 %, pero aclarar a qué se refiere este «umbral del 25 %».

– *Responsabilidades de supervisión de las autoridades del país de origen y las del país de acogida en materia de lucha contra el blanqueo de capitales*: introducir nuevas normas que aclaren que las sucursales y filiales situadas en Estados miembros distintos del de la sede central aplican las normas del país de acogida en materia de blanqueo de capitales y reforzar las disposiciones de cooperación entre los supervisores del país de origen y los del país de acogida.

– *Cooperación transfronteriza entre las unidades de información financiera (UIF)*: introducir nuevos requisitos que refuercen las competencias de las UIF y la cooperación entre las mismas.

– *Evaluaciones nacionales de riesgos*: introducir para los Estados miembros la obligación de llevar a cabo una evaluación de los riesgos a nivel nacional y de tomar medidas para atenuarlos.

– *Diligencia debida con respecto al cliente*: obligar a los Estados miembros a garantizar la aplicación de procedimientos reforzados de diligencia debida en determinadas situaciones de elevado riesgo, permitiéndoles al mismo tiempo autorizar la aplicación de procedimientos simplificados en situaciones de menor riesgo.

– *Equivalencia de los regímenes de terceros países*: eliminar el proceso de «lista blanca».

– *Aplicación a la supervisión de un enfoque basado en el riesgo:* reconocer expresamente en la Directiva que la supervisión podrá modularse en función de los riesgos.

– *Tratamiento de las personas del medio político:* introducir nuevos requisitos para las personas del medio político de la UE o las que trabajan en organizaciones internacionales, aplicando medidas basadas en los riesgos.

Además, la evaluación de impacto ha analizado la incidencia de las propuestas legislativas en los derechos fundamentales. De acuerdo con la Carta de los Derechos Fundamentales, las propuestas pretenden, en particular, garantizar la protección de los datos de carácter personal (artículo 8 de la Carta) precisando las condiciones en las que estos datos podrán conservarse y transferirse. La propuestas no modificarán y, por tanto, no afectarán al derecho a la tutela judicial efectiva y a un juez imparcial (artículo 47 de la Carta), que la Directiva no vulnera, tal como confirmó el Tribunal de Justicia Europeo (asunto C-305/05). Se han tenido debidamente en cuenta el respeto de la vida privada (artículo 7), la libertad de empresa (artículo 16) y la no discriminación (artículo 21). Por último, la propuesta contribuirá indirectamente a proteger el derecho a la vida (artículo 2 de la Carta).

3. ASPECTOS JURÍDICOS DE LA PROPUESTA

Base jurídica

La presente propuesta se basa en el artículo 114 del TFUE.

Subsidiariedad y proporcionalidad

De conformidad con los principios de subsidiariedad y de proporcionalidad enunciados en el artículo 5 del Tratado de la Unión Europea, los objetivos de la propuesta no pueden ser alcanzados de manera suficiente por los Estados miembros y, por consiguiente, pueden lograrse mejor a nivel de la Unión. La propuesta no excede de lo necesario para alcanzar estos objetivos.

El considerando 2 de la tercera Directiva contra el blanqueo de capitales subraya la necesidad de disponer de medidas a escala de la UE destinadas a proteger la solidez, integridad y estabilidad de las entidades financieras y de crédito, así como la confianza en el sistema financiero en su conjunto: «A fin de evitar que los Estados miembros adopten medidas para proteger su sistema financiero que puedan ser contrarias al funcionamiento del mercado interior y a las normas del Estado de Derecho y del orden público comunitario, es necesaria una actuación comunitaria en este ámbito».

Puesto que los flujos masivos de dinero negro y la financiación del terrorismo pueden perjudicar la estabilidad y la reputación del sector financiero y poner en peligro el mercado interior, cualquier medida adoptada exclusivamente a nivel nacional podría tener efectos negativos para el mercado único de la UE: la ausencia de normas coordinadas en los Estados miembros para proteger sus sistemas financieros podría ser incompatible con el funcionamiento del mercado interior y causar su fragmentación. La actuación de la UE también se justifica por la necesidad de mantener condiciones de competencia equitativas en toda la UE: las entidades de todos los Estados miembros quedarán sujetas a un conjunto coherente de obligaciones para combatir el blanqueo de capitales y la financiación del terrorismo.

La Comisión considera que las modificaciones propuestas son proporcionadas a los objetivos. Al imponer umbrales en el ámbito de aplicación y las normas de diligencia debida con respecto al cliente, la Comisión ha tomado medidas proporcionadas para limitar, en su caso, la aplicación de la Directiva. Por otra parte, la Directiva permite que algunas medidas de carácter preventivo que deben adoptar las PYME guarden proporción con el tamaño y la naturaleza de la entidad obligada. Al mismo tiempo, al aplicar un enfoque adaptado y flexible basado en el riesgo, los Estados miembros podrán adoptar medidas y emprender actuaciones que sean necesarias para contrarrestar los riesgos a que puedan verse expuestos a nivel nacional. Estas medidas se prestan mejor a una directiva que a un reglamento plenamente armonizado, con la inclusión de procesos a nivel de la UE que garanticen una mayor coordinación y el desarrollo de enfoques supranacionales, así como una mayor armonización en ámbitos específicos para garantizar también el logro de los objetivos de la UE. Aunque aplicar un sistema eficaz de lucha contra el blanqueo de capitales y la financiación del terrorismo implica algunos costes para las entidades obligadas (costes que se han analizado en la evaluación de impacto), la Comisión considera que los beneficios asociados a la prevención de estas actividades seguirán siendo superiores a los costes.

La evaluación de las nuevas normas internacionales se iniciará en el último trimestre de 2013. Si la Comisión no proporciona rápidamente indicaciones claras sobre el enfoque que conviene seguir a nivel de la UE para su aplicación, existe el riesgo de que los Estados miembros de la UE que sean evaluados en primer lugar opten por soluciones que quizá no coincidan con el enfoque propuesto para la UE, lo que complicaría el logro de un acuerdo sobre normas comunes.

Por último, con la adopción de las normas internacionales revisadas, la Comisión y todos los Estados miembros de la UE (ya sea directamente o en su calidad de miembros del GAFI o Moneyval) se han comprometido a garantizar su aplicación.

4. REPERCUSIONES PRESUPUESTARIAS

La propuesta no tiene incidencia alguna en el presupuesto de la Unión Europea.

5. INFORMACIÓN ADICIONAL

Explicación detallada de la propuesta

Las principales modificaciones que se propone introducir en la tercera Directiva contra el blanqueo de capitales son las siguientes:

– *Ampliación del ámbito de aplicación de la Directiva*: se proponen dos cambios principales en el ámbito de aplicación:

(a) En el caso de los pagos en efectivo, el umbral a partir del cual la Directiva es aplicable a las personas que comercian con bienes de elevado valor se reduce de 15 000 EUR a 7 500 EUR. Actualmente, estas personas solo están incluidas en el ámbito de aplicación si efectúan o reciben pagos en efectivo de un importe igual o superior a 15 000 EUR. Tras haber informado los Estados miembros de que este umbral relativamente elevado estaba siendo aprovechado por los delincuentes, se propone rebajarlo hasta los 7 500 EUR. Además, la nueva propuesta exige a estas personas que apliquen procedimientos de diligencia debida con respecto al cliente cuando realicen una transacción ocasional de un importe de como mínimo 7 500 EUR, lo que supone una reducción del anterior umbral, fijado en 15 000 EUR. Tanto la definición como el umbral representan un endurecimiento de las medidas contra la utilización de estas personas con fines de blanqueo de capitales en toda la UE.

(b) El ámbito de aplicación de la Directiva incluye ahora a los «proveedores de servicios de juegos de azar» (de conformidad con la Directiva 2000/31/CE, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico, en el mercado interior[21]). En virtud de la tercera Directiva contra el blanqueo de capitales y de las Recomendaciones del GAFI, solo los casinos debían incluirse en el ámbito de la lucha contra el blanqueo de capitales y la financiación del terrorismo. Hay datos de la UE que muestran que así se deja la puerta abierta a que los delincuentes se aprovechen de otros sectores de los juegos de azar.

– *Enfoque basado en el riesgo:* la Directiva reconoce que aplicar un enfoque basado en el riesgo es una forma eficaz de identificar y atenuar los riesgos para el sistema financiero y la estabilidad económica general en el mercado interior. Las nuevas disposiciones propuestas exigen la aplicación de medidas bien fundamentadas en tres ámbitos principales; en cada uno de ellos, las medidas se completarán con una lista mínima de factores a tener en cuenta o con orientaciones elaboradas por las Autoridades Europeas de Supervisión:

(c) Los Estados miembros deberán identificar, comprender y atenuar los riesgos que afronten. Podrán complementar estas tareas con evaluaciones de riesgos realizadas a nivel supranacional (por ejemplo, por las Autoridades Europeas de Supervisión o Europol) y los resultados deberán ser compartidos con los demás Estados miembros y las entidades obligadas. Este sería el punto de partida del enfoque basado en el riesgo, y supone el reconocimiento de que una respuesta a escala de la Unión puede inspirarse en la experiencia de los Estados miembros.

(d) Las entidades obligadas que desarrollen actividades incluidas en el ámbito de aplicación de la Directiva deberán identificar, comprender y atenuar sus riesgos, así como documentar y actualizar las evaluaciones de riesgos que emprendan. Este es un elemento clave del enfoque basado en el riesgo, que permitirá a las autoridades competentes (por ejemplo, los supervisores) de los Estados miembros analizar a fondo y comprender las decisiones adoptadas por las entidades obligadas que supervisen. En última instancia, las entidades que adopten un enfoque basado en el riesgo serán plenamente responsables de las decisiones que tomen.

(e) La propuesta admite que los recursos de los supervisores puedan utilizarse para concentrarse en aquellos ámbitos en los que los riesgos de blanqueo de capitales y de financiación del terrorismo sean mayores. La aplicación de un enfoque basado en el riesgo implicará que los datos obtenidos se utilizarán para centrarse mejor en los riesgos.

[21] DO L 178 de 17.7.2000, p. 1.

– *Procedimientos reforzados y simplificados de diligencia debida con respecto al cliente:* en virtud de la propuesta, las entidades obligadas deberán tomar medidas reforzadas cuando los riesgos sean más importantes y podrán ser autorizadas a tomar medidas simplificadas cuando se haya demostrado que los riesgos son menores. Con respecto a la tercera Directiva sobre blanqueo de capitales, se consideró que las disposiciones en materia de diligencia debida simplificada eran demasiado laxas, al eximir totalmente de los requisitos de diligencia debida a determinadas categorías de clientes o transacciones. Así pues, la Directiva revisada endurece las normas relativas a la diligencia debida simplificada y no autoriza situaciones en las que puedan aplicarse exenciones. En cambio, deben justificarse en función del riesgo las decisiones sobre cuándo y cómo aplicar procedimientos simplificados, mientras que se indican los requisitos mínimos en cuanto a los factores a tener en cuenta. En uno de los supuestos en los que es obligatorio aplicar procedimientos reforzados, a saber, en el caso de las personas del medio político, la Directiva incluye también ahora a las personas del medio político que desempeñan funciones públicas importantes por encargo de un Estado miembro, así como a las que trabajan para organizaciones internacionales.

– *Información sobre el titular real:* la Directiva revisada propone nuevas medidas para hacer más clara y accesible la información sobre la titularidad real. Exige a las personas jurídicas disponer de información sobre sus propios titulares reales. Esta información debe ponerse a disposición tanto de las autoridades competentes como de las entidades obligadas. En cuanto a las estructuras jurídicas, los fideicomisarios deben declarar su condición cuando se conviertan en clientes y debe ponerse igualmente a disposición de las autoridades competentes y de las entidades obligadas información sobre la titularidad real.

– *Equivalencia de terceros países:* la Directiva revisada elimina las disposiciones relativas a la equivalencia «positiva», habida cuenta de que el régimen de diligencia debida con respecto al cliente se basa en mayor medida en los riesgos y de que el uso de exenciones por motivo de factores puramente geográficos es menos relevante. En virtud de lo dispuesto en la tercera Directiva contra el blanqueo de capitales, debía adoptarse una decisión sobre si los sistemas de lucha contra el blanqueo de capitales y la financiación del terrorismo existentes en terceros países eran «equivalentes» a los de la UE. Esta información se utilizaba entonces para autorizar exenciones a determinados aspectos de la diligencia debida con respecto al cliente.

– *Sanciones administrativas:* en consonancia con la política de la Comisión de armonizar las sanciones administrativas, la Directiva revisada contiene una serie de sanciones cuya aplicación deben garantizar los Estados miembros en caso de que se incumplan sistemáticamente los principales requisitos de la Directiva, a saber, la diligencia debida con respecto al cliente, la conservación de documentos, la notificación de las transacciones sospechosas y los controles internos.

– *Unidades de información financiera:* la propuesta incorpora lo dispuesto en la Decisión 2000/642/JAI del Consejo, de 17 de octubre de 2000, relativa a las disposiciones de cooperación entre las unidades de información financiera de los Estados miembros para el intercambio de información, y amplía y refuerza la cooperación.

– *Autoridades Europeas de Supervisión (AES):* la propuesta prevé varios ámbitos de intervención de las AES. En particular, la ABE, la AESPJ y la AEVM deberán realizar una evaluación y emitir un dictamen sobre los riesgos de blanqueo de capitales y financiación del terrorismo a que se enfrenta la UE. Además, la mayor importancia que se otorga al enfoque basado en el riesgo obliga a asesorar en mayor medida a los Estados miembros y las entidades financieras sobre los factores que han de tenerse en cuenta para aplicar procedimientos simplificados o reforzados de diligencia debida con respecto al cliente y sobre cuándo aplicar a la supervisión un enfoque basado en el riesgo. Por otro lado, se ha encomendado a las AES la tarea de elaborar normas técnicas de regulación sobre determinadas cuestiones en las que las entidades financieras deberán adaptar sus controles internos para hacer frente a situaciones específicas.

– *Protección de datos*: en la propuesta se refleja la necesidad de alcanzar un equilibrio entre, por un lado, el establecimiento de sistemas y controles sólidos y medidas preventivas contra el blanqueo de capitales y la financiación del terrorismo, y, por otro, la protección de los derechos de los interesados.

– *Medidas de transposición:* Debido a la complejidad y al alcance de la propuesta, los Estados miembros deben transmitir un cuadro de correspondencias entre las disposiciones de su legislación nacional y las de la Directiva.

Espacio Económico Europeo

La propuesta es pertinente para los países del EEE.

2013/0025 (COD)

Propuesta de

DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo

(Texto pertinente a efectos del EEE)

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, su artículo 114,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de acto legislativo a los parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo[22],

Visto el dictamen del Banco Central Europeo[23],

Previa consulta al Supervisor Europeo de Protección de Datos[24],

De conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

(1) Los flujos masivos de dinero negro pueden dañar la estabilidad y la reputación del sector financiero y poner en peligro el mercado único, y el terrorismo sacude los cimientos mismos de nuestra sociedad. Unida al planteamiento basado en el Derecho penal, una actuación preventiva a través del sistema financiero puede surtir resultados.

(2) La solidez, integridad y estabilidad de las entidades financieras y de crédito, así como la confianza en el sistema financiero en su conjunto, podrían verse en grave peligro debido a los esfuerzos de los delincuentes y sus cómplices, ya sea por encubrir el origen de los productos del delito, ya por canalizar el producto de actividades legítimas o ilegítimas a fines terroristas. Si no se adoptan medidas de coordinación en el ámbito de la Unión, los blanqueadores de capitales y los financiadores del terrorismo podrían aprovechar la libre circulación de capitales y la libre prestación de servicios financieros que trae consigo un espacio financiero integrado para facilitar sus actividades delictivas.

(3) La propuesta actual es la cuarta Directiva para responder a la amenaza del blanqueo de capitales. La Directiva 91/308/CEE del Consejo, de 10 de junio de 1991, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales[25], definía el blanqueo de capitales en términos de delitos relacionados con el tráfico de estupefacientes e imponía obligaciones exclusivamente al sector financiero. La Directiva 2001/97/CE del Parlamento Europeo y del Consejo, de 4 de diciembre de 2001, por la que se modifica la Directiva 91/308/CEE del Consejo[26], amplió el ámbito de aplicación, tanto desde el punto de vista de los delitos cubiertos como de las profesiones y actividades reguladas. En junio de 2003, el Grupo de Acción Financiera Internacional (en lo sucesivo denominado «GAFI») revisó sus Recomendaciones para incluir la financiación del terrorismo e introdujo requisitos más detallados en lo que respecta a la identificación y verificación de la identidad de los clientes y a las situaciones en las cuales el mayor riesgo de blanqueo de capitales puede justificar medidas más estrictas, así como aquellas otras en las que un menor riesgo puede justificar controles menos rigurosos. Estos cambios se reflejaron en la Directiva 2005/60/CE del Parlamento Europeo y del Consejo, de 26 de octubre de 2005, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y la financiación del terrorismo[27], y la Directiva 2006/70/CE de la Comisión, de 1 de agosto de 2006, por la que se establecen disposiciones de aplicación de la Directiva 2005/60/CE del Parlamento Europeo y del Consejo en lo relativo a la definición de personas del medio político y los criterios técnicos aplicables en los procedimientos simplificados de diligencia debida con

22 DO C de , p. .
23 DO C de , p. .
24 DO C de , p. .
25 DO L 166 de 28.6.1991, p. 77.
26 DO L 344 de 28.12.2001, p. 76.
27 DO L 309 de 25.11.2005, p. 15.

respecto al cliente así como en lo que atañe a la exención por razones de actividad financiera ocasional o muy limitada[28].

(4) El blanqueo de capitales y la financiación del terrorismo se efectúan, con frecuencia, en un contexto internacional. Las medidas adoptadas únicamente en el ámbito nacional o incluso a nivel de la Unión Europea, sin coordinación ni cooperación internacionales, tendrían efectos muy limitados. Toda medida adoptada por la Unión Europea a este respecto debe ser compatible con las que se emprendan en otros foros internacionales. En particular, la actuación de la Unión Europea debe seguir atendiendo a las Recomendaciones del GAFI, principal organismo internacional en la lucha contra el blanqueo de capitales y la financiación del terrorismo. Con vistas a reforzar la eficacia de la lucha contra el blanqueo de capitales y la financiación del terrorismo, las Directivas 2005/60/CE y 2006/70/CE deben adaptarse a las nuevas Recomendaciones del GAFI adoptadas y ampliadas en febrero de 2012.

(5) Por otra parte, la utilización fraudulenta del sistema financiero a fin de canalizar el producto de actividades delictivas o incluso de actividades lícitas con fines terroristas plantea riesgos evidentes para la integridad, el correcto funcionamiento, la reputación y la estabilidad del sistema financiero. Por consiguiente, las medidas preventivas de la presente Directiva deben ampliarse no solo a la manipulación de fondos procedentes de actividades delictivas, sino también a la percepción de fondos o bienes con fines terroristas.

(6) La realización de operaciones con grandes sumas en efectivo es susceptible de ser utilizada para el blanqueo de capitales y la financiación del terrorismo. A fin de mejorar la vigilancia y atenuar los riesgos que plantean los pagos en efectivo, las personas físicas o jurídicas que negocien con bienes deben quedar sujetas a lo dispuesto en la presente Directiva, siempre que efectúen o reciban pagos en efectivo de un importe igual o superior a 7 500 EUR. Los Estados miembros podrán decidir adoptar disposiciones más estrictas, incluido un umbral más bajo.

(7) Los profesionales del Derecho, tal y como hayan sido definidos por los Estados miembros, deben quedar sujetos a lo dispuesto en la presente Directiva cuando participen en operaciones financieras o empresariales, incluido el asesoramiento fiscal, en las que existe mayor riesgo de que los servicios de dichos profesionales del Derecho se empleen indebidamente a fin de blanquear el producto de actividades delictivas o financiar el terrorismo. No obstante, deben existir dispensas a la obligación de comunicación de la información obtenida antes, durante o después de un procedimiento judicial, o en el proceso de determinación de la situación jurídica de un cliente. Así pues, el asesoramiento jurídico debe seguir sujeto a la obligación de secreto profesional, salvo en caso de que el asesor letrado esté implicado en blanqueo de capitales o financiación del terrorismo, de que la finalidad del asesoramiento jurídico sea el blanqueo de capitales o la financiación del terrorismo, o de que el abogado sepa que el cliente solicita asesoramiento jurídico con fines de blanqueo de capitales o financiación del terrorismo.

(8) Servicios directamente comparables deben ser objeto de idéntico trato, cuando los que presten dichos servicios sean profesionales de los contemplados en la presente Directiva. Con el fin de garantizar el respeto de los derechos establecidos por la Carta de los Derechos Fundamentales de la Unión Europea, por lo que respecta a los auditores, contables externos y asesores fiscales que en determinados Estados miembros pueden defender o representar a sus clientes en el contexto de una acción judicial o determinar la situación jurídica de sus clientes, la información que aquellos obtengan en el ejercicio de esas funciones no debe estar sujeta a la obligación de comunicación con arreglo a la presente Directiva.

(9) Es importante destacar expresamente que los «delitos fiscales» relacionados con los impuestos directos e indirectos están incluidos en la definición de «actividad delictiva» en sentido amplio con arreglo a la presente Directiva, de conformidad con las Recomendaciones revisadas del GAFI.

(10) Es necesario identificar a toda persona física que ostente la propiedad o el control de una persona jurídica. Si bien establecer un porcentaje de participación no permitirá encontrar automáticamente al titular real, es un factor probatorio que debe tenerse en cuenta. La identificación del titular real y la comprobación de su identidad debe hacerse extensiva, en su caso, a las entidades jurídicas que posean otras entidades jurídicas, y debe remontar la cadena de propiedad hasta que se encuentre a la persona física que ostente la propiedad o el control de la persona jurídica que sea el cliente.

(11) La necesidad de información precisa y actualizada sobre el titular real es un factor clave para la localización de los delincuentes, que, de otro modo, podrían ocultar su identidad tras una estructura empresarial. Por consiguiente, los Estados miembros deben velar por que las sociedades conserven información sobre su titularidad real y pongan esta información a disposición de las autoridades competentes y las entidades obligadas. Además, los fideicomisarios deben declarar su condición a las entidades obligadas.

(12) La presente Directiva debe aplicarse igualmente a aquellas actividades de las entidades obligadas a las que es aplicable la presente Directiva que se lleven a cabo a través de internet.

[28] DO L 214 de 4.8.2006, p. 29.

(13) La utilización del sector de los juegos de azar para el blanqueo del producto de actividades delictivas es motivo de preocupación. A fin de atenuar los riesgos relacionados con este sector y garantizar la equidad entre los proveedores de servicios de juegos de azar, resulta oportuno imponer a estos la obligación de aplicar medidas de diligencia debida con respecto al cliente en cada operación de un valor igual o superior a 2 000 EUR. Los Estados miembros deben estudiar la posibilidad de aplicar este umbral a la recogida de ganancias y a las apuestas. Los proveedores de servicios de juegos de azar con locales físicos (por ejemplo, casinos y casas de apuestas) deben velar por que, si se aplican a la entrada de dichos locales, las medidas de diligencia debida con respecto al cliente permitan establecer una conexión con las transacciones realizadas por los clientes en esos locales.

(14) El riesgo de blanqueo de capitales y financiación del terrorismo no es el mismo en todos los casos. Por ello, conviene aplicar un enfoque basado en el riesgo. Este tipo de enfoque no constituye una opción excesivamente permisiva para los Estados miembros y las entidades obligadas. Implica tomar decisiones basadas en hechos para centrarse mejor en los riesgos de blanqueo de capitales y financiación del terrorismo a que se enfrenta la Unión Europea y quienes operan en ella.

(15) Es necesario cimentar el enfoque basado en el riesgo para que los Estados miembros puedan identificar, comprender y atenuar los riesgos de blanqueo de capitales y financiación del terrorismo a que se enfrentan. La importancia de aplicar un enfoque supranacional a la identificación de los riesgos ha sido reconocida a nivel internacional, y debe encomendarse a la Autoridad Europea de Supervisión (Autoridad Bancaria Europea) (en lo sucesivo, «ABE»), creada mediante el Reglamento (UE) nº 1093/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Bancaria Europea), se modifica la Decisión nº 716/2009/CE y se deroga la Decisión 2009/78/CE de la Comisión[29]; a la Autoridad Europea de Supervisión (Autoridad Europea de Seguros y Pensiones de Jubilación) (en lo sucesivo, «AESPJ»), creada mediante el Reglamento (UE) nº 1094/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Europea de Seguros y Pensiones de Jubilación), se modifica la Decisión nº 716/2009/CE y se deroga la Decisión 2009/79/CE de la Comisión[30]; y a la Autoridad Europea de Supervisión (Autoridad Europea de Valores y Mercados) (en lo sucesivo, «AEVM»), creada mediante el Reglamento (UE) nº 1095/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Europea de Valores y Mercados), se modifica la Decisión nº 716/2009/CE y se deroga la Decisión 2009/77/CE de la Comisión[31], la tarea de emitir un dictamen sobre los riesgos que afectan al sector financiero.

(16) Los resultados de la evaluación de riesgos a nivel de los Estados miembros deben, cuando proceda, ponerse a disposición de las entidades obligadas para que estas puedan identificar, comprender y atenuar sus propios riesgos.

(17) A fin de comprender mejor y atenuar los riesgos a nivel de la Unión Europea, los Estados miembros deben compartir los resultados de sus evaluaciones de riesgos con los demás Estados miembros, con la Comisión y con la ABE, la AESPJ y la AEVM, cuando proceda.

(18) Al aplicar lo dispuesto en la presente Directiva, conviene tener en cuenta las características y necesidades de las entidades obligadas de menor tamaño incluidas en su ámbito de aplicación y garantizar un tratamiento adaptado a las necesidades específicas de estas pequeñas entidades y a la naturaleza de su actividad.

(19) El riesgo en sí mismo es variable por naturaleza y los factores que intervengan, ya sean solos o combinados, pueden aumentar o reducir el riesgo potencial planteado, influyendo de esta forma en el nivel adecuado de las medidas preventivas, como las medidas de diligencia debida con respecto al cliente. Así pues, existen situaciones en las que conviene aplicar procedimientos reforzados de diligencia debida y otras en las que puede resultar oportuno aplicar procedimientos simplificados.

(20) Hay que reconocer que determinadas situaciones presentan mayor riesgo de blanqueo de capitales o de financiación del terrorismo. Si bien debe determinarse la identidad y el perfil empresarial de todos los clientes, hay casos en que son necesarios procedimientos particularmente rigurosos de identificación del cliente y comprobación de su identidad.

(21) Lo anterior se aplica de modo particular a las relaciones de negocios con personas que ocupen o hayan ocupado cargos públicos importantes, máxime cuando procedan de países donde está extendida la corrupción. Dichas relaciones pueden exponer el sector financiero a riesgos considerables, en particular jurídicos y de reputación. El esfuerzo internacional para luchar contra la corrupción también justifica la necesidad de prestar una atención especial a estos casos y de aplicar medidas reforzadas de diligencia debida con respecto al cliente a las personas que ocupen o hayan ocupado cargos públicos importantes, ya sea en su propio país o en el extranjero, y a los altos cargos de organizaciones internacionales.

29 DO L 331 de 15.12.2010, p. 12.
30 DO L 331 de 15.12.2010, p. 48.
31 DO L 331 de 15.12.2010, p. 84.

(22) La obtención de la aprobación de la dirección para establecer relaciones de negocios no debe implicar, en todos los casos, la obtención de la aprobación del consejo de administración. Deben poder otorgar esta aprobación las personas con un conocimiento suficiente de la exposición de la entidad al riesgo de blanqueo de capitales y financiación del terrorismo y con antigüedad suficiente para tomar decisiones que afecten a esta exposición.

(23) A fin de evitar la repetición de los procedimientos de identificación de clientes, que ocasionaría retrasos e ineficacia en las transacciones, es preciso, con las garantías adecuadas, autorizar la presentación a las entidades obligadas de clientes cuya identificación se haya llevado a cabo en otro lugar. En los casos en que una entidad obligada recurra a un tercero, la responsabilidad última en los procedimientos de diligencia debida con respecto al cliente sigue recayendo sobre la entidad obligada a la que es presentado el cliente. El tercero, o la persona que ha presentado al cliente, debe asimismo seguir siendo responsable en lo que atañe a todos los requisitos de la presente Directiva, incluida la obligación de comunicar las transacciones sospechosas y conservar los registros, en la medida en que mantenga una relación con el cliente al que se aplica la presente Directiva.

(24) En caso de que exista una relación de externalización o agencia, sobre una base contractual, entre entidades obligadas y personas físicas o jurídicas externas no incluidas en el ámbito de la presente Directiva, las obligaciones en materia de lucha contra el blanqueo de capitales y financiación del terrorismo para los mencionados agentes o proveedores externos como parte de las entidades obligadas solo podrán derivarse del contrato y no de la presente Directiva. La responsabilidad del cumplimiento de la presente Directiva debe seguir incumbiendo a las entidades obligadas contempladas en la misma.

(25) Todos los Estados miembros han creado, o deberían crear, unidades de información financiera (en lo sucesivo denominadas «UIF») con la misión de recoger y analizar la información que reciban con la finalidad de establecer vínculos entre transacciones sospechosas y la actividad delictiva subyacente, a fin de prevenir y luchar contra el blanqueo de capitales y la financiación del terrorismo. Las transacciones sospechosas deben comunicarse a las UIF, que deben servir de centro nacional de recepción, análisis y transmisión a las autoridades competentes de las comunicaciones de transacciones sospechosas y demás información relativa a posibles blanqueos de capitales o financiación del terrorismo. Esto no debería obligar a los Estados miembros a modificar sus actuales sistemas de comunicación en los que la labor de información corra a cargo de una fiscalía u otras autoridades de defensa de la legalidad, siempre y cuando la información se transmita a las UIF con prontitud y no filtrada para que estas puedan realizar adecuadamente sus tareas, incluida la cooperación internacional con otras UIF.

(26) Como excepción a la prohibición general de llevar a cabo transacciones sospechosas, las entidades obligadas podrán ejecutar transacciones sospechosas antes de informar a la autoridad competente cuando la no ejecución de las mismas resulte imposible o pueda comprometer el enjuiciamiento de los beneficiarios de una presunta operación de blanqueo de capitales o de financiación del terrorismo. No obstante, esta excepción ha de entenderse sin perjuicio de las obligaciones internacionales asumidas por los Estados miembros de inmovilizar inmediatamente los fondos u otros bienes de terroristas, de organizaciones terroristas y de quienes financian actividades terroristas, conforme a las correspondientes resoluciones del Consejo de Seguridad de las Naciones Unidas.

(27) Los Estados miembros deben poder designar al organismo autorregulador pertinente de las profesiones contempladas en el artículo 2, apartado 1, punto 3, letras a), b) y d), como la autoridad a la que se ha de informar en primera instancia en lugar de la UIF. De acuerdo con la jurisprudencia del Tribunal Europeo de Derechos Humanos, un sistema de notificación en primera instancia a un organismo autorregulador constituye una salvaguardia importante para la protección de los derechos fundamentales en lo que se refiere a las obligaciones de información aplicables a los abogados.

(28) En la medida en que un Estado miembro haya decidido acogerse a las excepciones previstas en el artículo 33, apartado 2, podrá permitir o exigir al organismo autorregulador representante de las personas mencionadas en ese artículo que no transmita a la UIF informaciones obtenidas de dichas personas en las condiciones establecidas en dicho artículo.

(29) Ha habido casos de empleados que, habiendo comunicado sospechas de blanqueo de capitales, han sufrido amenazas o acciones hostiles. Si bien la presente Directiva no puede interferir con los procedimientos judiciales de los Estados miembros, se trata de un aspecto crucial para la eficacia del sistema de lucha contra el blanqueo de capitales y la financiación del terrorismo. Los Estados miembros deben ser conscientes del problema y hacer todo lo posible por proteger a los empleados frente a este tipo de amenazas o acciones hostiles.

(30) La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación

de estos datos[32], incorporada al Derecho nacional, se aplica al tratamiento de los datos personales a efectos de la presente Directiva.

(31) Determinados aspectos de la aplicación de la presente Directiva implican la recogida, el análisis, la conservación y el intercambio de datos. Debe permitirse el tratamiento de datos personales a fin de cumplir con las obligaciones establecidas en la presente Directiva, en particular la aplicación de las medidas de diligencia debida con respecto al cliente y las medidas de seguimiento continuo, la investigación y la notificación de las transacciones sospechosas e inusuales, la identificación del titular real de una persona jurídica o estructura jurídica, y el intercambio de información por las autoridades competentes y las entidades financieras. Los datos personales que se recojan deben limitarse a lo estrictamente necesario para el cumplimiento de los requisitos de la presente Directiva y no tratarse ulteriormente de una manera incompatible con la Directiva 95/46/CE. En particular, debe prohibirse estrictamente el tratamiento posterior de datos de carácter personal con fines comerciales.

(32) Todos los Estados miembros reconocen que la lucha contra el blanqueo de capitales y la financiación del terrorismo constituye una cuestión importante de interés general.

(33) La presente Directiva se entiende sin perjuicio de la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, incluidas las disposiciones de la Decisión marco 2008/977/JAI.

(34) Los derechos de acceso de los interesados son aplicables a los datos personales tratados a efectos de la presente Directiva. No obstante, el acceso de los interesados a la información contenida en una notificación de transacción sospechosa podría poner en grave peligro la eficacia de la lucha contra el blanqueo de capitales y la financiación del terrorismo. Por ello puede justificarse la imposición de limitaciones a este derecho de conformidad con las normas establecidas en el artículo 13 de la Directiva 95/46/CE.

(35) Las personas que se limitan a convertir documentos en soporte papel en datos electrónicos y que actúan basándose en un contrato celebrado con una entidad de crédito o financiera no están incluidas en el ámbito de aplicación de la presente Directiva, como tampoco lo están las personas físicas o jurídicas que solo proporcionan a las entidades de crédito o financieras un sistema de mensajería u otros sistemas de apoyo para la transmisión de fondos, o sistemas de compensación y liquidación.

(36) El blanqueo de capitales y la financiación del terrorismo son problemas internacionales, por lo que deben combatirse a escala mundial. En los casos en que las entidades de crédito y entidades financieras de la Unión tengan sucursales y filiales en terceros países donde la legislación en este ámbito sea deficiente, y a fin de evitar la aplicación de normas muy diferentes en una misma entidad o grupo de entidades, estas deben aplicar normas de la Unión o, cuando la aplicación de tales normas sea imposible, notificárselo a las autoridades competentes del Estado miembro de origen.

(37) A ser posible, las entidades obligadas deben ser informadas de la utilidad y las consecuencias de sus comunicaciones sobre transacciones sospechosas. A tal fin, y para poder evaluar la eficacia de sus sistemas de lucha contra el blanqueo de capitales y la financiación del terrorismo, los Estados miembros deben conservar y perfeccionar las estadísticas al respecto. Para mejorar la calidad y la coherencia de los datos estadísticos recogidos a nivel de la Unión, la Comisión debe seguir la evolución de la situación a escala de la UE con respecto a la lucha contra el blanqueo de capitales y la financiación del terrorismo y publicar estudios periódicos.

(38) Las autoridades competentes deben cerciorarse de la competencia y honorabilidad de las personas que de hecho dirijan las actividades de las agencias de cambio, los proveedores de servicios a sociedades y fideicomisos o los proveedores de servicios de juegos de azar, así como de la competencia y honorabilidad de los titulares reales de dichas entidades. Los criterios para determinar la competencia y honorabilidad deben reflejar, como mínimo, la necesidad de proteger a tales entidades de la posibilidad de que sean utilizadas por sus directivos o sus titulares reales con fines delictivos.

(39) A la vista del carácter transnacional del blanqueo de capitales y de la financiación del terrorismo, la coordinación y la cooperación entre las UIF de la UE revisten suma importancia. Esta cooperación solo se ha abordado, por el momento, en la Decisión 2000/642/JAI del Consejo, de 17 de octubre de 2000, relativa a las disposiciones de cooperación entre las unidades de información financiera de los Estados miembros para el intercambio de información[33]. A fin de garantizar una mejor coordinación y cooperación entre las UIF y velar en particular por que las notificaciones sobre transacciones sospechosas lleguen a la UIF del Estado miembro donde puedan resultar más útiles, conviene incluir en la presente Directiva normas más detalladas, de mayor alcance y actualizadas.

---

32 DO L 281 de 23.11.1995, p. 31.

33 DO L 271 de 24.10.2000, p. 4.

(40) Mejorar el intercambio de información entre las UIF dentro de la UE reviste especial importancia para hacer frente al carácter transnacional del blanqueo de capitales y la financiación del terrorismo. Los Estados miembros deben fomentar la utilización de medios seguros para el intercambio de información, en particular la red informática descentralizada FIU.net y las técnicas que ofrece dicha red.

(41) La importancia de la lucha contra el blanqueo de capitales y la financiación del terrorismo debe llevar a los Estados miembros a establecer sanciones eficaces, proporcionadas y disuasorias de Derecho nacional en caso de incumplimiento de las disposiciones nacionales que se adopten en aplicación de la presente Directiva. Los Estados miembros disponen actualmente de una amplia gama de medidas y sanciones administrativas frente a las vulneraciones de las principales medidas preventivas. Esta diversidad puede resultar perjudicial para los esfuerzos realizados en la lucha contra el blanqueo de capitales y la financiación del terrorismo y puede fragmentar la respuesta de la Unión. Por tanto, la presente Directiva debe incluir una serie de medidas y sanciones administrativas a disposición de los Estados miembros, aplicables en caso de vulneración sistemática de los requisitos relativos a las medidas de diligencia debida con respecto al cliente, la conservación de documentos, la notificación de las transacciones sospechosas y los controles internos. Esta serie de medidas debe ser suficientemente amplia para permitir a los Estados miembros y a las autoridades competentes tener en cuenta las diferencias entre entidades obligadas, en particular entre las entidades financieras y otras entidades obligadas, por lo que se refiere a su tamaño, características y ámbitos de actividad. Al aplicar la presente Directiva, los Estados miembros deben velar por que la imposición de medidas y sanciones administrativas, con arreglo a la presente Directiva, y de sanciones penales, con arreglo al Derecho nacional, no vulnere el principio *non bis in idem*.

(42) Las normas técnicas de los servicios financieros deben garantizar una armonización coherente y una protección adecuada de los depositantes, inversores y consumidores de la Unión. Como organismos con conocimientos altamente especializados, se considera eficaz y adecuado confiar a la ABE, la AESPJ y la AEVM la elaboración de proyectos de normas técnicas de regulación que no impliquen decisiones estratégicas, para su presentación a la Comisión.

(43) La Comisión debe adoptar los proyectos de normas técnicas de regulación elaborados por la ABE, la AESPJ y la AEVM, de conformidad con el artículo 42 de la presente Directiva, por medio de actos delegados, de conformidad con el artículo 290 del Tratado de Funcionamiento de la Unión Europea y con los artículos 10 a 14 del Reglamento (UE) nº 1093/2010, el Reglamento (UE) nº 1094/2010 y el Reglamento (UE) nº 1095/2010.

(44) En aras de la claridad y la coherencia, procede fusionar y sustituir las Directivas 2005/60/CE y 2006/70/CE, habida cuenta de las considerables modificaciones necesarias.

(45) Dado que el objetivo de la presente Directiva, a saber, la protección del sistema financiero mediante la prevención, la investigación y la detección del blanqueo de capitales y la financiación del terrorismo, no puede ser alcanzado de manera suficiente por los Estados miembros, ya que las medidas individuales adoptadas por los Estados miembros para proteger su sistema financiero podrían ser contrarias al funcionamiento del mercado interior y a las normas del Estado de Derecho y de orden público de la Unión y que, por consiguiente, puede lograrse mejor, debido a la dimensión o a los efectos de la acción propuesta, a nivel de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad consagrado en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad enunciado en el artículo mencionado, la presente Directiva no excede de lo necesario para alcanzar ese objetivo.

(46) La presente Directiva respeta los derechos fundamentales y observa los principios reconocidos por la Carta de los Derechos Fundamentales de la Unión Europea, en particular el respeto de la vida privada y familiar, el derecho a la protección de los datos de carácter personal, la libertad de empresa, la prohibición de discriminación, el derecho a la tutela judicial efectiva y a un juez imparcial, y los derechos de defensa.

(47) De conformidad con el artículo 21 de la Carta de Derechos Fundamentales de la UE, que prohíbe toda discriminación por cualquier motivo, los Estados miembros deben velar por que, en lo que respecta a la evaluación de riesgos en el contexto de la diligencia debida con respecto al cliente, la presente Directiva se aplique sin discriminación.

(48) De conformidad con la Declaración política común de los Estados miembros y de la Comisión de 28 de septiembre de 2011, relativa a los documentos explicativos, los Estados miembros se han comprometido a adjuntar a la notificación de sus medidas de transposición, en aquellos casos en que esté justificado, uno o varios documentos que expliquen la relación entre los elementos de una directiva y las partes correspondientes de los instrumentos nacionales de transposición. Por lo que respecta a la presente Directiva, el legislador considera que la transmisión de tales documentos está justificada.

HAN ADOPTADO LA PRESENTE DIRECTIVA:

CAPÍTULO I

DISPOSICIONES GENERALES

SECCIÓN 1

ÁMBITO DE APLICACIÓN Y DEFINICIONES

Artículo 1

1. Los Estados miembros velarán por que el blanqueo de capitales y la financiación del terrorismo queden prohibidos.

2. A efectos de la presente Directiva, las siguientes actividades, realizadas intencionadamente, se considerarán blanqueo de capitales:

   (a) la conversión o la transferencia de bienes, a sabiendas de que dichos bienes proceden de una actividad delictiva o de la participación en ese tipo de actividad, con el propósito de ocultar o encubrir el origen ilícito de los bienes o de ayudar a personas que estén implicadas en dicha actividad a eludir las consecuencias jurídicas de su acto;

   (b) la ocultación o el encubrimiento de la naturaleza, el origen, la localización, la disposición, el movimiento o la propiedad reales de bienes o de derechos sobre esos bienes, a sabiendas de que dichos bienes proceden de una actividad delictiva o de la participación en ese tipo de actividad;

   (c) la adquisición, posesión o utilización de bienes, a sabiendas, en el momento de la recepción de los mismos, de que proceden de una actividad delictiva o de la participación en ese tipo de actividad;

   (d) la participación en alguna de las acciones mencionadas en las letras a), b) y c), la asociación para cometer ese tipo de acciones, las tentativas de perpetrarlas y el hecho de ayudar, instigar o aconsejar a alguien para realizarlas o de facilitar su ejecución.

3. Se considerará que hay blanqueo de capitales aun cuando las actividades que hayan generado los bienes que vayan a blanquearse se hayan desarrollado en el territorio de otro Estado miembro o en el de un tercer país.

4. A efectos de la presente Directiva, se entenderá por «financiación del terrorismo» el suministro o la recogida de fondos, por cualquier medio, de forma directa o indirecta, con la intención de utilizarlos o con el conocimiento de que serán utilizados, íntegramente o en parte, para la comisión de cualquiera de los delitos contemplados en los artículos 1 a 4 de la Decisión marco 2002/475/JAI del Consejo, de 13 de junio de 2002, sobre la lucha contra el terrorismo[34], modificada por la Decisión marco 2008/919/JAI del Consejo, de 28 de noviembre de 2008[35].

5. El conocimiento, la intención o la motivación que han de darse en las actividades a que se refieren los apartados 2 y 4 del presente artículo podrán establecerse basándose en elementos de hecho objetivos.

Artículo 2

1. La presente Directiva se aplicará a las siguientes entidades obligadas:

   (1) las entidades de crédito;

   (2) las entidades financieras;

   (3) las siguientes personas físicas o jurídicas que actúen en el ejercicio de su profesión:

      (a) los auditores, contables externos y asesores fiscales;

      (b) los notarios y otros profesionales independientes del Derecho cuando participen, ya actuando en nombre de su cliente y por cuenta del mismo, en cualquier transacción financiera o inmobiliaria, ya asistiendo en la concepción o realización de transacciones por cuenta de su cliente relativas a:

[34] DO L 164 de 22.6.2002, p. 3.
[35] DO L 330 de 9.12.2008, p. 21.

i) la compraventa de bienes inmuebles o entidades comerciales,

ii) la gestión de fondos, valores u otros activos pertenecientes al cliente,

iii) la apertura o gestión de cuentas bancarias, cuentas de ahorros o cuentas de valores,

iv) la organización de las aportaciones necesarias para la creación, el funcionamiento o la gestión de empresas,

v) la creación, el funcionamiento o la gestión de sociedades, fideicomisos o estructuras análogas;

(c) los proveedores de servicios a sociedades y fideicomisos que no estén ya contemplados en las letras a) o b);

(d) los agentes de la propiedad inmobiliaria, incluidas las agencias de alquiler;

(e) otras personas físicas o jurídicas que comercien con bienes únicamente en la medida en que los pagos se efectúen o se reciban al contado y por importe igual o superior a 7 500 EUR, ya se realicen en una o en varias transacciones entre las que parezca existir algún tipo de relación;

(f) los proveedores de servicios de juegos de azar.

2. Los Estados miembros podrán decidir no incluir en el ámbito de aplicación de la presente Directiva a las personas físicas o jurídicas que realicen actividades financieras con carácter ocasional o de manera muy limitada y cuando exista escaso riesgo de blanqueo de capitales o de financiación del terrorismo, a condición de que cumplan la totalidad de los requisitos siguientes:

(a) que la actividad financiera sea limitada en términos absolutos;

(b) que la actividad financiera sea limitada en lo relativo a las transacciones;

(c) que la actividad financiera no sea la actividad principal;

(d) que la actividad financiera sea secundaria y esté directamente relacionada con la actividad principal;

(e) que, con excepción de la actividad contemplada en el apartado 1, punto 3), letra e), la actividad principal no sea una de las actividades mencionadas en el apartado 1;

(f) que la actividad financiera solo se preste a los clientes de la actividad principal y no se ofrezca al público con carácter general.

El párrafo anterior no se aplicará a las personas físicas y jurídicas que participen en la actividad de envío de dinero a tenor del artículo 4, apartado 13, de la Directiva 2007/64/CE del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, sobre servicios de pago en el mercado interior, por la que se modifican las Directivas 97/7/CE, 2002/65/CE, 2005/60/CE y 2006/48/CE y por la que se deroga la Directiva 97/5/CE[36].

3. A efectos del apartado 2, letra a), los Estados miembros exigirán que el volumen de negocios total de la actividad financiera no pueda superar un umbral suficientemente bajo. Este umbral se establecerá en el ámbito nacional, atendiendo al tipo de actividad financiera.

4. A efectos del apartado 2, letra b), los Estados miembros aplicarán un umbral máximo por cliente y transacción, tanto si esta última consiste en una sola operación como si consta de varias operaciones aparentemente vinculadas. Este umbral se establecerá en el ámbito nacional, atendiendo al tipo de actividad financiera. Será suficientemente bajo para garantizar que esos tipos de transacciones sean un método poco práctico e ineficaz para el blanqueo de capitales o la financiación del terrorismo y no superará los 1 000 EUR.

5. A efectos del apartado 2, letra c), los Estados miembros exigirán que el volumen de negocios de la actividad financiera no supere el 5 % del volumen de negocios total de la persona jurídica o física de que se trate.

6. Al evaluar el riesgo de blanqueo de capitales o de financiación del terrorismo a efectos de lo dispuesto en el presente artículo, los Estados miembros prestarán especial atención a toda actividad financiera que, por su naturaleza, se considere especialmente susceptible de uso o abuso a efectos de blanqueo de capitales o financiación del terrorismo.

7. Toda decisión adoptada de conformidad con lo establecido en el presente artículo deberá motivarse. Los Estados miembros preverán la posibilidad de revocar esa decisión si cambiaran las circunstancias.

[36] DO L 319 de 5.12.2007, p. 1.

8. Los Estados miembros preverán actividades de supervisión basadas en el riesgo o adoptarán otras medidas oportunas destinadas a garantizar que la exención concedida mediante decisiones adoptadas al amparo de lo dispuesto en el presente artículo no sea utilizada abusivamente.

Artículo 3

A efectos de la presente Directiva, se entenderá por:

(1) «entidad de crédito»: toda entidad que se ajuste a la definición del artículo 4, punto 1, de la Directiva 2006/48/CE del Parlamento Europeo y del Consejo, de 14 de junio de 2006, relativa al acceso a la actividad de las entidades de crédito y a su ejercicio[37], así como toda sucursal, tal y como se define en el artículo 4, punto 3, de dicha Directiva, establecida en la Unión Europea por entidades de crédito que tengan su sede central dentro o fuera de la Unión Europea;

(2) «entidad financiera»:

(a) toda empresa distinta de una entidad de crédito que efectúe una o varias de las operaciones mencionadas en el anexo I, puntos 2 a 12 y 14 y 15, de la Directiva 2006/48/CE, incluidas las actividades de las agencias de cambio (*bureaux de change*);

(b) toda empresa de seguros debidamente autorizada con arreglo a la Directiva 2002/83/CE del Parlamento Europeo y del Consejo, de 5 de noviembre de 2002, sobre el seguro de vida[38], en la medida en que realice actividades contempladas en dicha Directiva;

(c) toda empresa de inversión tal como se define en el artículo 4, apartado 1, punto 1, de la Directiva 2004/39/CE del Parlamento Europeo y del Consejo, de 21 de abril de 2004, relativa a los mercados de instrumentos financieros[39];

(d) todo organismo de inversión colectiva que comercialice sus participaciones o acciones;

(e) los intermediarios de seguros según se definen en el artículo 2, apartado 5, de la Directiva 2002/92/CE del Parlamento Europeo y del Consejo, de 9 de diciembre de 2002, sobre la mediación en los seguros[40], con excepción de los intermediarios a que se refiere el artículo 2, apartado 7, de dicha Directiva, cuando actúen en relación con seguros de vida u otros servicios relacionados con la inversión;

(f) las sucursales, situadas en la Unión Europea, de las entidades financieras contempladas en las letras a) a e) que tengan su sede central dentro o fuera de la Unión Europea;

(3) «bienes»: todo tipo de activos, tanto materiales como inmateriales, muebles o inmuebles, tangibles o intangibles, así como los documentos o instrumentos jurídicos con independencia de su forma, incluidas la electrónica o la digital, que acrediten la propiedad de dichos activos o un derecho sobre los mismos;

(4) «actividad delictiva»: cualquier tipo de participación delictiva en la comisión de los delitos graves siguientes:

(a) los actos definidos en los artículos 1 a 4 de la Decisión marco 2002/475/JAI sobre la lucha contra el terrorismo, modificada por la Decisión marco 2008/919/JAI del Consejo, de 28 de noviembre de 2008;

(b) cualquiera de los delitos contemplados en el artículo 3, apartado 1, letra a), de la Convención de las Naciones Unidas de 1988 contra el tráfico ilícito de estupefacientes y sustancias psicotrópicas;

(c) las actividades de las organizaciones delictivas definidas en el artículo 1 de la Acción Común 98/733/JAI del Consejo, de 21 de diciembre de 1998, relativa a la tipificación penal de la participación en una organización delictiva en los Estados miembros de la Unión Europea[41];

(d) el fraude, según se define en el artículo 1, apartado 1, y el artículo 2 del Convenio relativo a la protección de los intereses financieros de las Comunidades Europeas[42], al menos en los casos graves;

(e) la corrupción;

(f) todos los delitos, incluidos los delitos fiscales relacionados con los impuestos directos e indirectos, que lleven aparejada una pena privativa de libertad o medida de seguridad de duración máxima

37 DO L 177 de 30.6.2006, p. 1.
38 DO L 345 de 19.12.2002, p. 1.
39 DO L 145 de 30.4.2004, p. 1.
40 DO L 9 de 15.1.2003, p. 3.
41 DO L 351 de 29.12.1998, p. 1.
42 DO C 316 de 27.11.1995, p. 49.

superior a un año o, en los Estados en cuyo sistema jurídico exista un umbral mínimo para los delitos, todos los delitos que lleven aparejada una pena privativa de libertad o medida de seguridad de duración mínima superior a seis meses;

(5) «titular real»: la persona o personas físicas que ostenten la propiedad o el control en último término del cliente y/o la persona física por cuenta de la cual se lleve a cabo una transacción o actividad. El titular real incluirá, como mínimo:

(a) en el caso de las personas jurídicas:

i) la persona o personas físicas que en último término ostenten la propiedad o el control de una entidad jurídica a través de la propiedad o el control, directos o indirectos, en dicha persona jurídica, de un porcentaje suficiente de acciones o derechos de voto, mediante la tenencia, en particular, de acciones al portador, exceptuando las sociedades que coticen en un mercado regulado y que estén sujetas a requisitos de información de Derecho de la Unión Europea o a normas internacionales equivalentes;

un porcentaje del 25 % más una acción acreditará la propiedad o el control a través de la tenencia de acciones y se aplicará a cada nivel de la propiedad directa e indirecta;

ii) en caso de que haya dudas de que la persona o personas identificadas en el inciso i) sean los titulares reales, la persona o personas físicas que ejerzan por otros medios el control de la gestión de una entidad jurídica;

(b) en el caso de las entidades jurídicas, como las fundaciones, y de las estructuras jurídicas, como los fideicomisos, que administren y distribuyan fondos:

i) la persona o personas físicas que ejerzan un control sobre el 25 % o más de los bienes de una entidad o una estructura jurídicas; y

ii) cuando ya se hayan designado los futuros titulares, la persona o personas físicas que sean titulares del 25 % o más de los bienes de una entidad o una estructura jurídicas; o

iii) cuando los beneficiarios de la entidad o la estructura jurídicas estén aún por designar, la categoría de personas en beneficio de la cual se ha creado o actúan principalmente la entidad o la estructura jurídicas; en el caso de los beneficiarios de fideicomisos, designados por características o por categoría, las entidades obligadas deberán obtener información suficiente sobre el beneficiario para asegurarse de que serán capaces de establecer la identidad del beneficiario en el momento del desembolso o cuando este se proponga ejercer los derechos adquiridos;

(6) «proveedores de servicios a sociedades o fideicomisos»: toda persona física o jurídica que preste con carácter profesional los siguientes servicios a terceros:

(a) constituir sociedades u otras personas jurídicas;

(b) ejercer funciones de dirección o secretaría de una sociedad, socio de una sociedad de personas o funciones similares en relación con otras personas jurídicas o disponer que otra persona ejerza dichas funciones;

(c) facilitar un domicilio social o una dirección comercial, postal, administrativa y otros servicios afines a una sociedad, una sociedad de personas o cualquier otra persona o estructura jurídicas;

(d) ejercer funciones de fideicomisario en un fideicomiso explícito o estructura jurídica similar o disponer que otra persona ejerza dichas funciones;

(e) ejercer funciones de accionista nominal por cuenta de otra persona, exceptuando las sociedades que coticen en un mercado regulado y estén sujetas a requisitos de información conformes con el Derecho de la Unión Europea o a normas internacionales equivalentes, o disponer que otra persona ejerza dichas funciones;

(7) (a) «personas del medio político extranjeras»: personas físicas que desempeñen o hayan desempeñado funciones públicas importantes por encargo de un tercer país;

(b) «personas del medio político de la UE»: personas físicas que desempeñen o hayan desempeñado funciones públicas importantes por encargo de un Estado miembro;

(c) «personas físicas que desempeñen o hayan desempeñado funciones importantes en una organización internacional»: los directores, directores adjuntos y los miembros del consejo de administración, o función equivalente, de una organización internacional;

(d) se entenderá por «personas físicas que desempeñen o hayan desempeñado funciones públicas importantes»:

i) jefes de Estado, jefes de Gobierno, ministros, subsecretarios o secretarios de Estado;

ii) parlamentarios;

iii) miembros de tribunales supremos, tribunales constitucionales u otras altas instancias judiciales cuyas decisiones no admitan normalmente recurso, salvo en circunstancias excepcionales;

iv) miembros de tribunales de cuentas o de los consejos de bancos centrales;

v) embajadores, encargados de negocios y altos funcionarios de las fuerzas armadas;

vi) miembros de los órganos administrativos, de gestión o de supervisión de empresas de propiedad estatal.

Ninguna de las categorías establecidas en los incisos i) a vi) comprenderá funcionarios de niveles intermedios o inferiores;

(e) se entenderá por «familiares»:

i) el cónyuge;

ii) toda pareja que sea asimilable al cónyuge;

iii) los hijos y sus cónyuges o personas asimilables a cónyuges;

iv) los padres;

(f) se entenderá por «personas reconocidas como allegados»:

i) toda persona física de la que sea notorio que ostenta la propiedad económica de una entidad jurídica u otra estructura jurídica conjuntamente con alguna de las personas mencionadas en el punto 7, letras a) a d), o mantiene otro tipo de relaciones empresariales estrechas con las mismas;

ii) toda persona física que ostente la propiedad económica exclusiva de una entidad jurídica u otra estructura jurídica que notoriamente se haya constituido en beneficio de la persona a que se refiere el punto 7, letras a) a d);

(8) «dirección»: los funcionarios o empleados que tengan un conocimiento suficiente de la exposición de la entidad al riesgo de blanqueo de capitales y financiación del terrorismo, así como antigüedad suficiente para tomar decisiones que afecten a la exposición al riesgo, sin que sea necesaria, en todos los casos, la implicación de un miembro del consejo de administración;

(9) «relación de negocios»: relación empresarial, profesional o comercial vinculada a la actividad profesional de las entidades obligadas y que, en el momento en el que se establece el contacto, se prevea que tenga una cierta duración;

(10) «servicios de juegos de azar»: todo servicio que implique apuestas de valor monetario en juegos de azar, incluidos aquellos con un componente de habilidad como las loterías, los juegos de casino, el póquer y las apuestas, y que se preste en una ubicación física, o por cualquier medio a distancia, por medios electrónicos o mediante cualquier otra tecnología que facilite la comunicación, y a petición individual del destinatario del servicio;

(11) «grupo»: lo definido en el artículo 2, punto 12, de la Directiva 2002/87/CE del Parlamento Europeo y del Consejo, de 16 de diciembre de 2002, relativa a la supervisión adicional de las entidades de crédito, empresas de seguros y empresas de inversión de un conglomerado financiero[43].

Artículo 4

1. Los Estados miembros velarán por hacer extensivas, total o parcialmente, las disposiciones de la presente Directiva a aquellas profesiones y categorías de empresas distintas de las entidades obligadas contempladas en el artículo 2, apartado 1, que ejerzan actividades particularmente susceptibles de ser utilizadas para el blanqueo de capitales o la financiación del terrorismo.

2. En caso de que un Estado miembro decida hacer extensivas las disposiciones de la presente Directiva a profesiones y categorías de empresas distintas de las que se mencionan en el artículo 2, apartado 1, deberá informar de ello a la Comisión.

43 DO L 35 de 11.2.2003, p. 1.

Artículo 5

Los Estados miembros podrán adoptar o mantener en el ámbito regulado por la presente Directiva disposiciones más estrictas para impedir el blanqueo de capitales y la financiación del terrorismo.

SECCIÓN 2

EVALUACIÓN DE RIESGOS

Artículo 6

1. La Autoridad Bancaria Europea (en lo sucesivo, «la ABE»), la Autoridad Europea de Seguros y Pensiones de Jubilación (en lo sucesivo, «la AESPJ») y la Autoridad Europea de Valores y Mercados (en lo sucesivo, «la AEVM») emitirán un dictamen conjunto sobre los riesgos de blanqueo de capitales y financiación del terrorismo que afectan al mercado interior.

   El dictamen se emitirá en un plazo de dos años a partir de la fecha de entrada en vigor de la presente Directiva.

2. La Comisión hará público el dictamen para ayudar a los Estados miembros y las entidades obligadas a identificar, gestionar y atenuar los riesgos de blanqueo de capitales y financiación del terrorismo.

Artículo 7

1. Cada Estado miembro adoptará medidas adecuadas para identificar, evaluar, comprender y atenuar los riesgos de blanqueo de capitales y financiación del terrorismo que le afecten y mantendrá la evaluación actualizada.

2. Cada Estado miembro designará a una autoridad encargada de coordinar la respuesta nacional a los riesgos contemplados en el apartado 1. La identidad de dicha autoridad se notificará a la Comisión, a la ABE, la AESPJ y la AEVM y a los demás Estados miembros.

3. Al llevar a cabo la evaluación contemplada en el apartado 1, los Estados miembros podrán utilizar el dictamen previsto en el artículo 6, apartado 1.

4. Cada Estado miembro llevará a cabo la evaluación contemplada en el apartado 1 y:

   (a) la utilizará para mejorar la lucha contra el blanqueo de capitales y la financiación del terrorismo, en particular determinando todos los ámbitos en los que las entidades obligadas deberán aplicar medidas reforzadas y, en su caso, especificando las medidas que hayan de adoptarse;

   (b) se servirá de ella como ayuda en la asignación y priorización de los recursos destinados a la lucha contra el blanqueo de capitales y la financiación del terrorismo;

   (c) pondrá información adecuada a disposición de las entidades obligadas para que lleven a cabo sus propias evaluaciones de riesgo de blanqueo de capitales y financiación del terrorismo.

5. Los Estados miembros pondrán los resultados de sus evaluaciones de riesgos a disposición de los demás Estados miembros, la Comisión, la ABE, la AESPJ y la AEVM, previa solicitud.

Artículo 8

1. Los Estados miembros velarán por que las entidades obligadas adopten medidas adecuadas para identificar y evaluar sus riesgos de blanqueo de capitales y financiación del terrorismo, teniendo en cuenta factores de riesgo, entre ellos clientes, países o zonas geográficas, productos, servicios, operaciones o canales de distribución. Estas medidas deberán guardar proporción con la naturaleza y el tamaño de las entidades.

2. Las evaluaciones contempladas en el apartado 1 deberán estar documentadas, mantenerse actualizadas y ponerse a disposición de las autoridades competentes y de los organismos autorreguladores.

3. Los Estados miembros velarán por que las entidades obligadas dispongan de políticas, controles y procedimientos para atenuar y gestionar eficazmente los riesgos de blanqueo de capitales y financiación del terrorismo identificados a nivel de la Unión, de los Estados miembros y de las entidades obligadas. Estas políticas, controles y procedimientos deberán guardar proporción con la naturaleza y el tamaño de las entidades.

4. Las políticas y procedimientos contemplados en el apartado 3 deberán incluir, como mínimo:

(a) la elaboración de políticas, procedimientos y controles internos, en particular en materia de diligencia debida con respecto al cliente, notificación, conservación de datos, control interno, gestión del cumplimiento (incluido, cuando resulte apropiado debido al tamaño y la naturaleza de la empresa, el nombramiento de un responsable del cumplimiento a nivel de dirección) y escrutinio de los empleados;

(b) cuando proceda habida cuenta del tamaño y la naturaleza de la empresa, una función de auditoría independiente para examinar las políticas, procedimientos y controles internos contemplados en la letra a).

5. Los Estados miembros exigirán a las entidades obligadas que obtengan la aprobación de la dirección para las políticas y procedimientos que establezcan, y supervisarán y reforzarán, en su caso, las medidas adoptadas.

CAPÍTULO II

DILIGENCIA DEBIDA CON RESPECTO AL CLIENTE

SECCIÓN 1

DISPOSICIONES GENERALES

Artículo 9

Los Estados miembros prohibirán a sus entidades de crédito y financieras mantener cuentas anónimas o libretas de ahorro anónimas. Los Estados miembros exigirán, sin excepciones de ningún tipo, que los actuales titulares y beneficiarios de cuentas anónimas o libretas de ahorro anónimas queden sujetos cuanto antes a las medidas de diligencia debida con respecto al cliente y, en cualquier caso, antes de que se haga uso alguno de dichas cuentas o libretas de ahorro.

Artículo 10

Los Estados miembros velarán por que las entidades obligadas apliquen medidas de diligencia debida con respecto al cliente en los siguientes casos:

(a) cuando establezcan una relación de negocios;

(b) cuando efectúen transacciones ocasionales por un valor igual o superior a 15 000 EUR, ya se lleven estas a cabo en una o en varias operaciones entre las que parezca existir algún tipo de relación;

(c) en el caso de las personas físicas o jurídicas que comercien con bienes, cuando efectúen transacciones ocasionales en efectivo por un valor igual o superior a 7 500 EUR, ya se lleven estas a cabo en una o en varias operaciones entre las que parezca existir algún tipo de relación;

(d) en el caso de los proveedores de servicios de juegos de azar, cuando efectúen transacciones ocasionales por un valor igual o superior a 2 000 EUR, ya se lleven estas a cabo en una o en varias operaciones entre las que parezca existir algún tipo de relación;

(e) cuando existan sospechas de blanqueo de capitales o de financiación del terrorismo, con independencia de cualquier excepción, exención o umbral;

(f) cuando existan dudas sobre la veracidad o adecuación de los datos de identificación del cliente obtenidos con anterioridad.

Artículo 11

1. Las medidas de diligencia debida con respecto al cliente comprenderán las actuaciones siguientes:

(a) la identificación del cliente y la comprobación de su identidad sobre la base de documentos, datos o informaciones obtenidas de fuentes fiables e independientes;

(b) la identificación del titular real y la adopción, a fin de comprobar su identidad, de medidas razonables tales que garanticen a la entidad o persona sujeta a lo dispuesto en la presente Directiva el conocimiento del titular real, incluida, en el caso de las personas jurídicas, fideicomisos y

estructuras jurídicas similares, la adopción de medidas razonables a fin de comprender la estructura de propiedad y control del cliente;

(c) la evaluación y, en su caso, la obtención de información sobre el propósito y la índole prevista de la relación de negocios;

(d) la aplicación de medidas de seguimiento continuo a la relación de negocios, incluido el escrutinio de las transacciones efectuadas a lo largo de dicha relación, a fin de garantizar que coincidan con el conocimiento que tengan la entidad o persona del cliente y de su perfil empresarial y de riesgo, incluido, en su caso, el origen de los fondos, y garantizar que los documentos, datos o informaciones de que se disponga estén actualizados.

2. Los Estados miembros velarán por que las entidades obligadas apliquen cada uno de los requisitos del apartado 1 sobre diligencia debida con respecto al cliente; no obstante estas entidades podrán determinar el grado de su aplicación en función del riesgo.

3. Al evaluar los riesgos de blanqueo de capitales y financiación del terrorismo, los Estados miembros exigirán a las entidades obligadas que tengan en cuenta como mínimo las variables indicadas en el anexo I.

4. Los Estados miembros velarán por que las entidades obligadas estén en condiciones de demostrar a las autoridades competentes o a los organismos autorreguladores que las medidas son adecuadas en vista de los riesgos detectados de blanqueo de capitales o de financiación del terrorismo.

5. En cuanto a las actividades en el ámbito de los seguros de vida u otros seguros relacionados con inversiones, los Estados miembros velarán por que, además de las medidas de diligencia debida requeridas con respecto al cliente y el titular real, las entidades financieras apliquen las siguientes medidas de diligencia debida con respecto al cliente a los beneficiarios de pólizas de seguros de vida u otros seguros relacionados con inversiones, en cuanto se identifique o designe a dichos beneficiarios:

(a) en el caso de los beneficiarios identificados como personas físicas o jurídicas o estructuras jurídicas con una denominación concreta, tomando el nombre de la persona;

(b) en el caso de los beneficiarios que sean designados por características o por categoría o por otros medios, obteniendo información suficiente sobre dichos beneficiarios para que la entidad financiera pueda estar segura de que será capaz de establecer la identidad de los mismos en el momento del desembolso.

En los dos casos contemplados en las letras a) y b), la verificación de la identidad de los beneficiarios tendrá lugar en el momento del desembolso. En caso de cesión, total o parcial, a un tercero de un seguro de vida u otro seguro relacionado con inversiones, las entidades financieras que tengan conocimiento de la cesión deberán identificar al titular real en el momento de la cesión a la persona física o jurídica o a la estructura jurídica que reciba para su propio beneficio el valor de la póliza cedida.

Artículo 12

1. Los Estados miembros exigirán que la comprobación de la identidad del cliente y del titular real se efectúe antes de que se establezca una relación de negocios o de que se realice una transacción.

2. No obstante lo dispuesto en el apartado 1, los Estados miembros podrán permitir que la comprobación de la identidad del cliente y del titular real se efectúe durante el establecimiento de una relación de negocios, cuando ello sea necesario para no interrumpir el desarrollo normal de la operación y cuando el riesgo de blanqueo de capitales o de financiación del terrorismo sea escaso. En tal caso, el procedimiento se concluirá lo antes posible tras el primer contacto.

3. No obstante lo dispuesto en los apartados 1 y 2, los Estados miembros podrán permitir la apertura de cuentas bancarias siempre y cuando existan suficientes garantías de que el cliente o cualquier otra persona en su nombre no efectúen operaciones hasta que se hayan cumplido los requisitos de dichos apartados.

4. Los Estados miembros prohibirán a la entidad o persona interesada que no pueda cumplir lo dispuesto en el artículo 11, apartado 1, letras a), b) y c), efectuar operaciones a través de una cuenta bancaria, establecer una relación de negocios o llevar a cabo una transacción, y le exigirán que se plantee la finalización de la relación de negocios y el envío de una notificación de transacción sospechosa en relación con el cliente a la unidad de inteligencia financiera (UIF), con arreglo al artículo 32.

Los Estados miembros eximirán de la aplicación del párrafo anterior a los notarios, otros profesionales independientes del Derecho, los auditores, los contables externos y los asesores fiscales única y exclusivamente en aquellos casos en que tal exención se refiera a la determinación de la posición jurídica de su cliente o al desempeño de su misión de defender o representar a dicho cliente en un procedimiento

judicial o en relación con dicho procedimiento, incluido el asesoramiento sobre la incoación de un procedimiento judicial o la forma de evitarlo.

5. Los Estados miembros exigirán a las entidades obligadas que no solo apliquen procedimientos de diligencia debida con respecto al cliente a todos los nuevos clientes, sino también, en el momento oportuno, a los clientes existentes, en función de un análisis del riesgo, en particular cuando cambien las circunstancias pertinentes de un cliente.

SECCIÓN 2

MEDIDAS SIMPLIFICADAS DE DILIGENCIA DEBIDA CON RESPECTO AL CLIENTE

Artículo 13

1. Cuando los Estados miembros o las entidades obligadas identifiquen ámbitos de menor riesgo, dichos Estados miembros podrán autorizar a las entidades obligadas a aplicar medidas simplificadas de diligencia debida con respecto al cliente.

2. Antes de aplicar las medidas simplificadas de diligencia debida con respecto al cliente, las entidades obligadas deberán determinar que la relación o transacción con el cliente presenta un menor grado de riesgo.

3. Los Estados miembros velarán por que las entidades obligadas controlen suficientemente la transacción o la relación de negocios para poder detectar operaciones inusuales o sospechosas.

Artículo 14

Al evaluar los riesgos de blanqueo de capitales y financiación del terrorismo en relación con distintos tipos de clientes, países o zonas geográficas, y con determinados productos, servicios, operaciones o canales de distribución, los Estados miembros y las entidades obligadas deberán tener en cuenta como mínimo los factores de identificación de situaciones potencialmente de menor riesgo que figuran en el anexo II.

Artículo 15

La ABE, la AESPJ y la AEVM emitirán directrices dirigidas a las autoridades competentes y a las entidades obligadas contempladas en el artículo 2, apartado 1, puntos 1 y 2, de conformidad con el artículo 16 del Reglamento (UE) nº 1093/2010, el Reglamento (UE) nº 1094/2010 y el Reglamento (UE) nº 1095/2010, sobre los factores de riesgo que deberán tenerse en cuenta y/o las medidas que deberán tomarse en las situaciones en que resulte oportuna la adopción de medidas simplificadas de diligencia debida. Procederá tener especialmente en cuenta la naturaleza y el tamaño de la empresa y, cuando resulte adecuado y proporcionado, prever medidas específicas. Estas directrices se emitirán en un plazo de dos años a partir de la fecha de entrada en vigor de la presente Directiva.

SECCIÓN 3

MEDIDAS REFORZADAS DE DILIGENCIA DEBIDA CON RESPECTO AL CLIENTE

Artículo 16

1. En los casos especificados en los artículos 17 a 23 de la presente Directiva y en otros casos de riesgo más elevado identificados por los Estados miembros o las entidades obligadas, los Estados miembros exigirán a las entidades obligadas que apliquen medidas reforzadas de diligencia debida con respecto al cliente a fin de gestionar y atenuar debidamente esos riesgos.

2. Los Estados miembros exigirán a las entidades obligadas que examinen, en la medida de lo posible, el contexto y la finalidad de todas las transacciones complejas o de un importe inusitadamente elevado, así como toda pauta de transacción no habitual que no presente un propósito económico aparente o visiblemente lícito. En particular, deberán aumentar el grado y la naturaleza de la supervisión de la relación de negocios, a fin de determinar si las transacciones o actividades parecen inusuales o sospechosas.

3. Al evaluar los riesgos de blanqueo de capitales y financiación del terrorismo, los Estados miembros y las entidades obligadas deberán tener en cuenta como mínimo los factores de identificación de situaciones potencialmente de mayor riesgo que figuran en el anexo III.

4. La ABE, la AESPJ y la AEVM emitirán directrices dirigidas a las autoridades competentes y a las entidades obligadas contempladas en el artículo 2, apartado 1, puntos 1 y 2, de conformidad con el artículo 16 del Reglamento (UE) nº 1093/2010, el Reglamento (UE) nº 1094/2010 y el Reglamento (UE) nº 1095/2010, sobre los factores de riesgo que deberán tenerse en cuenta y/o las medidas que deberán tomarse en las situaciones en que deban aplicarse medidas reforzadas de diligencia debida. Esas directrices se emitirán en un plazo de dos años a partir de la fecha de entrada en vigor de la presente Directiva.

Artículo 17

Con respecto a las relaciones transfronterizas de corresponsalía bancaria con entidades clientes de terceros países, los Estados miembros exigirán a sus entidades de crédito, además de las medidas de diligencia debida con respecto al cliente que se establecen en el artículo 11:

(a) que reúnan sobre la entidad cliente información suficiente para comprender cabalmente la naturaleza de sus actividades y determinar, a partir de información de dominio público, la reputación de la entidad y su calidad de supervisión;

(b) que evalúen los controles contra el blanqueo de capitales y la financiación del terrorismo de que disponga la entidad cliente;

(c) que obtengan autorización de la dirección antes de establecer nuevas relaciones de corresponsalía bancaria;

(d) que documenten las responsabilidades respectivas de cada entidad;

(e) con respecto a las cuentas de transferencias de pagos en otras plazas (*payable-through accounts*), que se cercioren de que la entidad cliente ha comprobado la identidad y aplicado en todo momento medidas de diligencia debida con respecto a los clientes que tienen acceso directo a cuentas de la entidad corresponsal y de que, a instancias de esta, puede facilitar los datos de un cliente que sean necesarios a efectos de la diligencia debida.

Artículo 18

En relación con las transacciones o relaciones de negocios con personas del medio político extranjeras, los Estados miembros exigirán a las entidades obligadas, además de las medidas de diligencia debida con respecto al cliente establecidas en el artículo 11:

(a) que dispongan de procedimientos adecuados en función del riesgo a fin de determinar si el cliente o el titular real del cliente pertenece a esa categoría de personas;

(b) que obtengan la autorización de la dirección para establecer o mantener relaciones de negocios con dichos clientes;

(c) que adopten medidas adecuadas a fin de determinar el origen del patrimonio y de los fondos con los que tendrá lugar la relación de negocios o transacción;

(d) que lleven a cabo una supervisión reforzada y permanente de la relación de negocios.

Artículo 19

En relación con las transacciones o relaciones de negocios con personas del medio político de la UE o con personas que desempeñen o hayan desempeñado funciones importantes en una organización internacional, los Estados miembros exigirán a las entidades obligadas, además de las medidas de diligencia debida con respecto al cliente establecidas en el artículo 11:

(a) que dispongan de procedimientos adecuados en función del riesgo a fin de determinar si el cliente o el titular real del cliente pertenece a una de esas categorías de personas;

(b) en los casos de relaciones de negocios de mayor riesgo con esas categorías de personas, que apliquen las medidas contempladas en el artículo 18, letras b), c) y d).

Artículo 20

Las entidades obligadas deberán tomar medidas razonables para determinar si los beneficiarios de pólizas de seguros de vida u otros seguros relacionados con inversiones y/o, en su caso, el titular real del beneficiario, son personas del medio político. Esas medidas se adoptarán a más tardar en el momento del desembolso o en el momento de la cesión, total o parcial, de la póliza. Cuando se identifiquen riesgos más elevados, además de adoptar las medidas normales de diligencia debida con respecto al cliente, los Estados miembros exigirán a las entidades obligadas:

(a) que informen a la dirección antes del desembolso del producto de la póliza;

(b) que procedan a un control reforzado de la relación de negocios con el titular de la póliza en su conjunto.

Artículo 21

Las medidas contempladas en los artículos 18, 19 y 20 serán también aplicables a los familiares o a las personas reconocidas como allegados de las mencionadas personas del medio político.

Artículo 22

Cuando una de las personas contempladas en los artículos 18, 19 y 20 haya dejado de desempeñar una función pública importante por encargo de un Estado miembro o de un tercer país, o una función importante en una organización internacional, las entidades obligadas deberán tener presente el riesgo que sigue representando dicha persona y aplicar las medidas adecuadas y basadas en el riesgo que sean necesarias hasta el momento en que se considere que ya no representa un riesgo. Este plazo no podrá ser inferior a 18 meses.

Artículo 23

1. Los Estados miembros prohibirán a las entidades de crédito establecer o mantener relaciones de corresponsalía bancaria con un banco pantalla y requerirán a las entidades de crédito que adopten medidas adecuadas para asegurar que no entablan o mantienen relaciones de corresponsalía con un banco del que se conozca que permite el uso de sus cuentas por bancos pantalla.

2. A efectos del apartado 1, se entenderá por «banco pantalla» una entidad de crédito o entidad que desarrolla una actividad similar, constituida en un país en el que no tenga una presencia física que permita ejercer una verdadera gestión y dirección y que no esté asociada a un grupo financiero regulado.

SECCIÓN 4

APLICACIÓN POR TERCEROS

Artículo 24

Los Estados miembros podrán permitir que las entidades obligadas recurran a terceros para aplicar los requisitos contemplados en el artículo 11, apartado 1, letras a), b) y c). No obstante, por lo que respecta al cumplimiento de dichos requisitos, seguirá siendo responsable última la entidad obligada que recurra al tercero.

Artículo 25

1. A efectos de la presente sección, se entenderá por «terceros» las entidades obligadas enumeradas en el artículo 2 u otras entidades y personas situadas en Estados miembros o en un tercer país que apliquen requisitos de diligencia debida con respecto al cliente y de conservación de documentos equivalentes a los establecidos en la presente Directiva, y que supervisen el cumplimiento de los requisitos de la presente Directiva de conformidad con el capítulo VI, sección 2.

2. Los Estados miembros deberán tomar en consideración la información disponible sobre el nivel de riesgo geográfico a la hora de decidir si un tercer país cumple los requisitos establecidos en el apartado 1 y se informarán mutuamente, e informarán a la Comisión, la ABE, la AESPJ y la AEVM, en la medida que corresponda a los fines de la presente Directiva y de conformidad con las disposiciones pertinentes del Reglamento (UE) nº 1093/2010, del Reglamento (UE) nº 1094/2010 y del Reglamento (UE) nº 1095/2010, de aquellos casos en que consideren que un tercer país cumple dichos requisitos.

Artículo 26

1. Los Estados miembros velarán por que las entidades obligadas obtengan de los terceros a los que recurran la información necesaria sobre los requisitos establecidos en el artículo 11, apartado 1, letras a), b) y c).

2. Los Estados miembros velarán por que las entidades obligadas a las que se remita al cliente adopten las medidas adecuadas para garantizar que los terceros les transmitan, previa solicitud, las correspondientes copias de los datos de comprobación de identidad y demás documentación pertinente sobre la identidad del cliente o titular real.

Artículo 27

Los Estados miembros velarán por que la autoridad competente del país de origen (en lo que respecta a las políticas y controles a nivel de grupo) y la autoridad competente del país de acogida (en lo que atañe a las sucursales y filiales) pueda considerar que una entidad obligada aplica las medidas establecidas en el artículo 25, apartado 1, y en el artículo 26 a través de su programa de grupo, cuando se cumplan las siguientes condiciones:

(a) que la entidad obligada se base en la información facilitada por un tercero que forme parte del mismo grupo;

(b) que dicho grupo aplique medidas de diligencia debida con respecto al cliente, normas sobre conservación de documentos y programas de lucha contra el blanqueo de capitales y la financiación del terrorismo de conformidad con la presente Directiva o disposiciones equivalentes;

(c) que la aplicación efectiva de los requisitos contemplados en la letra b) sea supervisada a nivel de grupo por una autoridad competente.

Artículo 28

Lo dispuesto en la presente sección no se aplicará a las relaciones de externalización o agencia cuando, en virtud de un acuerdo contractual, el proveedor de servicios de externalización o agente deba considerarse parte de la entidad obligada.

CAPÍTULO III

INFORMACIÓN SOBRE LA TITULARIDAD REAL

Artículo 29

1. Los Estados miembros velarán por que las sociedades u otras personas jurídicas establecidas en su territorio obtengan y mantengan información adecuada, precisa y actual sobre su titularidad real.

2. Los Estados miembros velarán por que las autoridades competentes y las entidades obligadas puedan acceder oportunamente a la información a que se refiere el apartado 1 del presente artículo.

Artículo 30

1. Los Estados miembros velarán por que los fideicomisarios de un fideicomiso explícito sujeto a su legislación obtengan y mantengan información adecuada, precisa y actual sobre la titularidad real en relación con el fideicomiso. Esa información incluirá la identidad del fideicomitente, del fideicomisario o fideicomisarios, del protector (si procede), de los beneficiarios o categoría de beneficiarios, y de cualquier otra persona física que ejerza el control efectivo del fideicomiso.

2. Los Estados miembros velarán por que los fideicomisarios comuniquen su condición a las entidades obligadas cuando, como tales, entablen una relación de negocios o realicen una transacción ocasional por encima del umbral fijado en el artículo 10, letras b), c) y d) .

3. Los Estados miembros velarán por que las autoridades competentes y las entidades obligadas puedan acceder oportunamente a la información a que se refiere el apartado 1 del presente artículo.

4. Los Estados miembros velarán por que las medidas correspondientes a lo dispuesto en los apartados 1, 2 y 3 se apliquen a otros tipos de persona o estructura jurídicas que tengan una estructura y una función similares a las de los fideicomisos.

CAPÍTULO IV

OBLIGACIONES DE INFORMACIÓN

SECCIÓN 1

DISPOSICIONES GENERALES

Artículo 31

1. Todos los Estados miembros establecerán una UIF a fin de prevenir, detectar e investigar el blanqueo de capitales y la financiación del terrorismo.

2. Los Estados miembros notificarán por escrito a la Comisión el nombre y la dirección de las UIF respectivas.

3. La UIF se establecerá como unidad nacional central. Será responsable de recibir (y, en la medida de sus competencias, solicitar), analizar y comunicar a las autoridades competentes la información que guarde relación con el blanqueo potencial de capitales o delitos principales conexos, la potencial financiación del terrorismo o que sea exigida en virtud de las disposiciones legales o reglamentarias nacionales. Se le dotará de los recursos adecuados para que lleve a cabo sus funciones.

4. Los Estados miembros deberán garantizar que la UIF tenga acceso, directa o indirectamente, en el plazo requerido, a la información financiera, administrativa y policial y judicial que necesite para llevar a cabo sus funciones de manera adecuada. Además, la UIF deberá responder a las solicitudes de información de las autoridades judiciales y policiales de su Estado miembro, salvo cuando razones de hecho hagan suponer que el suministro de la información tendría un impacto negativo en investigaciones o análisis en curso, o, en circunstancias excepcionales, cuando la divulgación de la información sea claramente desproporcionada respecto a los intereses legítimos de la persona física o jurídica, o no sea pertinente con respecto a los fines para los que se haya solicitado.

5. Los Estados miembros velarán por que las UIF estén facultadas para tomar medidas urgentes, ya sea directa o indirectamente, cuando se sospeche que una transacción está relacionada con el blanqueo de capitales o la financiación del terrorismo, y para suspender o no autorizar una transacción en curso, a fin de analizar la transacción y confirmar la sospecha.

6. La función de análisis de las UIF consistirá en un análisis operativo de casos individuales y objetivos específicos y en un análisis estratégico que examine las tendencias y pautas del blanqueo de capitales y la financiación del terrorismo.

Artículo 32

1. Los Estados miembros exigirán a las entidades obligadas y, en su caso, a sus directivos y empleados que colaboren plenamente:

   (a) informando por iniciativa propia, y sin demora, a la UIF cuando la entidad o persona sujetas a lo dispuesto en la presente Directiva sepan, sospechen o tengan motivos razonables para sospechar que unos fondos son el producto de actividades delictivas o están relacionados con la financiación del terrorismo y respondiendo sin demora a las solicitudes de información adicional que les dirija la UIF en tales casos;

   (b) facilitando de inmediato a la UIF, a petición de esta, toda la información que sea necesaria de conformidad con los procedimientos establecidos en la legislación aplicable.

2. La información a que hace referencia el apartado 1 del presente artículo será remitida a la UIF del Estado miembro en cuyo territorio se encuentre situada la entidad o persona que facilite dicha información. Se encargarán de remitir la información la persona o personas que hayan sido designadas de conformidad con los procedimientos contemplados en el artículo 8, apartado 4.

Artículo 33

1. No obstante lo dispuesto en el artículo 32, apartado 1, en el caso de las personas contempladas en el artículo 2, apartado 1, punto 3, letras a), b) y d), los Estados miembros podrán designar a un organismo autorregulador pertinente de la profesión de que se trate como la autoridad que debe recibir la información mencionada en el artículo 32, apartado 1.

Sin perjuicio de lo dispuesto en el apartado 2, en los casos contemplados en el párrafo primero los organismos autorreguladores designados transmitirán de inmediato la información sin filtrar a la UIF.

2. Los Estados miembros eximirán de la aplicación de las obligaciones establecidas en el artículo 32, apartado 1, a los notarios, otros profesionales independientes del Derecho, los auditores, los contables externos y los asesores fiscales única y exclusivamente en aquellos casos en que tal exención se refiera a la información que estos reciban de uno de sus clientes u obtengan sobre él al determinar la posición jurídica de su cliente o desempeñar su misión de defender o representar a dicho cliente en un procedimiento judicial o en relación con dicho procedimiento, incluido el asesoramiento sobre la incoación de un procedimiento judicial o la forma de evitarlo, independientemente de si han recibido u obtenido dicha información antes, durante o después de tal procedimiento.

Artículo 34

1. Los Estados miembros exigirán a las entidades obligadas que se abstengan de ejecutar transacciones de las que sepan o sospechen que están relacionadas con el blanqueo de capitales o la financiación del terrorismo hasta tanto no hayan completado la actuación necesaria de conformidad con el artículo 32, apartado 1, letra a).

Con arreglo a la legislación de los Estados miembros, podrán darse instrucciones para que no se ejecute la operación.

2. Cuando se sospeche que la transacción considerada implicará blanqueo de capitales o financiación del terrorismo y abstenerse de ejecutarla resulte imposible o pueda comprometer el procesamiento de los beneficiarios de la presunta operación de blanqueo o financiación del terrorismo, las entidades obligadas informarán de ello a la UIF inmediatamente después.

Artículo 35

1. Los Estados miembros velarán por que las autoridades competentes contempladas en el artículo 45, en caso de que descubran hechos que puedan estar relacionados con el blanqueo de capitales o la financiación del terrorismo, ya sea durante las inspecciones efectuadas por esas autoridades en las entidades obligadas o de cualquier otro modo, informen de ello sin demora a la UIF.

2. Los Estados miembros velarán por que las autoridades supervisoras facultadas mediante disposiciones legales o reglamentarias para supervisar las bolsas de valores y los mercados de divisas y de derivados financieros informen a la UIF cuando descubran hechos que puedan estar relacionados con el blanqueo de capitales o la financiación del terrorismo.

Artículo 36

La comunicación, de buena fe, con arreglo a lo previsto en el artículo 32, apartado 1, y en el artículo 33 de la información contemplada en los artículos 32 y 33 a la UIF, por parte de una entidad obligada, o de sus empleados o directivos no constituirá violación de las restricciones sobre divulgación de información impuestas por vía contractual o por cualquier disposición legal, reglamentaria o administrativa y no implicará ningún tipo de responsabilidad para la entidad obligada, sus directivos o empleados.

Artículo 37

Los Estados miembros tomarán todas las medidas apropiadas a fin de proteger frente a toda amenaza o acción hostil a los empleados de las entidades obligadas que comuniquen sus sospechas de blanqueo de capitales o de financiación del terrorismo, ya sea por vía interna o a la UIF.

SECCIÓN 2

PROHIBICIÓN DE REVELACIÓN

Artículo 38

1. Las entidades obligadas, así como sus directivos y empleados, no revelarán al cliente de que se trate ni a terceros que se ha transmitido información de conformidad con los artículos 32 y 33 ni que está realizándose o puede realizarse una investigación sobre blanqueo de capitales o financiación del terrorismo.

2. La prohibición del apartado 1 no incluirá la revelación a las autoridades competentes de los Estados miembros, incluidos los organismos autorreguladores, o la revelación a efectos de aplicación de la ley.

3. La prohibición establecida en el apartado 1 no impedirá la comunicación de información entre entidades de los Estados miembros, o de terceros países que impongan requisitos equivalentes a los enunciados en la presente Directiva, siempre que pertenezcan al mismo grupo.

4. La prohibición establecida en el apartado 1 no impedirá la comunicación de información entre las personas a que se refiere el artículo 2, apartado 1, punto 3, letras a) y b), situadas en los Estados miembros, o en terceros países que impongan requisitos equivalentes a los enunciados en la presente Directiva, que ejerzan sus actividades profesionales, ya sea como empleados o de otro modo, dentro de una misma entidad jurídica o en una red.

   A los efectos del párrafo primero, se entenderá por «red» la estructura más amplia a la que pertenece la persona y que comporta una propiedad, una gestión o una supervisión del cumplimiento comunes.

5. Cuando se trate de las entidades o personas a que se refiere el artículo 2, apartado 1, puntos 1 y 2, y punto 3, letras a) y b), en los casos que se refieran a un mismo cliente y a una misma transacción en la que intervengan dos o más entidades o personas, la prohibición establecida en el apartado 1 del presente artículo no impedirá la comunicación de información entre las entidades o personas pertinentes, siempre que estén establecidas en un Estado miembro, o en un tercer país que imponga requisitos equivalentes a los establecidos por la presente Directiva, pertenezcan a la misma categoría profesional y estén sujetas a obligaciones en lo relativo al secreto profesional y la protección de los datos personales.

6. Cuando las personas a que se refiere el artículo 2, apartado 1, punto 3, letras a) y b), intenten disuadir a un cliente de una actividad ilegal, ello no constituirá revelación a efectos del apartado 1.

CAPÍTULO V

CONSERVACIÓN DE DOCUMENTOS Y DATOS ESTADÍSTICOS

Artículo 39

Los Estados miembros exigirán a las entidades obligadas que conserven los siguientes documentos y datos de conformidad con el Derecho nacional, con fines de prevención, detección e investigación, por parte de la UIF o de cualquier otra autoridad competente, de posibles casos de blanqueo de capitales o de financiación del terrorismo:

(a) En los casos de diligencia debida con respecto al cliente, copia o referencias de las pruebas exigidas durante un período de cinco años desde que hayan finalizado las relaciones de negocios con su cliente. Tras la expiración de este plazo, los datos personales deberán eliminarse salvo que la legislación nacional disponga lo contrario, en cuyo caso se determinará en qué circunstancias las entidades obligadas podrán o deberán conservar más tiempo estos datos. Los Estados miembros podrán autorizar o exigir que los datos se conserven más allá de dicho plazo únicamente si es necesario a efectos de prevención, detección o investigación de blanqueo de capitales y financiación del terrorismo. El período máximo de conservación tras la finalización de la relación de negocios no será superior a diez años.

(b) En los casos de relaciones de negocios y transacciones, los justificantes y registros, consistentes en documentos originales o en copias que tengan fuerza probatoria similar en virtud del Derecho nacional, durante un período mínimo de cinco años tras la ejecución de las transacciones, o tras la conclusión de la relación de negocios si este período fuera más breve. Tras la expiración de este plazo, los datos personales deberán eliminarse salvo que la legislación nacional disponga lo contrario, en cuyo caso se determinará en qué circunstancias las entidades obligadas podrán o deberán conservar más tiempo estos datos. Los Estados miembros podrán autorizar o exigir que los datos se conserven más allá de dicho plazo únicamente si es necesario a efectos de prevención, detección o investigación de blanqueo de capitales y financiación del terrorismo. El período máximo de conservación, tras la ejecución de las transacciones, o tras la conclusión de la relación de negocios si este período finalizara antes, no podrá exceder de diez años.

Artículo 40

Los Estados miembros exigirán que sus entidades obligadas instauren sistemas que les permitan responder de forma completa y diligente a las solicitudes de información que les curse la UIF u otras autoridades con arreglo a su Derecho nacional sobre si mantienen o han mantenido a lo largo de los cinco años anteriores relaciones de negocios con determinadas personas físicas o jurídicas y sobre la naturaleza de dichas relaciones.

Artículo 41

1. A efectos de la preparación de las evaluaciones nacionales de riesgos, de conformidad con el artículo 7, los Estados miembros garantizarán que están en condiciones de evaluar la eficacia de sus sistemas de lucha contra el blanqueo de capitales y la financiación del terrorismo y, a tal fin, dispondrán de estadísticas exhaustivas sobre cuestiones pertinentes para la eficacia de tales sistemas.

2. Las estadísticas mencionadas en el apartado 1 incluirán:

   (a) datos relativos al tamaño y la importancia de los diferentes sectores incluidos en el ámbito de aplicación de la presente Directiva, en particular el número de entidades y personas y la importancia económica de cada uno de los sectores;

   (b) datos relativos a las fases de información, de investigación y judicial del sistema nacional de lucha contra el blanqueo de capitales y la financiación del terrorismo, en particular el número de comunicaciones de transacciones sospechosas remitidas a la UIF, el seguimiento dado a dichas comunicaciones y el número anual de asuntos investigados, así como el número de personas procesadas, el número de personas condenadas por delitos relacionados con el blanqueo de capitales o con la financiación del terrorismo y el valor en euros de los bienes congelados, incautados o confiscados.

3. Los Estados miembros deberán garantizar la publicación de un estado consolidado de sus informes estadísticos y transmitir a la Comisión los datos estadísticos contemplados en el apartado 2.

CAPÍTULO VI

POLÍTICAS, PROCEDIMIENTOS Y SUPERVISIÓN

SECCIÓN 1

PROCEDIMIENTOS INTERNOS, FORMACIÓN Y COMUNICACIÓN DE OBSERVACIONES

Artículo 42

1. Los Estados miembros exigirán que las entidades obligadas que formen parte de un grupo apliquen, a nivel de grupo, políticas y procedimientos, incluidas políticas de protección de datos y políticas y procedimientos para el intercambio de información dentro del grupo, contra el blanqueo de capitales y la financiación del terrorismo. Dichas políticas y procedimientos se aplicarán de manera efectiva a nivel de las sucursales y las filiales en las que tengan participación mayoritaria en los Estados miembros y terceros países.

2. Los Estados miembros velarán por que, cuando las entidades obligadas posean sucursales o filiales en las que tengan participación mayoritaria que estén situadas en un tercer país donde los requisitos mínimos en materia de lucha contra el blanqueo de capitales y la financiación del terrorismo sean menos estrictos que los de los Estados miembros, estas sucursales y filiales apliquen los requisitos del Estado miembro, incluidos los relativos a la protección de datos, en la medida en que lo permitan las disposiciones legales y reglamentarias de dicho tercer país.

3. Los Estados miembros, la ABE, la AESPJ y la AEVM se informarán mutuamente de aquellos casos en que consideren que el Derecho del tercer país no permite la aplicación de las medidas exigidas con arreglo al apartado 1 y en los que se pueda actuar en el marco de un procedimiento acordado para hallar una solución.

4. Los Estados miembros requerirán que, cuando el Derecho del tercer país no permita la aplicación de las medidas exigidas con arreglo al apartado 1, párrafo primero, las entidades obligadas adopten medidas adicionales para hacer frente eficazmente al riesgo de blanqueo de capitales o de financiación del terrorismo e informen a los supervisores de su país de origen. Si las medidas adicionales no son suficientes, las autoridades competentes del país de origen estudiarán la adopción de actuaciones de supervisión adicionales, entre ellas, en su caso, solicitar al grupo financiero que cese sus actividades en el país de acogida.

5. La ABE, la AESPJ y la AEVM elaborarán proyectos de normas técnicas de regulación que especifiquen el tipo de medidas adicionales contempladas en el apartado 4 del presente artículo y las medidas mínimas que deberán tomar las entidades obligadas a que se refiere el artículo 2, apartado 1, puntos 1 y 2, cuando el Derecho del tercer país no permita la aplicación de las medidas exigidas con arreglo a los apartados 1 y 2. La ABE, la AESPJ y la AEVM presentarán a la Comisión dichos proyectos de normas técnicas de regulación en el plazo de dos años a partir de la fecha de entrada en vigor de la presente Directiva.

6. Se delegan en la Comisión poderes para adoptar las normas técnicas de regulación a que se refiere el apartado 5, de conformidad con el procedimiento establecido en los artículos 10 a 14 del Reglamento (UE) nº 1093/2010, del Reglamento (UE) nº 1094/2010 y del Reglamento (UE) nº 1095/2010.

7. Los Estados miembros velarán por que se permita el intercambio de información dentro del grupo, a condición de que ello no afecte a la investigación o análisis de posibles casos de blanqueo de capitales o de financiación del terrorismo por parte de la UIF o de cualquier otra autoridad competente en virtud del Derecho nacional.

8. Los Estados miembros podrán exigir a los emisores de dinero electrónico, tal como se definen en la Directiva 2009/110/CE del Parlamento Europeo y del Consejo[44], y a los proveedores de servicios de pago, tal como se definen en la Directiva 2007/64/CE del Parlamento Europeo y del Consejo [45], establecidos en su territorio, y cuya sede central se encuentre en otro Estado miembro o fuera de la Unión, que designen un punto de contacto central en su territorio para supervisar el cumplimiento de las normas contra el blanqueo de capitales y la financiación del terrorismo.

9. La ABE, la AESPJ y la AEVM elaborarán proyectos de normas técnicas de regulación sobre los criterios para determinar las circunstancias en que resulta adecuada la designación de un punto de contacto central en virtud del apartado 8 y las funciones que deben desempeñar estos puntos de contacto. La ABE, la AESPJ y la AEVM presentarán a la Comisión dichos proyectos de normas técnicas de regulación en el plazo de dos años a partir de la fecha de entrada en vigor de la presente Directiva.

10. Se delegan en la Comisión poderes para adoptar las normas técnicas de regulación a que se refiere el apartado 9, de conformidad con el procedimiento establecido en los artículos 10 a 14 del Reglamento (UE) nº 1093/2010, del Reglamento (UE) nº 1094/2010 y del Reglamento (UE) nº 1095/2010.

Artículo 43

1. Los Estados miembros exigirán a las entidades obligadas que adopten medidas proporcionadas a sus riesgos, naturaleza y tamaño, para que sus empleados tengan conocimiento de las disposiciones adoptadas en aplicación de la presente Directiva, incluidos los requisitos pertinentes en materia de protección de datos.

   Estas medidas incluirán la participación de los empleados correspondientes en cursos especiales de formación permanente para ayudarles a detectar las operaciones que puedan estar relacionadas con el blanqueo de capitales o la financiación del terrorismo y enseñarles la manera de proceder en tales casos.

   En caso de que una persona física perteneciente a alguna de las categorías enumeradas en el artículo 2, apartado 1, punto 3, ejerza su profesión en calidad de empleado de una persona jurídica, las obligaciones impuestas por la presente sección recaerán en dicha persona jurídica en vez de en la persona física.

2. Los Estados miembros velarán por que las entidades obligadas tengan acceso a información actualizada sobre las prácticas de los autores de blanqueo de capitales y de los financiadores del terrorismo y sobre los indicios que permiten detectar las transacciones sospechosas.

3. Los Estados miembros velarán por que, siempre que sea posible, se aporte oportunamente información sobre la eficacia y el seguimiento de las comunicaciones relativas a presuntos casos de blanqueo de capitales o financiación del terrorismo.

SECCIÓN 2

SUPERVISIÓN

Artículo 44

1. Los Estados miembros dispondrán que los establecimientos de cambio y los proveedores de servicios a sociedades o fideicomisos estén sujetos a la obligación de obtener licencia o de registrarse y los proveedores de servicios de juegos de azar, a la de obtener autorización.

2. Con respecto a las entidades a que se refiere el apartado 1, los Estados miembros exigirán a las autoridades competentes que se cercioren de la honorabilidad y profesionalidad de las personas que de hecho dirijan o vayan a dirigir las actividades de dichas entidades o la de sus titulares reales.

[44] DO L 267 de 10.10.2009, p. 7.
[45] DO L 319 de 5.12.2007, p. 1.

3. Por lo que se refiere a las entidades obligadas a que se refiere el artículo 2, apartado 1, punto 3, letras a), b), d) y e), los Estados miembros velarán por que las autoridades competentes adopten las medidas necesarias para evitar que los delincuentes o sus cómplices posean o sean titulares reales de una participación significativa o mayoritaria, o desempeñen una función de gestión en esas entidades obligadas.

Artículo 45

1. Los Estados miembros exigirán a las autoridades competentes que supervisen eficazmente y tomen las medidas necesarias para garantizar el cumplimiento de lo dispuesto en la presente Directiva.

2. Los Estados miembros velarán por que las autoridades competentes posean las competencias adecuadas, entre ellas la de obligar a aportar cualquier información que sea pertinente a efectos de la supervisión del cumplimiento y la de realizar controles, y por que dispongan de los recursos financieros, humanos y técnicos adecuados para desempeñar sus funciones. Los Estados miembros velarán por que el personal de estas autoridades observe unas estrictas normas profesionales, en particular en materia de confidencialidad y protección de datos, tenga un elevado nivel de integridad y esté debidamente cualificado.

3. En el caso de las entidades de crédito, entidades financieras y proveedores de servicios de juegos de azar, las autoridades competentes tendrán facultades de supervisión reforzadas, en particular la posibilidad de realizar inspecciones *in situ*.

4. Los Estados miembros velarán por que las entidades obligadas que disponen de sucursales o filiales en otros Estados miembros respeten las disposiciones nacionales de esos Estados miembros por lo que se refiere a la presente Directiva.

5. Los Estados miembros velarán por que las autoridades competentes del Estado miembro en el que esté establecida la sucursal o filial cooperen con las autoridades competentes del Estado miembro en el que la entidad obligada tenga su sede central, a fin de garantizar una supervisión eficaz de los requisitos de la presente Directiva.

6. Los Estados miembros velarán por que las autoridades competentes que apliquen a la supervisión un enfoque basado en el riesgo:

   (a) conozcan perfectamente los riesgos de blanqueo de capitales y financiación del terrorismo existentes en su país;

   (b) tengan acceso *in situ* y desde el exterior a toda la información pertinente sobre los riesgos nacionales e internacionales específicos asociados a los clientes, productos y servicios de las entidades obligadas; y

   (c) basen la frecuencia e intensidad de la supervisión *in situ* y desde el exterior en el perfil de riesgo de la entidad obligada y en los riesgos de blanqueo de capitales y financiación del terrorismo existentes en el país.

7. La evaluación del perfil de riesgo de las entidades obligadas en materia de blanqueo de capitales y financiación del terrorismo, incluidos los riesgos de incumplimiento, se revisará periódicamente y cuando se produzcan acontecimientos o novedades importantes en la gestión y el funcionamiento de la entidad obligada.

8. Los Estados miembros velarán por que las autoridades competentes tengan en cuenta el grado de discrecionalidad permitido a la entidad obligada y revisen debidamente las evaluaciones de riesgo en que se basa esta discrecionalidad, así como la adecuación y la aplicación de sus políticas, controles internos y procedimientos.

9. En el caso de las entidades obligadas contempladas en el artículo 2, apartado 1, punto 3, letras a), b) y d), los Estados miembros podrán permitir que las funciones mencionadas en el apartado 1 sean realizadas por organismos autorreguladores, siempre que cumplan lo dispuesto en el apartado 2 del presente artículo.

10. La ABE, la AESPJ y la AEVM emitirán directrices dirigidas a las autoridades competentes de conformidad con el artículo 16 del Reglamento (UE) nº 1093/2010, del Reglamento (UE) nº 1094/2010 y del Reglamento (UE) nº 1095/2010, sobre los factores que deben tomarse en consideración al realizar la supervisión sobre la base de un análisis de riesgos. Procede tener especialmente en cuenta la naturaleza y el tamaño de la empresa y, cuando resulte adecuado y proporcionado, prever medidas específicas. Estas directrices se emitirán en un plazo de dos años a partir de la fecha de entrada en vigor de la presente Directiva.

SECCIÓN 3

COOPERACIÓN

SUBSECCIÓN I

COOPERACIÓN NACIONAL

Artículo 46

Los Estados miembros velarán por que las instancias de decisión, las UIF, las autoridades judiciales y policiales, las autoridades de supervisión y otras autoridades competentes que participen en la lucha contra el blanqueo de capitales y la financiación del terrorismo dispongan de mecanismos eficaces que les permitan cooperar y coordinar a escala nacional la elaboración y la aplicación de las políticas y actividades destinadas a combatir el blanqueo de capitales y la financiación del terrorismo.

SUBSECCIÓN II

COOPERACIÓN CON LA ABE, LA AESPJ Y LA AEVM

Artículo 47

Las autoridades competentes facilitarán a la ABE, la AESPJ y la AEVM toda la información necesaria para llevar a cabo sus obligaciones de conformidad con la presente Directiva.

SUBSECCIÓN III

COOPERACIÓN ENTRE LAS UIF Y CON LA COMISIÓN EUROPEA

Artículo 48

La Comisión podrá prestar la asistencia necesaria para facilitar la coordinación, incluido el intercambio de información, entre las UIF dentro de la Unión. Podrá convocar regularmente reuniones con representantes de las UIF de los Estados miembros a fin de facilitar la cooperación e intercambiar puntos de vista sobre cuestiones relacionadas con la cooperación.

Artículo 49

Los Estados miembros velarán por que sus UIF cooperen entre sí en la mayor medida posible, con independencia de que sean autoridades administrativas, policiales o judiciales, o mixtas.

Artículo 50

1. Los Estados miembros velarán por que las UIF intercambien, por propia iniciativa o previa solicitud, toda información que pueda ser pertinente para el tratamiento o el análisis de información o la investigación, por parte de las UIF, sobre operaciones financieras relacionadas con el blanqueo de capitales o la financiación del terrorismo y sobre las personas físicas o jurídicas implicadas. La solicitud expondrá los hechos pertinentes, los antecedentes y los motivos de la solicitud, y explicará la forma en que se utilizará la información solicitada.

2. Los Estados miembros velarán por que la UIF a la que se dirija la solicitud venga obligada a utilizar todas las competencias de que disponga a nivel nacional para la recepción y análisis de la información cuando responda a una solicitud de información contemplada en el apartado 1, cursada desde otra UIF establecida en la Unión Europea. La UIF a la que vaya dirigida la solicitud deberá responder con diligencia, y tanto la UIF requirente como la UIF requerida utilizarán, en la medida de lo posible, medios digitales seguros para el intercambio de información.

3. Una UIF podrá negarse a divulgar información cuando ello pueda comprometer una investigación penal en el Estado miembro requerido o, en circunstancias excepcionales, en caso de que la divulgación de la información sea claramente desproporcionada para los intereses legítimos de una persona física o jurídica o

del Estado miembro de que se trate, o en caso de que no sea pertinente para los fines para los que fue recogida. Dicha denegación deberá justificarse adecuadamente a la UIF requirente.

Artículo 51

La información y los documentos recibidos con arreglo a los artículos 49 y 50 se utilizarán para el desempeño de las funciones de las UIF establecidas en la presente Directiva. Al transmitir información o documentos con arreglo a los artículos 49 y 50, la UIF transmisora podrá imponer restricciones y condiciones con respecto al uso de la información. La UIF receptora respetará dichas restricciones y condiciones. Ello no afectará a su utilización en investigaciones y procedimientos penales relacionados con las funciones de las UIF para prevenir, detectar e investigar el blanqueo de capitales y la financiación del terrorismo.

Artículo 52

Los Estados miembros velarán por que las UIF adopten todas las medidas necesarias, incluidas medidas de seguridad, a fin de garantizar que ninguna otra autoridad, agencia o departamento pueda acceder a la información presentada con arreglo a los artículos 49 y 50, salvo que la UIF que facilita la información otorgue previamente su consentimiento.

Artículo 53

1. Los Estados miembros animarán a sus UIF a utilizar canales de comunicación protegidos para comunicarse entre sí y a utilizar la red informática descentralizada FIU.net.

2. Los Estados miembros velarán por que, a fin de desempeñar sus funciones con arreglo a lo dispuesto en la presente Directiva, sus UIF cooperen en la aplicación de tecnologías sofisticadas. Estas tecnologías permitirán a las UIF cotejar sus datos con los de otras UIF de forma anónima garantizando una protección plena de los datos personales, con el fin de detectar sujetos de interés para las UIF en otros Estados miembros e identificar sus ingresos y fondos.

Artículo 54

Los Estados miembros velarán por que sus UIF cooperen con Europol en relación con los análisis efectuados que tengan una dimensión transfronteriza y afecten al menos a dos Estados miembros.

SECCIÓN 4

SANCIONES

Artículo 55

1. Los Estados miembros velarán por que a las entidades obligadas pueda imputárseles responsabilidad cuando incumplan las disposiciones de Derecho nacional adoptadas de conformidad con la presente Directiva.

2. Sin perjuicio de su derecho a imponer sanciones penales, los Estados miembros velarán por que las autoridades competentes puedan adoptar las medidas administrativas apropiadas e imponer sanciones administrativas a las entidades obligadas que incumplan las disposiciones nacionales adoptadas para dar cumplimiento a la presente Directiva y garantizarán su aplicación. Esas medidas y sanciones deberán ser efectivas, proporcionadas y disuasorias.

3. Los Estados miembros velarán por que, cuando las obligaciones sean aplicables a personas jurídicas, puedan aplicarse sanciones a los miembros del órgano de dirección o a cualquier otra persona física que, en virtud del Derecho nacional, sea responsable del incumplimiento de las disposiciones.

4. Los Estados miembros velarán por que las autoridades competentes dispongan de todas las facultades de investigación necesarias para el ejercicio de sus funciones. Al ejercer sus facultades sancionadoras, las autoridades competentes cooperarán estrechamente para garantizar que las sanciones o medidas administrativas ofrezcan los resultados deseados y coordinen su actuación en los casos transfronterizos.

Artículo 56

1. El presente artículo se aplicará como mínimo a las situaciones en que se demuestre que las entidades obligadas incumplen sistemáticamente los requisitos previstos en los artículos siguientes:

(a) artículos 9 a 23 (diligencia debida con respecto al cliente);

(b) artículos 32, 33 y 34 (notificación de las transacciones sospechosas);

(c) artículo 39 (conservación de documentos); y

(d) artículos 42 y 43 (controles internos).

2. Los Estados miembros velarán por que, en los casos a que se refiere el apartado 1, entre las sanciones y medidas administrativas aplicables se cuenten como mínimo las siguientes:

(a) una declaración pública que indique la persona física o jurídica y la naturaleza del incumplimiento;

(b) un requerimiento dirigido a la persona física o jurídica para que ponga fin a su conducta y se abstenga de repetirla;

(c) en el caso de una entidad obligada sujeta a autorización, retirada de la autorización;

(d) la imposición de una prohibición temporal de ejercer funciones en entidades a alguno de los miembros del órgano de dirección de la entidad obligada;

(e) si se trata de una persona jurídica, sanciones pecuniarias administrativas de hasta el 10 % de su volumen de negocios total en el ejercicio anterior;

(f) si se trata de una persona física, sanciones pecuniarias administrativas de hasta 5 000 000 EUR o, en los Estados miembros en los que el euro no sea la moneda oficial, el valor correspondiente en la moneda nacional en la fecha de entrada en vigor de la presente Directiva;

(g) sanciones pecuniarias administrativas de hasta el doble del importe de los beneficios obtenidos o de las pérdidas evitadas gracias al incumplimiento, en caso de que puedan determinarse.

A efectos de la letra e), cuando la persona jurídica sea una filial de una empresa matriz, el volumen de negocios total anual pertinente será el volumen de negocios total anual resultante de las cuentas consolidadas de la empresa matriz última en el ejercicio anterior.

Artículo 57

1. Los Estados miembros velarán por que toda sanción o medida que las autoridades competentes impongan por incumplir las disposiciones nacionales adoptadas en aplicación de la presente Directiva se publique sin demora indebida, en particular la información sobre el tipo y la naturaleza del incumplimiento y la identidad de las personas responsables del mismo, a menos que dicha publicación pudiera comprometer gravemente la estabilidad de los mercados financieros. Cuando la publicación pudiera causar un daño desproporcionado a las partes implicadas, las autoridades competentes publicarán las sanciones de manera anónima.

2. Los Estados miembros velarán por que, a la hora de determinar el tipo de sanciones o medidas administrativas y el nivel de las sanciones pecuniarias administrativas, las autoridades competentes tengan en cuenta todas las circunstancias pertinentes, entre ellas:

(a) la gravedad y duración del incumplimiento;.

(b) el grado de responsabilidad de la persona física o jurídica responsable;

(c) la solidez financiera de la persona física o jurídica responsable, reflejada en su volumen de negocios total o en sus ingresos anuales;

(d) la importancia de los beneficios obtenidos o las pérdidas evitadas por la persona física o jurídica responsable, en la medida en que puedan determinarse;

(e) las pérdidas para terceros causadas por el incumplimiento, en la medida en que puedan determinarse;

(f) el nivel de cooperación de la persona física o jurídica responsable con la autoridad competente;

(g) anteriores incumplimientos de la persona física o jurídica responsable.

3. La ABE, la AESPJ y la AEVM emitirán directrices dirigidas a las autoridades competentes de conformidad con el artículo 16 del Reglamento (UE) nº 1093/2010, del Reglamento (UE) nº 1094/2010 y del Reglamento (UE) nº 1095/2010 en relación con los tipos de medidas y sanciones administrativas y el nivel de las sanciones pecuniarias administrativas aplicables a las entidades obligadas contempladas en el artículo 2, apartado 1, puntos 1 y 2. Estas directrices se emitirán en un plazo de dos años a partir de la fecha de entrada en vigor de la presente Directiva.

4. En el caso de las personas jurídicas, los Estados miembros garantizarán que se les pueda imputar responsabilidad por los incumplimientos a que se refiere el artículo 56, apartado 1, cuando los cometa en su provecho, actuando a título individual o como parte de un órgano de la persona jurídica, cualquier persona que en el seno de dicha persona jurídica ostente un cargo directivo que suponga:

   (a) poder de representación de dicha persona jurídica;

   (b) autoridad para tomar decisiones en nombre de dicha persona jurídica; o

   (c) autoridad para ejercer control en el seno de dicha persona jurídica.

5. Sin perjuicio de los casos ya previstos en el apartado 4, los Estados miembros velarán por que a las personas jurídicas pueda imputárseles responsabilidad cuando la falta de vigilancia o control por parte de una de las personas a que se refiere el apartado 4 haya hecho posible que una persona sometida a su autoridad cometa por cuenta de la persona jurídica una de las infracciones mencionadas en el artículo 56, apartado 1.

Artículo 58

1. Los Estados miembros velarán por que las autoridades competentes establezcan mecanismos eficaces para alentar la notificación a las autoridades competentes del incumplimiento de las disposiciones nacionales de aplicación de la presente Directiva.

2. Los mecanismos contemplados en el apartado 1 incluirán, como mínimo:

   (a) procedimientos específicos para la recepción de informes sobre incumplimientos y su seguimiento;

   (b) protección adecuada de los empleados de las entidades que notifiquen incumplimientos cometidos en la entidad;

   (c) la protección de los datos personales relativos tanto a las personas que notifican un incumplimiento como a la persona física presuntamente responsable del mismo, de conformidad con los principios establecidos en la Directiva 95/46/CE.

3. Los Estados miembros exigirán a las entidades obligadas que dispongan de procedimientos adecuados para que sus empleados puedan comunicar incumplimientos a nivel interno a través de un canal específico, independiente y anónimo.

CAPÍTULO VII

DISPOSICIONES FINALES

Artículo 59

En un plazo de cuatro años a partir de la fecha de entrada en vigor de la presente Directiva, la Comisión elaborará un informe sobre la aplicación de la presente Directiva y lo presentará al Parlamento Europeo y al Consejo.

Artículo 60

Quedan derogadas las Directivas 2005/60/CE y 2006/70/CE con efecto a partir del [*insertar fecha - día siguiente a la fecha establecida en el artículo 61, párrafo primero*].

Las referencias a las Directivas derogadas se entenderán hechas a la presente Directiva con arreglo a la tabla de correspondencias que figura en el anexo IV.

Artículo 61

1. Los Estados miembros pondrán en vigor las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva a más tardar [*dos años desde su adopción*]. Comunicarán inmediatamente a la Comisión el texto de dichas disposiciones.

   Cuando los Estados miembros adopten dichas disposiciones, estas incluirán una referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia.

2. Los Estados miembros comunicarán a la Comisión el texto de las principales disposiciones de Derecho interno que adopten en el ámbito regulado por la presente Directiva.

Artículo 62

La presente Directiva entrará en vigor el vigésimo día siguiente al de su publicación en el *Diario Oficial de la Unión Europea*.

Artículo 63

Los destinatarios de la presente Directiva serán los Estados miembros.

Hecho en Estrasburgo, el

Por el Parlamento Europeo
El Presidente

Por el Consejo
El Presidente

N. de la R.: La documentació que acompanya aquesta proposta pot ésser consultada a l'Arxiu del Parlament.

Tramesa a la Comissió

Comissió competent: Comissió d'Economia, Finances i Pressupost.
Acord: Mesa del Parlament, 12.02.2013.

Termini de formulació d'observacions

Termini: 4 dies hàbils (del 19.02.2013 al 22.02.2013).
Finiment del termini: 25.02.2013; 09:30 h.
Acord: Mesa del Parlament, 12.02.2013.

——

Control del principi de subsidiarietat amb relació a la Proposta de directiva del Parlament Europeu i del Consell relativa a la protecció penal de l'euro i d'altres monedes contra la falsificació i per la qual se substitueix la Decisió marc 2000/383/JAI del Consell
Tram. 295-00015/10

Text presentat
Tramesa de la Secretaria de la Comissió Mixta de la Unió Europea del 12.02.2013
Reg. 2569 / Admissió a tràmit: Presidència del Parlament, 13.02.2013

Asunto: Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección penal del euro y otras monedas frente a la falsificación, y por la que se sustituye la Decisión marco 2000/383/JAI del Consejo [COM(2013) 42 final] [2013/0023 (COD)] {SWD(2013) 19 final} {SWD(2013) 20 final}

En aplicación del artículo 6.1 de la Ley 8/1994, de 19 de mayo, la Comisión Mixta para la Unión Europea remite a su Parlamento, por medio del presente correo electrónico, la iniciativa legislativa de la Unión Europea que se acompaña, a efectos de su conocimiento y para que, en su caso, remita a las Cortes Generales un dictamen motivado que exponga las razones por las que considera que la referida iniciativa de la Unión Europea no se ajusta al principio de subsidiariedad.

Aprovecho la ocasión para recordarle que, de conformidad con el artículo 6.2 de la mencionada Ley 8/1994, el dictamen motivado que, en su caso, apruebe su Institución debería ser recibido por las Cortes Generales en el plazo de cuatro semanas a partir de la remisión de la iniciativa legislativa europea.

Con el fin de agilizar la transmisión de los documentos en relación con este procedimiento de control del principio de subsidiariedad, le informo que se ha habilitado el siguiente correo electrónico de la Comisión Mixta para la Unión Europea: cmue@congreso.es

Secretaría de la Comisión Mixta para la Unión Europea

Estrasburgo, 5.2.2013
COM(2013) 42 final
2013/0023 (COD)

Propuesta de

DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativa a la protección penal del euro y otras monedas frente a la falsificación, y por la que se sustituye la Decisión marco 2000/383/JAI del Consejo

{SWD(2013) 19 final}
{SWD(2013) 20 final}

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

1.1. Contexto general

La falsificación del euro y otras monedas sigue siendo una preocupación en toda la Unión Europea. Es fundamental garantizar la confianza de los ciudadanos, las empresas y las entidades financieras en la autenticidad de los billetes y monedas. Las falsificaciones perjudican a los ciudadanos y a las empresas, ya que aquellas no les son reembolsadas aunque las hayan recibido de buena fe. También reduce la aceptabilidad de los billetes y monedas.

La falsificación del euro resulta especialmente preocupante debido a su importancia. El euro es la moneda única compartida por los 17 Estados miembros de la zona del euro y utilizada en ella por 330 millones de personas. Se utiliza también a gran escala en las transacciones comerciales internacionales y sirve a terceros países de importante moneda de reserva. El valor de los billetes de euro que circulan en todo el mundo, que en enero de 2013 asciende casi a 913 000 millones EUR, equivale aproximadamente al de los billetes de dólar. Cerca de un cuarto de ese valor circula fuera de la zona del euro, en particular en las regiones limítrofes[1]. Hoy el euro es la segunda moneda internacional más importante del mundo.

El euro sigue siendo un objetivo de los grupos de delincuencia organizada dedicados a la falsificación de dinero. La falsificación del euro ha causado un perjuicio financiero de al menos 500 millones EUR desde su introducción en 2002. Las cifras del Banco Central Europeo (BCE) muestran picos en el número de billetes falsos durante el periodo 2009-2010 y otros dos picos durante el segundo semestre de los años 2011[2] y 2012[3]. El BCE señala un incremento del 11,6 % por lo que se refiere a la cantidad recuperada en la segunda mitad de 2012, frente a los meses anteriores. El informe anual de 2011[4] del Centro Técnico y Científico Europeo (CTCE) evidencia el continuo descubrimiento de nuevos tipos de monedas de euro falsificadas y un fuerte aumento del número de monedas falsas sumamente perfeccionadas. Europol considera que existe una tendencia a largo plazo hacia un incremento de la delincuencia y señala que la amenaza sigue siendo seria[5]. Los recientes decomisos a gran escala de billetes y monedas de euro falsos y el continuo desmantelamiento de imprentas y cecas clandestinas cada año confirman la evaluación de Europol[6].

---

1 Véase la página del Banco Central Europeo (BCE): http://www.ecb.int/press/key/date/2013/html/sp130110.en.html (únicamente en inglés).

2 Informe anual de 2011 del BCE.

3 Comunicado de prensa del BCE de 10 de enero de 2013: http://www.ecb.int/press/pr/date/2013/html/pr130110_2.fr.html.

4 The Protection of Euro Coins in 2011. Situation as regards euro coins counterfeiting and the activities of the European Technical and Scientific Centre (ETSC) based on Article 4 of Commission Decision C (2004) 4290 of 29 October 2004 [La protección de las monedas de euro en 2011. Situación de la falsificación de las monedas de euro y de las actividades del Centro Técnico y Científico Europeo (CTCE) sobre la base del artículo 4 de la Decisión C(2004) 4290 de 29 de octubre de 2004].

5 Europol, Evaluación de la Amenaza de la Delincuencia Organizada de la UE en 2011 (OCTA 2011).

6 Véanse, por ejemplo, los comunicados de prensa de Europol de 13 de diciembre de 2011, 15 y 29 de junio de 2012, 13 de agosto de 2012 y 9 de diciembre de 2012 en: https://www.europol.europa.eu/latest_press_releases.

Estos elementos muestran que las medidas que combaten actualmente la falsificación no han alcanzado el nivel de disuasión necesario y, por lo tanto, evidencian la necesidad de una mejora de la protección frente a las falsificaciones. En particular, existen diferencias considerables en cuanto a los niveles de sanción aplicables en los Estados miembros a las principales formas de falsificación, a saber, la fabricación y distribución de moneda falsa[7]. Si bien es cierto que el nivel mínimo de la pena máxima aplicable a la fabricación de moneda falsa se armonizó en el año 2000, fijándose en ocho años de prisión, la situación es distinta por lo que se refiere al nivel mínimo de las penas aplicables a la falsificación de moneda. En algunos Estados miembros no hay penas mínimas, o las disposiciones legales sólo contemplan multas, mientras que en otros la pena mínima se eleva a nada menos que diez años de prisión. Estas diferencias son perjudiciales para la aplicación transfronteriza de la ley y la cooperación judicial[8]. Por otra parte, los datos recogidos en el marco de un estudio del «Grupo de expertos sobre falsificación del euro»[9] indican que en los últimos nueve años se han descubierto numerosas imprentas clandestinas en los Estados miembros que no tienen penas mínimas o solo aplican multas como pena mínima a la falsificación de moneda, lo que hace suponer que los falsificadores buscan un foro de conveniencia (*forum shopping*). Por último, la ausencia actual de unos niveles mínimo y máximo para las penas aplicables a los delitos de distribución constituye una peligrosa amenaza por lo que respecta a la distribución, en la Unión Europea, de billetes falsos fabricados en terceros países, como lo demuestra el elevado número de imprentas desmanteladas en terceros países (en Colombia y en Perú, por ejemplo) y el correspondiente decomiso de importantes cantidades de euros y otras monedas falsas listas para ser exportadas a la Unión Europea o distribuidas en su territorio. Se puede, pues, concluir que las notables diferencias actuales entre los sistemas punitivos de los Estados miembros tienen un impacto negativo en la protección penal del euro y otras monedas frente a su falsificación.

El actual nivel de sanciones es una de las razones del insuficiente efecto disuasorio y de la desigualdad de la protección de la moneda en el conjunto de la Unión Europea. El nivel máximo de las penas es un instrumento que permite a los jueces y fiscales determinar la pena que debe imponerse a los delincuentes, pero es un instrumento incompleto sin la fijación de un nivel mínimo. Como la norma mínima de pena máxima se aplica raramente en la práctica, una pena mínima puede considerarse más disuasoria y resultar de un gran valor práctico para la protección del euro. El conocimiento de las posibles penas ejercerá un efecto disuasorio sobre quienes se sientan tentados de falsificar euros; la diferencia entre ser condenado a una pena de prisión de una duración mínima en vez de a pagar una multa, por ejemplo, es obvia. Así, las penas mínimas contribuyen a la institución de un sistema coherente a nivel de la UE para la protección del euro.

El euro es la moneda única de la unión económica y monetaria establecida por la Unión Europea. Es, en este sentido, un auténtico «bien» común que debe ser protegido de manera coherente en toda la Unión Europea, estableciendo, en particular, un nivel mínimo de penas aplicables a los casos graves de fabricación y distribución ilegales.

La Unión Europea y los Estados miembros deberían garantizar una protección global del euro y perseguir los delitos contra el euro sobre una base común. De acuerdo con el Convenio internacional para la represión de la falsificación de moneda (en lo sucesivo, «el Convenio de Ginebra»)[10] y del principio de no discriminación de otras monedas contemplado en su artículo 5, todas las monedas se beneficiarán de esta mayor protección del euro.

1.2. Contexto legal

1.2.1. Derecho penal

El Convenio de Ginebra establece unas normas encaminadas a garantizar que puedan imponerse severas sanciones penales y de otro tipo para los delitos de falsificación. Contiene asimismo normas relativas a la competencia judicial y a la cooperación. A raíz de la ratificación del Convenio de Ginebra adoptado el 20 de abril de 1929, se ha venido registrando un cierto grado de aproximación de las legislaciones nacionales contra la falsificación.

La Decisión marco 2000/383/JAI del Consejo sobre el fortalecimiento de la protección, por medio de sanciones penales y de otro tipo, contra la falsificación de moneda con miras a la introducción del euro[11] tiene por objeto completar, en el territorio de la Unión Europea, las disposiciones del Convenio de Ginebra de 1929. Recoge las prácticas que deben considerarse punibles, aparte de la falsificación propiamente dicha, como la distribución. Para estos delitos, la Decisión marco exige sanciones penales efectivas, proporcionadas y disuasorias. Además, contiene disposiciones en materia de competencia judicial y responsabilidad de las personas jurídicas. La citada Decisión fue

---

7 Anexo 6 de la evaluación de impacto, cuadro con las sanciones vigentes en los Estados miembros desde abril de 2011, según los datos del Bundesbank alemán.

8 Véase la sección 3.2.1.3 de la evaluación de impacto y su anexo 3.

9 Este estudio se centra en los 15 Estados miembros siguientes: Alemania, Bulgaria, Dinamarca, España, Finlandia, Francia, Grecia, Hungría, Italia, Letonia, Países Bajos, Polonia, Portugal, Rumania y Suecia.

10 N° 2623, p. 372. Serie de Tratados de la Sociedad de Naciones, 1931. Este Convenio ha sido ratificado por 26 Estados miembros. Malta (todavía) no lo ha ratificado.

11 DO L 140 de 14.6.2000, p. 1.

modificada por la Decisión marco 2001/888/JAI del Consejo, de 6 de diciembre de 2001[12], que introduce una disposición relativa al reconocimiento mutuo de las condenas a los efectos del reconocimiento de los casos de «reincidencia».

Los Estados miembros tenían que transponer la Decisión marco 2000/383/JAI del Consejo a más tardar el 29 de mayo de 2001 y la Decisión marco 2001/888/JAI del Consejo, a más tardar el 31 de diciembre de 2002. La Comisión ha evaluado su aplicación en tres informes[13]. Pese al desarrollo del acervo de la Unión en este ámbito, se han constatado algunas deficiencias. Aunque todos los Estados miembros, con muy pocas excepciones, han aplicado formalmente la Decisión marco de forma correcta, en la práctica han adoptado normas divergentes, lo que ha resultado a menudo en grados de protección y prácticas también divergentes en sus respectivos ordenamientos jurídicos.

1.2.2. Otras disposiciones de la Unión en este ámbito

La Decisión marco forma parte de un corpus jurídico más amplio que incluye también medidas administrativas y de formación, como:

- El Reglamento (CE) n° 974/98 del Consejo, de 3 de mayo de 1998, sobre la introducción del euro[14]. Este Reglamento impone a los Estados miembros de la zona del euro aplicar sanciones adecuadas contra la falsificación de los billetes y monedas de euro.
- El Reglamento (CE) n° 1338/2001 del Consejo, de 28 de junio de 2001, por el que se definen las medidas necesarias para la protección del euro contra la falsificación[15], actualizado por el Reglamento (CE) n° 44/2009 del Consejo, de 18 de diciembre de 2008[16]. Este Reglamento regula la forma en que los billetes y monedas de euro pueden ser puestos en circulación, para protegerlos frente a la falsificación. Por otra parte, aborda cuestiones tales como la recopilación y acceso a los datos técnicos y estadísticos relativos a los billetes y monedas falsificados, su examen por parte de los Centros Nacionales de Análisis de Monedas, las obligaciones de las entidades de crédito y la centralización de la información a nivel nacional. El Reglamento (CE) n° 1339/2001 del Consejo, de 28 de junio de 2001[17], ha extendido los efectos del Reglamento (CE) n° 1338/2001 a los Estados miembros que no han adoptado el euro como moneda única.
- La Decisión del Banco Central Europeo, de 16 de septiembre de 2010, sobre la comprobación de la autenticidad y aptitud de los billetes en euros y sobre su recirculación (ECB/2010/14)[18].
- El Reglamento (UE) n° 1210/2010 del Parlamento Europeo y del Consejo, de 15 de diciembre de 2010, relativo a la autentificación de las monedas de euros y el tratamiento de las monedas de euros no aptas para la circulación[19].
- El Reglamento (CE) n° 2182/2004 del Consejo, de 6 de diciembre de 2004, sobre medallas y fichas similares a monedas de euro[20], modificado por el Reglamento (CE) n° 46/2009 del Consejo, de 18 de diciembre de 2008[21].
- La Decisión 2005/511/JAI del Consejo, de 12 de julio de 2005, relativa a la protección del euro contra la falsificación mediante la designación de Europol como organismo central para la lucha contra la falsificación del euro[22].
- Decisión 2002/187/JAI del Consejo, de 28 de febrero de 2002, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia mediante el fomento y la mejora de la coordinación y la cooperación entre las autoridades judiciales competentes de los Estados miembros, inclusive en el ámbito de la falsificación del euro[23];

---

12 DO L 329 de 14.12.2001, p. 3.
13 El primer informe fue adoptado en diciembre de 2001 [COM(2001) 771 final]; el segundo informe, en septiembre de 2003 [COM(2003) 532 final]; y el tercer informe, en septiembre de 2007 [COM(2007) 524 final].
14 DO L 139 de 11.5.1998, p.1.
15 DO L 181 de 4.7.2001, p. 6.
16 DO L 17 de 22.1.2009, p. 1.
17 DO L 181 de 4.7.2001, p. 11.
18 DO L 267 de 9.10.2010, p.1.
19 DO L 339 de 22.12.2010, p.1.
20 DO L 373 de 21.12.2004, p. 1.
21 DO L 17 de 22.1.2009, p. 5.
22 DO L 185 de 17.7.2005, p. 35.
23 DO L 63 de 6.3.2002, p.1.

- A través del programa Pericles, instituido en virtud de la Decisión 2001/923/CE del Consejo, de 17 de diciembre de 2001[24], la Unión financia varias acciones específicas centradas en los intercambios y en la asistencia y formación de agentes del orden para establecer unos vínculos profesionales más estrechos que permitan luchar más eficazmente contra la falsificación del euro.

2. RESULTADOS DE LAS CONSULTAS CON LAS PARTES INTERESADAS Y DE LAS EVALUACIONES DE IMPACTO

2.1. Consulta de las partes interesadas

La Comisión ha consultado a las partes interesadas especializadas en varias ocasiones. Esa consulta comenzó en la 58ª reunión del «Grupo de expertos sobre falsificación del euro»[25] (ECEG, por sus siglas en inglés) el 10 de noviembre de 2011 y prosiguió en otras reuniones de dicho grupo. También se consultó a expertos y especialistas[26] en el marco de la Conferencia de La Haya, que se celebró del 23 al 25 de noviembre de 2011. El 20 de diciembre de 2011 se envió a los Estados miembros un cuestionario sobre la aplicación de la Decisión marco. Los resultados de este cuestionario y una posible línea de actuación de cara al futuro se examinaron en la 59ª reunión del ECEG de 14 de marzo y en su 60ª reunión de 13 de junio de 2012. El BCE y Europol participaron en este proceso mediante aportaciones que consistieron, en particular, en contribuciones directas dirigidas a la Comisión.

De la consulta, puede concluirse que las partes interesadas consideran necesario proporcionar un valor añadido a los profesionales del ramo para la protección del euro y otras monedas a través de medidas penales. Se recibieron dos propuestas concretas con relación a la mejora del Derecho penal procesal: la propuesta de alinear las técnicas de investigación como las entregas vigiladas o los agentes infiltrados; y la propuesta de introducir disposiciones que obliguen a las autoridades judiciales a transmitir las muestras de monedas falsificadas incautadas para su análisis técnico con vistas a detectar ulteriores falsificaciones en circulación.

El BCE se ha mostrado firmemente partidario de reforzar el marco jurídico penal, en particular mediante el endurecimiento y la armonización de las penas, lo que incluye el establecimiento de penas mínimas.

2.2. Evaluación de impacto

La Comisión llevó a cabo una evaluación de impacto de las alternativas políticas, teniendo en cuenta las consultas de las partes interesadas. Tras considerar las posibles opciones, la evaluación de impacto concluye que la siguiente solución parece preferible:

– Mantenimiento de la mayor parte de las disposiciones de la Decisión marco 2000/383/JAI del Consejo mediante su incorporación en una nueva propuesta, con modificaciones menores, teniendo en cuenta el Tratado de Lisboa.

– Modificación de las disposiciones en materia de penas con la introducción de una pena mínima de seis meses para la fabricación y distribución de moneda falsa y de una pena máxima de al menos ocho años para la distribución.

– Introducción de una nueva disposición que obligue a los Estados miembros a contemplar la posibilidad de utilizar ciertas herramientas de investigación.

– La introducción de una nueva disposición que obligue a los Estados miembros a garantizar que los Centros Nacionales de Análisis y los Centros Nacionales de Análisis de Moneda puedan igualmente analizar las falsificaciones de euro durante los procesos judiciales en curso a los efectos de detectar ulteriores falsificaciones.

---

24 DO L 339 de 21.12.2001, p. 50. Para una actualización referente al programa, véase la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establece un programa en materia de intercambios, asistencia y formación para la protección del euro contra la falsificación de moneda [COM(2011) 913 final].

25 El ECEG se instituyó en virtud del Reglamento (CE) n° 1338/2001 y está compuesto por expertos de los Estados miembros, del BCE, de Europol y de la OLAF/CTCE.

26 Representantes de las fuerzas de seguridad, de las autoridades judiciales y de los bancos centrales y cecas nacionales.

3. ASPECTOS JURÍDICOS DE LA PROPUESTA

3.1. Base jurídica

La competencia de la UE para establecer «normas mínimas relativas a la definición de las infracciones penales y de las sanciones en ámbitos delictivos que sean de especial gravedad y tengan una dimensión transfronteriza derivada del carácter o de las repercusiones de dichas infracciones o de una necesidad particular de combatirlas según criterios comunes» se establece en el artículo 83, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE).

La falsificación de los medios de pago se menciona explícitamente en el apartado 1 del artículo 83 TFUE como ámbito delictivo de especial gravedad.

3.2. Subsidiariedad, proporcionalidad y respeto de los derechos fundamentales

Se considera que existe la necesidad de una acción de la UE basada en los siguientes factores:

La falsificación del euro y otras monedas plantea un verdadero problema a la Unión y a sus ciudadanos, empresas y entidades financieras. El hecho de que el euro sea la moneda única de la zona del euro nos lleva a considerar que el delito de falsificación del euro causa el mismo perjuicio en toda la zona del euro, independientemente del lugar en que se haya perpetrado. Esta dimensión paneuropea exige que la falsificación se combata de forma similar y que a los delincuentes se les apliquen penas equivalentes independientemente del país de la Unión Europea en que se haya cometido el delito.

Esta posición particular del euro, que es la moneda única de la unión económica y monetaria establecida por la Unión Europea, y, por lo tanto, un verdadero «bien» europeo, exige que su protección se garantice en toda la UE. Como tal, es un ámbito más eurocéntrico, incluso, que cualquier ámbito sujeto a una armonización normativa en los Estados miembros.

Sólo la UE está en condiciones de desarrollar una legislación vinculante aplicable en todos los Estados miembros y, por lo tanto, de crear un marco legal que contribuya a superar las deficiencias de la actual situación.

De conformidad con el artículo 5 del Convenio de Ginebra, «no deberán establecerse, desde el punto de vista de las sanciones, distinción entre los hechos según se trate de una moneda nacional o de una moneda extranjera.» Así pues, la mayor protección del euro debería extenderse a todas las monedas.

Las penas propuestas son proporcionales a la gravedad de los delitos y al considerable impacto de la falsificación del euro y otras monedas en los ciudadanos y empresas. Además, están en consonancia con las sanciones actualmente previstas en la legislación de la mayoría de los Estados miembros. Dado que muchos Estados miembros ya contemplan el concepto de penas mínimas, es apropiado y coherente utilizarlo a nivel de la Unión. Con el fin de garantizar que la severidad de las penas no sea desproporcionada con respecto al delito, se ha añadido una cláusula de salvaguardia específica para los casos de falsificación de monedas y billetes menores, es decir, un primer umbral por debajo del cual puede imponerse una pena de prisión menos larga y un segundo umbral por debajo del cual puede asimismo imponerse una multa, a menos que concurran en el caso circunstancias especialmente graves. Esto ocurre, por ejemplo, cuando el dinero falso se descubre en circunstancias que permiten claramente suponer que se han fabricado o iban a fabricarse cantidades más importantes. Los umbrales elegidos deben ser lo suficientemente altos como para tener en cuenta los casos de menor importancia, y al mismo tiempo lo suficientemente bajos como para garantizar el efecto disuasorio de la pena y tener en cuenta la importancia de la autenticidad de los billetes y monedas y la confianza que los ciudadanos depositan en ellos.

La presente Directiva impone a los Estados miembros la obligación de incluir en sus legislaciones nacionales la escala de sanciones contemplada en el artículo 5, no situándose por debajo de los niveles mínimos exigidos. No obstante, siguen siendo aplicables los principios y normas generales del Derecho penal nacional sobre aplicación y ejecución de las sentencias según las circunstancias concretas. Se trata, en particular, de las normas generales relativas a la aplicación de las penas a los menores de edad, a los casos de tentativa, a los casos de simple apoyo a la participación o a los casos en que el autor del delito contribuye al descubrimiento o a la prevención de delitos graves. Por lo que se refiere a la ejecución de las penas, seguirán aplicándose los principios generales relativos, en particular, a las penas privativas de libertad con suspensión de la ejecución, a las penas alternativas a la privación de libertad (vigilancia electrónica) o a la excarcelación anticipada. En cada caso concreto, los tribunales ejercerán su facultad discrecional teniendo en cuenta todas las circunstancias agravantes y atenuantes dentro del marco legal aplicable.

Cada una de las medidas jurídico penales propuestas ha sido evaluada y diseñada cuidadosamente teniendo en cuenta sus posibles efectos en la protección de los derechos fundamentales.

La propuesta afecta a los siguientes derechos y principios de la Carta de los Derechos Fundamentales de la UE (en lo sucesivo, la Carta): el derecho a la libertad y la vida familiar (mediante el posible encarcelamiento de los infractores condenados), el derecho a elegir libremente una profesión y a dirigir una empresa (mediante la posible inhabilitación de los infractores condenados), el derecho a la propiedad (mediante el posible cierre de las empresas que hayan

cometido el delito), el principio de legalidad y proporcionalidad de los delitos y penas (mediante la definición de los delitos y la escala de penas), el derecho a no ser juzgado dos veces (mediante la interacción con los regímenes de sanciones administrativas). Estas interferencias están justificadas por cuanto permiten alcanzar los objetivos de interés general reconocidos por la Unión (véase el artículo 52, apartado 1, de la Carta), y, en particular, ofrecer medidas efectivas y disuasorias para la protección del euro y otras monedas. Se ha procurado cuidadosamente que las medidas no excedan de lo que es necesario para alcanzar este objetivo y sean, por lo tanto, proporcionadas. En particular, se han establecido varias salvaguardias explícitas en el propio instrumento que especifican el derecho a la tutela judicial efectiva y a un juez imparcial, incluido el derecho a la defensa, y garantizan un nivel equivalente de protección judicial efectiva por los tribunales nacionales. Las penas propuestas son proporcionales a los delitos cometidos.

3.3. Instrumentos elegidos

La directiva es el instrumento adecuado para establecer disposiciones de Derecho penal sobre la base del artículo 83, apartado 1, del TFUE.

3.4. Disposiciones específicas

Artículo 1: Contenido - esta disposición facilita una descripción del ámbito y propósito de la propuesta.

Artículo 2: Definiciones - esta disposición establece definiciones que se aplican en todo el instrumento.

Artículo 3: Delitos - esta disposición define los principales delitos que los Estados miembros deben tipificar y aclara que determinadas circunstancias de la comisión del delito entran en su ámbito de aplicación.

Artículo 4: Instigación, Complicidad y Tentativa - esta disposición es aplicable a todos los delitos anteriormente mencionados y requiere que los Estados miembros tipifiquen como delito todas las formas de preparación y participación. Se incluye la responsabilidad penal de la tentativa para la mayoría de los delitos.

Artículo 5: Sanciones – esta disposición se aplica a todos los delitos mencionados en los artículos 3 y 4. Impone a los Estados miembros la obligación de aplicar sanciones efectivas, proporcionadas y disuasorias con arreglo a la jurisprudencia del Tribunal de Justicia. Para los casos más graves de los delitos de fabricación y distribución de falsa moneda, prevé una pena de privación de libertad que va de como mínimo seis meses a ocho años para las personas físicas. El nivel mínimo de una pena máxima de ocho años ya se establece en la Decisión marco 2000/383/JAI para el delito de fabricación.

Artículos 6 y 7: Responsabilidad de las personas jurídicas y tipos de sanciones aplicables – estas disposiciones son aplicables a todos los delitos mencionados en los artículos 3 y 4. Imponen a los Estados miembros la obligación de garantizar la responsabilidad de las personas jurídicas, impidiendo que dicha responsabilidad constituya una alternativa a la de las personas físicas, y de aplicar penas efectivas, proporcionadas y disuasorias a las personas jurídicas, y exponen las posibles penas.

Artículo 8: Jurisdicción: esta disposición se basa en los principios de territorialidad y personalidad. Es aplicable a todos los delitos mencionados en los artículos 3 y 4. Requiere la existencia de una base de competencias que permita a las autoridades judiciales iniciar investigaciones, entablar acciones judiciales y llevar ante los tribunales los casos relativos a la falsificación. Obliga a los Estados miembros cuya moneda es el euro a ejercer una jurisdicción universal sobre los delitos de falsificación del euro, en determinadas condiciones. En los casos de procesos paralelos, la Decisión marco 2009/948/JAI del Consejo, de 30 de noviembre de 2009, sobre la prevención y resolución de conflictos de ejercicio de jurisdicción en los procesos penales[27], aboga por una mayor cooperación entre las autoridades competentes. De conformidad con lo dispuesto en la Decisión 2002/187/JAI del Consejo, de 28 de febrero de 2002, el miembro nacional de Eurojust deberá ser informado de cualquier caso en que se hayan planteado o puedan plantearse conflictos de competencia. Por otra parte, el artículo 8 de la presente Directiva impone a los Estados miembros la obligación de concentrar los procesos penales en un único Estado miembro, a menos que sea improcedente.

Artículo 9: Instrumentos de investigación – esta disposición tiene por objeto garantizar que los instrumentos de investigación previstos por la legislación nacional para combatir la delincuencia organizada u otras formas graves de delincuencia puedan igualmente utilizarse en los casos de falsificación de moneda.

Artículo 10: Obligación de transmitir los falsos billetes y monedas de euro a efectos de análisis y detección de falsificaciones – esta disposición impone a los Estados miembros la obligación de garantizar que los Centros Nacionales de Análisis y los Centros Nacionales de Análisis de Moneda puedan igualmente analizar los euros falsificados durante los procesos judiciales en curso con el fin de detectar ulteriores falsificaciones.

Artículo 11: Relación con el Convenio de Ginebra – esta disposición exige que los Estados miembros sean parte contratante del Convenio internacional de Ginebra de 20 de abril de 1929.

---

[27] DO L 328 de 15.12.2009, p.42.

Artículo 12: Sustitución de la Decisión marco 2000/383/JAI del Consejo – esta disposición sustituye a las disposiciones actuales en el ámbito de la falsificación de moneda por lo que se refiere a los Estados miembros que participan en la presente Directiva.

Artículo 13: Transposición – esta disposición exige que los Estados miembros transpongan la Directiva en el plazo de dieciocho meses a partir de su entrada en vigor. Los Estados Miembros deberán comunicar a la Comisión el texto de estas disposiciones y de las disposiciones futuras que se adopten en el ámbito regulado por la presente Directiva. Los Estados miembros no están obligados a transmitir los documentos explicativos por cuanto la Directiva contiene un número limitado de obligaciones legales y se refiere a un ámbito delimitado a nivel nacional.

Artículos 14, 15 y 16 – Estos artículos contienen otras disposiciones relativas a los informes de la Comisión y a la revisión; entrada en vigor y destinatarios.

4. REPERCUSIONES PRESUPUESTARIAS

La presente propuesta no tiene repercusiones presupuestarias para el presupuesto de la Unión Europea.

2013/0023 (COD)

Propuesta de

DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativa a la protección penal del euro y otras monedas frente a la falsificación, y por la que se sustituye la Decisión marco 2000/383/JAI del Consejo

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, su artículo 83, apartado 1,

Vista la propuesta de la Comisión Europea,

Tras haber consultado al Banco Central Europeo,

Previa transmisión del proyecto de acto legislativo a los parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo[28],

De conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

(1) Como moneda única compartida por los Estados miembros de la zona del euro, el euro se ha convertido en un factor importante en la economía de la Unión y en la vida cotidiana de sus ciudadanos. Interesa a la Unión en su conjunto combatir y perseguir cualquier actividad que pueda poner en peligro la autenticidad del euro mediante su falsificación.

(2) El dinero falso tiene un efecto considerablemente nocivo en la sociedad. Perjudica a los ciudadanos y a las empresas, ya que ese dinero no les es reembolsado aunque lo hayan recibido de buena fe. Es fundamental

[28] DO C de..., p. .

garantizar la confianza de los ciudadanos, las empresas y las entidades financieras en la autenticidad de los billetes y monedas.

(3) Es esencial garantizar la protección del euro y de cualquier otra moneda cuya circulación esté legalmente autorizada, de manera adecuada y en todos los Estados miembros, a través de medidas jurídico-penales efectivas y eficientes.

(4) El Reglamento (CE) n° 974/98 del Consejo, de 3 de mayo de 1998, sobre la introducción del euro[29], impone a los Estados miembros cuya moneda única es el euro la obligación de aplicar las sanciones adecuadas en caso de falsificación de billetes y monedas de euro.

(5) Los Reglamentos (CE) n° 1338/2001[30] y (CE) n° 1339/2001[31] del Consejo, de 28 de junio de 2001, establecen las medidas necesarias para la protección del euro frente a la falsificación, y, en particular, las medidas para retirar de la circulación los euros falsificados.

(6) El Convenio internacional para la represión de la falsificación de moneda firmado en Ginebra el 20 de abril de 1929 y su Protocolo (en lo sucesivo, «el Convenio de Ginebra»)[32] establecen normas destinadas a prevenir, perseguir y sancionar el delito de falsificación. Este Convenio tiene más específicamente por objeto garantizar que puedan castigarse los delitos de falsificación con severas sanciones penales y de otro tipo. Todas las partes contratantes del Convenio de Ginebra deben aplicar el principio de no discriminación a las monedas distintas de su moneda nacional.

(7) El propósito de la presente Directiva es complementar las disposiciones y facilitar la aplicación de Convenio de Ginebra por los Estados miembros.

(8) La presente Directiva se basa, actualizándola, en la Decisión marco 2000/383/JAI del Consejo sobre el fortalecimiento de la protección, por medio de sanciones penales y de otro tipo, contra la falsificación de moneda con miras a la introducción del euro[33]. La presente Directiva completa la citada Decisión marco mediante otras disposiciones relativas al nivel de las sanciones y a los instrumentos de investigación, así como al análisis, la identificación y la detección de las falsificaciones durante los procesos judiciales. La Decisión marco debería sustituirse por la presente Directiva con relación a los Estados miembros que participan en su adopción.

(9) La Directiva debería proteger cualquier billete o moneda cuya circulación esté legalmente autorizada, independientemente de si está fabricada en papel, metal o cualquier otro material.

(10) La protección del euro y otras monedas exige una definición común de los delitos relacionados con la falsificación de moneda, así como unos tipos de sanción comunes para las personas tanto físicas como jurídicas. Para garantizar la coherencia con el Convenio de Ginebra, la presente Directiva debería considerar punibles los mismos delitos que el Convenio. Por lo tanto, la fabricación de billetes y monedas falsos y su distribución deberían constituir un delito. El importante trabajo preparatorio de tales delitos, como la producción de instrumentos y componentes para la falsificación, deberían castigarse independientemente. El objetivo común de esas definiciones de delitos debería ser actuar como factor disuasorio de toda manipulación de billetes y monedas falsos y de instrumentos y herramientas para la falsificación.

(11) También debería considerarse falsificación la utilización abusiva de instalaciones o materiales legales, o de imprentas o cecas autorizadas para la fabricación de billetes y monedas no autorizados con fines fraudulentos. Se incluye aquí el supuesto de que un banco central o ceca nacional u otra industria autorizada fabrique billetes o monedas por encima de la cuota fijada por el Banco Central Europeo. Abarca asimismo el supuesto de que un empleado de una imprenta o ceca legal haga un uso abusivo de las instalaciones para sus propios fines. Ese comportamiento debería ser punible como delito de falsificación aunque no se hayan superado las cantidades autorizadas, dado que las falsificaciones serían, una vez en circulación, indistinguibles de los billetes y monedas autorizados.

(12) Los billetes y monedas que el Banco Central Europeo o los bancos centrales y cecas nacionales todavía no hayan emitido oficialmente deberían asimismo beneficiarse de la protección de la presente Directiva. Así por ejemplo, las monedas de euro con nuevas caras nacionales o las nuevas series de billetes de euro deberían recibir protección antes incluso de ser puestas oficialmente en circulación.

---

29 DO L 139 de 11.5.1998, p. 1.
30 DO L 181 de 4.7.2001, p. 6.
31 DO L 181 de 4.7.2001, p. 11.
32 N° 2623, p. 372. Serie de Tratados de la Sociedad de Naciones, 1931.
33 DO L 140 de 14.6.2000, p. 1.

(13) La instigación, la complicidad y la tentativa de cometer los principales delitos de falsificación, incluyendo el uso abusivo de instalaciones o materiales legales y la falsificación de billetes y monedas aún no emitidos pero destinados a ser puestos en circulación, también deberían penalizarse, cuando proceda. La presente Directiva no exige a los Estados miembros la penalización de la tentativa de cometer un delito relacionado con un instrumento o componente del proceso de falsificación.

(14) Las sanciones aplicables a los delitos de falsificación deberían ser efectivas, proporcionadas y disuasorias en toda la Unión.

(15) Tradicionalmente la falsificación de moneda es un delito severamente penado en los Estados miembros. Esto se debe a su gravedad y a su fuerte impacto en los ciudadanos y empresas, así como a la necesidad de garantizar la confianza de los ciudadanos de la Unión en la autenticidad del euro y otras monedas. Esto es especialmente verdad en el caso del euro, que es la moneda única de 330 millones de personas en la zona del euro y la segunda moneda internacional más importante.

(16) Por lo tanto, los Estados miembros deberían contemplar ciertos tipos y niveles mínimos de sanciones. El concepto de penas mínimas existe en la mayoría de los Estados miembros. Es, pues, coherente y apropiado adoptar este enfoque a nivel de la Unión.

(17) Los niveles de las sanciones deben ser efectivos y disuasorios, pero no deben ir más allá de lo que es proporcional a los delitos. La pena aplicable a las personas físicas en los casos graves, es decir, a los principales delitos de fabricación y distribución de moneda falsa que implican una gran cantidad de billetes y monedas falsos o circunstancias especialmente graves, debería, por lo tanto, consistir en una pena mínima de al menos seis meses y en una pena máxima de al menos ocho años de prisión.

(18) La pena mínima de seis meses contribuye a garantizar que las autoridades policiales y judiciales otorgan idéntica prioridad a los delitos de falsificación del euro y otras monedas y, al mismo tiempo, facilita la cooperación transfronteriza. Contribuye a limitar el riesgo de búsqueda de un foro de conveniencia. Además, permite que los delincuentes condenados puedan ser entregados con la ayuda de una orden de detención europea, de forma que la pena privativa de libertad o la orden de detención puedan ser ejecutadas.

(19) Los Estados miembros deberían tener la posibilidad de imponer una pena de prisión breve o de no imponerla en los casos en que el valor nominal total de los billetes y monedas falsos no sea significativo o no concurran circunstancias especialmente graves. Ese valor debería ser inferior a 5 000 EUR, es decir, diez veces la máxima denominación del euro, para los casos en que se aplica una pena distinta de la pena de prisión, e inferior a 10 000 EUR para los casos en que la pena impuesta sea de menos de seis meses.

(20) La presente Directiva se entenderá sin perjuicio de los principios y normas generales del Derecho penal nacional sobre aplicación y ejecución de sentencias de conformidad con las circunstancias concretas de cada caso.

(21) Dado que la confianza en la autenticidad de los billetes y monedas puede también verse dañada o amenazada por el comportamiento de personas jurídicas, éstas deberían responder de los delitos penales cometidos en su nombre.

(22) Para garantizar el éxito de las investigaciones y de la persecución de los delitos de falsificación de moneda, los responsables de investigar y procesar tales delitos deberían tener acceso a las herramientas de investigación utilizadas para combatir la delincuencia organizada u otros delitos graves. Entre esas herramientas figuran, por ejemplo, la interceptación de las comunicaciones, la vigilancia discreta (incluida la electrónica), el control de las cuentas bancarias y otras investigaciones financieras, teniendo en cuenta, entre otras cosas, el principio de proporcionalidad y la naturaleza y gravedad de los delitos investigados.

(23) Los Estados miembros deberían establecer su competencia de acuerdo con el Convenio de Ginebra y las disposiciones sobre determinación de la competencia incluidas en otros actos del Derecho penal de la Unión, a saber, con relación a los delitos cometidos en su territorio y a los delitos cometidos por sus nacionales. El destacado papel del euro para la economía y la sociedad de la Unión Europea, así como la amenaza específica que pesa sobre él como moneda de importancia mundial, exigen nuevas medidas de protección. Por lo tanto, cada Estado miembro que tenga el euro como moneda debería gozar de jurisdicción universal con respecto a los delitos relacionados con el euro cometidos fuera de la Unión Europea tanto si el delincuente se encuentra en su territorio como si los euros falsos relacionados con el delito son detectados en ese Estado miembro. Al ejercer la jurisdicción universal, los Estados miembros deberían respetar el principio de proporcionalidad, en particular con relación a las condenas impuestas por un tercer país por la misma conducta.

(24) La falsificación afecta con frecuencia a varios Estados miembros en paralelo, como por ejemplo en los casos en que la moneda falsa se fabrica en un Estado miembro y se distribuye en otro u otros Estados miembros. En consonancia con los mecanismos establecidos en la Decisión marco 2009/948/JAI del Consejo, de 30 de

noviembre de 2009, sobre la prevención y resolución de conflictos de ejercicio de jurisdicción en los procesos penales, en los casos transfronterizos y a menos que sea improcedente[34], los Estados miembros deberían concentrar las acciones penales, incluido el procesamiento, en un único Estado miembro. Esta concentración se considerará especialmente procedente cuando contribuya a racionalizar la investigación, facilitando, por ejemplo, la obtención de pruebas, o cuando permita al tribunal valorar globalmente la importancia del delito en una condena. De conformidad con lo establecido en la Decisión 2002/187/JAI del Consejo, de 28 de febrero de 2002, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia[35], el miembro nacional de Eurojust deberá ser informado de cualquier caso en que se hayan planteado o puedan plantearse conflictos de competencia.

(25) Por lo que atañe al euro, la identificación de billetes y monedas falsos se centraliza en los Centros Nacionales de Análisis y, respectivamente, en los Centros Nacionales de Análisis de Monedas designados o establecidos de acuerdo con el Reglamento (CE) nº 1338/2001. El análisis, la identificación y la detección de billetes y monedas falsos de euro deberían también poderse hacer durante los procesos judiciales en curso para evitar e impedir que ese tipo de falsificaciones sigan circulando, sin menoscabo del principio del derecho a la tutela judicial efectiva y a un juez imparcial. En general, las autoridades judiciales deberían autorizar la transmisión física de las falsificaciones a los Centros Nacionales de Análisis y a los Centros Nacionales de Análisis de Monedas. En determinadas circunstancias, por ejemplo en los casos en que solo unos pocos billetes o monedas falsos constituyen la prueba del proceso penal o cuando la transmisión física conlleve el riesgo de destrucción de pruebas como las huellas, las autoridades judiciales deberían poder decidir si permiten el acceso a los billetes y monedas.

(26) La presente Directiva respeta los derechos fundamentales y los principios reconocidos, concretamente, en la Carta de los Derechos Fundamentales de la Unión Europea, y en particular, el derecho a la libertad y a la seguridad, el respeto a la vida familiar y privada, la libertad profesional y el derecho a trabajar, el derecho a dirigir una empresa, el derecho a la propiedad, el derecho a la tutela judicial efectiva y a un juez imparcial, la presunción de inocencia y el derecho a la defensa, los principios de legalidad y proporcionalidad de los delitos y penas, así como la prohibición de ser juzgado o condenado penalmente dos veces por la misma infracción. La presente Directiva tiene por objeto garantizar el pleno respeto de tales derechos y principios y debe aplicarse en consecuencia.

(27) Dado que los objetivos de la presente Directiva no pueden alcanzarse de manera suficiente por los Estados miembros de forma individual y, por consiguiente, debido a su dimensión y efectos, pueden lograrse mejor a nivel de la Unión, esta puede adoptar las medidas contempladas en la presente Directiva, de acuerdo con el principio de subsidiariedad consagrado en el artículo 5 del Tratado de la Unión Europea. De acuerdo con el principio de proporcionalidad enunciado en el citado artículo, la presente Directiva no excede de lo necesario para alcanzar dichos objetivos.

(28) De conformidad con el artículo 3 del Protocolo (nº 21) sobre la posición del Reino Unido y de Irlanda respecto del espacio de libertad, seguridad y justicia, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, el Reino Unido e Irlanda han notificado su deseo de participar en la adopción y aplicación de la presente Directiva.

Y/O

(29) De conformidad con los artículos 1 y 2 del Protocolo (nº 21) sobre la posición del Reino Unido y de Irlanda respecto del espacio de libertad, seguridad y justicia, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, y sin perjuicio del artículo 4 del citado Protocolo, el Reino Unido e Irlanda no participan en la adopción y aplicación de la presente Directiva, y no están vinculados por ella ni sujetos a su aplicación.

(30) De conformidad con lo dispuesto en los artículos 1 y 2 del Protocolo (nº 22) sobre la posición de Dinamarca, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, Dinamarca no participa en la adopción de la presente Directiva y no está vinculada por ella ni sujeta a su aplicación.

---

34 DO L 328 de 15.12.2009, pp. 42 a 47.
35 DO L 63, de 6.3.2002, p. 1.

HAN ADOPTADO LA PRESENTE DIRECTIVA:

Artículo 1

Objeto

La presente Directiva establece normas mínimas relativas a la definición de los delitos y sanciones penales en el ámbito de la falsificación del euro y otras monedas. También introduce disposiciones comunes para reforzar la lucha contra esos delitos y mejorar su investigación.

Artículo 2

Definiciones

A efectos de la presente Directiva, se entenderá por:

a) «moneda»: los billetes y monedas cuya circulación está legalmente autorizada, incluidos los billetes de euro y las monedas de euro cuya circulación está legalmente autorizada en virtud del Reglamento (CE) nº 974/98;

b) «persona jurídica»: cualquier entidad que tenga personalidad jurídica con arreglo al Derecho aplicable, con excepción de los Estados u otros organismos públicos en el ejercicio de su potestad pública y de las organizaciones internacionales públicas.

c) «Convenio de Ginebra»: el Convenio internacional para la represión de la falsificación de moneda, firmado en Ginebra el 20 de abril de 1929, y su Protocolo.

Artículo 3

Delitos

1. Los Estados miembros adoptarán las medidas necesarias para asegurarse de que constituyan un delito, cuando se cometan intencionadamente, las siguientes conductas:

   a) cualquier actividad fraudulenta de fabricación o alteración de moneda, independientemente del medio empleado al efecto;

   b) la puesta en circulación fraudulenta de moneda falsa;

   c) la importación, exportación, transporte, recepción u obtención de moneda falsa para ponerla en circulación, a sabiendas de que es falsa;

   d) la fabricación, recepción, obtención o posesión fraudulentas de:

      i) instrumentos, objetos, programas informáticos u otros medios destinados por su naturaleza a la falsificación o alteración de moneda; o

      ii) hologramas u otros componentes de la moneda que sirvan para protegerla contra la falsificación.

2. Dentro de las conductas mencionadas en el apartado 1 se incluye la consistente en fabricar o haber fabricado billetes o monedas utilizando instalaciones o materiales legales infringiendo los derechos o condiciones bajo los cuales las autoridades competentes pueden emitir billetes o monedas.

3. Dentro de las conductas mencionadas en el apartado 1 se incluyen las relacionadas con billetes y monedas no emitidos todavía pero que están destinados a la circulación y son de una moneda que es moneda de curso legal.

Artículo 4

Instigación, complicidad y tentativa

1. Los Estados miembros adoptarán las medidas necesarias para garantizar que la instigación y la complicidad relacionadas con los delitos a que se refiere el artículo 3 estén a su vez tipificadas como delitos.

2. Los Estados miembros adoptarán las medidas necesarias para garantizar que la tentativa de comisión de alguno de los delitos a que se refiere el artículo 3, apartado 1, letras a), b) o c), esté tipificada como delito.

Artículo 5

Sanciones

1. Los Estados miembros adoptarán las medidas necesarias para garantizar que las conductas a que se refieren los artículos 3 y 4 sean punibles con sanciones penales efectivas, proporcionadas y disuasorias, inclusive con multas y penas de prisión.

2. Para los delitos mencionados en el artículo 3, apartado 1, letras a), b) y c), referentes a billetes y monedas de un valor nominal total de menos de 5 000 EUR y en que no concurran circunstancias especialmente graves, los Estados miembros podrán establecer una pena distinta de la pena de prisión.

3. Los delitos mencionados en el artículo 3, apartado 1, letras a), b) y c), referentes a billetes y monedas de un valor nominal total de al menos 5 000 EUR serán punibles con penas de prisión, con una pena máxima de al menos ocho años.

4. Los delitos mencionados en el artículo 3, apartado 1, letras a), b) y c), referentes a billetes y monedas de un valor nominal total de al menos 10 000 EUR o en que concurran circunstancias especialmente graves serán punibles con:

   a) una pena mínima de al menos seis meses de prisión;

   b) una pena máxima de al menos ocho años de prisión.

Artículo 6

Responsabilidad de las personas jurídicas

1. Los Estados miembros adoptarán las medidas necesarias para garantizar que las personas jurídicas puedan ser consideradas responsables de los delitos contemplados en los artículos 3 y 4 cuando los haya cometido en su provecho, actuando a título individual o como parte de un órgano de la persona jurídica, cualquier persona que ostente en el seno de esa persona jurídica un cargo directivo que lleve aparejado:

   a) poder para representarla, o

   b) autoridad para adoptar decisiones en su nombre, o

   c) autoridad para ejercer el control en su seno.

2. Los Estados miembros adoptarán las medidas necesarias para garantizar que una persona jurídica pueda ser considerada responsable cuando la falta de supervisión o control por parte de una de las personas a que se refiere el apartado 1 haya hecho posible que otra persona sometida a su autoridad cometa uno de los delitos contemplados en los artículos 3 y 4, en provecho de esa persona jurídica.

3. La responsabilidad de una persona jurídica en virtud de los apartados 1 y 2 se entenderá sin perjuicio de las acciones penales entabladas contra las personas físicas que sean autoras, instigadoras o cómplices de los delitos a que se refieren los artículos 3 y 4.

Artículo 7

Tipos de sanciones aplicables a las personas jurídicas

Los Estados miembros adoptarán las medidas necesarias para garantizar que una persona jurídica considerada responsable en virtud de lo dispuesto en el artículo 6 esté sujeta a sanciones efectivas, proporcionadas y disuasorias, incluidas multas de carácter penal o administrativo y otras sanciones como:

a) la exclusión del disfrute de ventajas o ayudas públicas;

b) la inhabilitación temporal o permanente para el ejercicio de actividades comerciales;

c) el sometimiento a vigilancia judicial;

d) una medida judicial de disolución;

e) el cierre temporal o definitivo de los establecimientos utilizados para cometer el delito.

Artículo 8

Jurisdicción

1. Los Estados miembros adoptarán las medidas necesarias para establecer su jurisdicción sobre los delitos contemplados en los artículos 3 y 4 cuando:

   a) el delito se haya cometido total o parcialmente en su territorio; o

   b) el autor del delito sea uno de sus nacionales.

2. Cada Estado miembro cuya moneda sea el euro adoptará las medidas necesarias para establecer su jurisdicción sobre los delitos mencionados en los artículos 3 y 4 cometidos fuera de la Unión Europea, al menos cuando se refieran al euro y cuando

   a) el autor del delito se halle en el territorio del Estado miembro; o

   b) los billetes o monedas de euro relacionados con el delito hayan sido detectados en el Estado miembro.

   A los efectos de persecución de cualquiera de los delitos, cada Estado miembro adoptará las medidas necesarias para garantizar que su jurisdicción no esté supeditada a la condición de que los actos sean un delito penal en el lugar en el que hayan sido cometidos.

3. Los Estados miembros concentrarán el proceso penal en un Estado miembro, a menos que sea improcedente.

Artículo 9

Herramientas de investigación

Los Estados miembros adoptarán las medidas necesarias para garantizar que las personas, unidades o servicios responsables de la investigación o persecución de los delitos contemplados en los artículos 3 a 4 disponen de instrumentos de investigación eficaces, como los que se utilizan en los casos relacionados con la delincuencia organizada u otros delitos graves.

Artículo 10

Obligación de transmitir los billetes y monedas de euro falsos para el análisis y la detección de falsificaciones

1. Los Estados miembros adoptarán las medidas necesarias para garantizar que las autoridades judiciales permiten el examen de los billetes y monedas de euro supuestamente falsos para el análisis, identificación y detección de ulteriores falsificaciones. Con este propósito, las autoridades judiciales transmitirán sin demora las muestras necesarias de cada tipo de billete supuestamente falso al Centro Nacional de Análisis y cada tipo de moneda supuestamente falsa al Centro Nacional de Análisis de Monedas.

2. Si las muestras necesarias de billetes y monedas supuestamente falsos no pueden transmitirse porque es preciso conservarlas como prueba en el proceso penal con vistas a garantizar un juicio justo y efectivo y el derecho de defensa del presunto delincuente, se dará acceso a ellas de forma inmediata al Centro Nacional de Análisis y al Centro Nacional de Análisis de Monedas.

Artículo 11

Relación con el Convenio de Ginebra

Los Estados miembros se adherirán al Convenio de Ginebra o seguirán siendo partes de dicho Convenio.

Artículo 12

Sustitución de la Decisión marco del Consejo 2000/383 /JAI

Se sustituye la Decisión marco 2000/383/JAI del Consejo en lo que respecta a los Estados miembros que participan en la adopción de la presente Directiva, sin perjuicio de las obligaciones de estos Estados miembros con relación a los plazos de transposición de la mencionada Decisión marco al Derecho nacional.

En el caso de los Estados miembros que participan en la adopción de la presente Directiva, las referencias a la Decisión marco 2000/383/JAI se entenderán hechas a la presente Directiva.

Artículo 13

Transposición

1. Los Estados miembros pondrán en vigor las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva a más tardar [18 meses después de la entrada en vigor de la presente Directiva]. Comunicarán inmediatamente a la Comisión el texto de dichas disposiciones.

   Cuando los Estados miembros adopten dichas disposiciones, estas harán referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia.

2. Los Estados miembros comunicarán a la Comisión el texto de las principales disposiciones de Derecho interno que adopten en el ámbito regulado por la presente Directiva.

Artículo 14

Informes de la Comisión y revisión

La Comisión enviará un informe sobre la aplicación de la presente Directiva al Parlamento Europeo y al Consejo dentro de los [5 años siguientes a su entrada en vigor]. Este informe evaluará la medida en que los Estados miembros han adoptado las medidas necesarias para cumplir la presente Directiva. Dicho informe deberá, en caso necesario, ir acompañado de una propuesta legislativa.

Artículo 15

Entrada en vigor

La presente Directiva entrará en vigor el [vigésimo] día siguiente al de su publicación en el *Diario Oficial de la Unión Europea*.

Artículo 16

Destinatarios

Los destinatarios de la presente Directiva serán los Estados miembros de conformidad con los Tratados.

Hecho en Estrasburgo, el

Por el Parlamento Europeo
El Presidente

Por el Consejo
El Presidente

N. de la R.: La documentació que acompanya aquesta proposta pot ésser consultada a l'Arxiu del Parlament.

Tramesa a la Comissió

Comissió competent: Comissió de Justícia.
Acord: Presidència del Parlament, 13.02.2013.

Termini de formulació d'observacions

Termini: 4 dies hàbils (del 19.02.2013 al 22.02.2013).
Finiment del termini: 25.02.2013; 09:30 h.
Acord: Presidència del Parlament, 13.02.2013.

Control del principi de subsidiarietat amb relació a la Proposta de reglament del Parlament Europeu i del Consell relatiu a informació que acompanya les transferències de fons
Tram. 295-00016/10

Text presentat
Tramesa de la Secretaria de la Comissió Mixta de la Unió Europea del 12.02.2013
Reg. 2570 / Admissió a tràmit: Presidència del Parlament, 13.02.2013

Asunto: Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la información que acompaña a las transferencias de fondos (Texto pertinente a efectos del EEE) [COM(2013) 44 final] [2013/0024 (COD)] {SWD(2013) 21 final} {SWD(2013) 22 final}

En aplicación del artículo 6.1 de la Ley 8/1994, de 19 de mayo, la Comisión Mixta para la Unión Europea remite a su Parlamento, por medio del presente correo electrónico, la iniciativa legislativa de la Unión Europea que se acompaña, a efectos de su conocimiento y para que, en su caso, remita a las Cortes Generales un dictamen motivado que exponga las razones por las que considera que la referida iniciativa de la Unión Europea no se ajusta al principio de subsidiariedad.

Aprovecho la ocasión para recordarle que, de conformidad con el artículo 6.2 de la mencionada Ley 8/1994, el dictamen motivado que, en su caso, apruebe su Institución debería ser recibido por las Cortes Generales en el plazo de cuatro semanas a partir de la remisión de la iniciativa legislativa europea.

Con el fin de agilizar la transmisión de los documentos en relación con este procedimiento de control del principio de subsidiariedad, le informo que se ha habilitado el siguiente correo electrónico de la Comisión Mixta para la Unión Europea: cmue@congreso.es

Secretaría de la Comisión Mixta para la Unión Europea

Estrasburgo, 5.2.2013
COM(2013) 44 final
2013/0024 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativo a la información que acompaña a las transferencias de fondos

(Texto pertinente a efectos del EEE)

{SWD(2013) 21 final}
{SWD(2013) 22 final}

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

Motivación y objetivos de la propuesta

La finalidad de la presente propuesta es revisar el Reglamento (CE) nº 1781/2006, relativo a la información sobre los ordenantes que acompaña a las transferencias de fondos[1] (en lo sucesivo, «el Reglamento relativo a las transferencias de fondos»), con vistas a mejorar el seguimiento de los pagos y garantizar que el marco de la UE siga siendo plenamente conforme con las normas internacionales.

[1] DO L 345 de 8.12.2006, p. 1.

Contexto general

El Reglamento relativo a las transferencias de fondos establece normas en virtud de las cuales los proveedores de servicios de pago deben enviar información sobre el ordenante a través de la cadena de pago con fines de prevención, investigación y detección del blanqueo de capitales y la financiación del terrorismo.

El Reglamento se basa, en gran medida, en la Recomendación Especial VII sobre las transferencias electrónicas, adoptada por el Grupo de Acción Financiera Internacional (GAFI)[2], y tiene por objeto garantizar que esta norma internacional se transponga de forma uniforme en toda la Unión, y, en particular, que no exista discriminación entre los pagos nacionales, esto es, dentro de un Estado miembro, y los pagos transfronterizos, esto es, entre Estados miembros.

Ante la variable naturaleza de la amenaza que representan el blanqueo de capitales y la financiación del terrorismo, como consecuencia de la permanente evolución de la tecnología y los medios a disposición de los delincuentes, el GAFI emprendió una profunda reforma de las normas internacionales, que culminó en la adopción de una nueva serie de Recomendaciones en febrero de 2012.

Paralelamente, la Comisión Europea ha emprendido su propia revisión del marco normativo de la UE. En el contexto de esa revisión, se ha procedido a la elaboración de un estudio externo, publicado por la Comisión, sobre la aplicación del Reglamento relativo a las transferencias de fondos y se han celebrado amplias consultas y mantenido numerosos contactos con interesados del sector privado y organizaciones de la sociedad civil, así como con representantes de las autoridades de reglamentación y supervisión de los Estados miembros de la Unión.

Este trabajo ha llevado a la conclusión de que el marco normativo de la UE, en el que se inscribe el Reglamento relativo a las transferencias de fondos, tendrá que evolucionar y adaptarse a cambios que han de poner mas énfasis en: a) la eficacia de los regímenes de lucha contra el blanqueo de capitales y la financiación del terrorismo, b) una mayor claridad y coherencia de las normas de todos los Estados miembros, y c) una ampliación del ámbito de aplicación, a fin de hacer frente a las nuevas amenazas y puntos vulnerables.

Disposiciones vigentes en este ámbito

La Directiva 2005/60/CE del Parlamento Europeo y del Consejo, de 26 de octubre de 2005, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo[3] (en lo sucesivo, «la Tercera Directiva sobre blanqueo de capitales») establece el marco destinado a proteger la solidez, integridad y estabilidad de las entidades de crédito y financieras, así como la confianza en el conjunto del sistema financiero, contra los riesgos del blanqueo de capitales y la financiación del terrorismo.

La Directiva 2006/70/CE[4] (en lo sucesivo, «la Directiva de aplicación») establece disposiciones de aplicación de la Directiva sobre el blanqueo de capitales en lo relativo a la definición de personas del medio político y los criterios técnicos aplicables en los procedimientos simplificados de diligencia debida con respecto al cliente, así como en lo que atañe a la exención por razones de actividad financiera ocasional o muy limitada.

El Reglamento relativo a las transferencias de fondos complementa esas disposiciones garantizando que la información básica sobre los ordenantes de las transferencias de fondos esté inmediatamente a disposición de las autoridades policiales y/o judiciales competentes, a fin de ayudarlas a detectar, investigar y enjuiciar a los terroristas y otros delincuentes, así como a localizar los activos de los terroristas.

Coherencia con otras políticas y objetivos de la Unión

La propuesta es coherente con la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la prevención del uso del sistema financiero para el blanqueo de capitales y la financiación del terrorismo. Estos dos actos legislativos persiguen el objetivo común de revisar el actual marco normativo de la UE aplicable al blanqueo de capitales y la financiación del terrorismo, a efectos de mejorar su eficacia y garantizar, al mismo tiempo, su conformidad con las normas internacionales.

La propuesta guarda también coherencia con los objetivos de la Estrategia de Seguridad Interior de la UE[5], que señala los retos más urgentes a que se enfrenta la seguridad europea en los próximos años y propone cinco objetivos estratégicos y medidas específicas para el periodo 2011-2014 a efectos de contribuir a dotar a la UE de mayor seguridad. Ello incluye la lucha contra el blanqueo de capitales y la prevención del terrorismo, en particular actualizando el marco normativo de la UE para incrementar la transparencia de la información relativa a la titularidad real de las personas jurídicas.

2 El GAFI, órgano internacional creado por el G-7 en la Cumbre de París en 1989, se considera que marca la pauta a escala mundial en la lucha contra el blanqueo de capitales y la financiación del terrorismo.
3 DO L 309 de 25.11.2005, p. 15.
4 DO L 214 de 4.8.2006, p. 29.
5 COM(2010) 673 final.

En relación con la protección de datos, las aclaraciones propuestas sobre el tratamiento de los datos personales son acordes con el enfoque adoptado por la Comisión en sus recientes propuestas sobre la protección de datos[6].

En lo tocante a las sanciones, la propuesta de introducir un conjunto de normas mínimas basadas en principios y destinadas a reforzar las sanciones y medidas administrativas es coherente con la política expuesta por la Comisión en su Comunicación «Regímenes sancionadores más rigurosos en el sector de servicios financieros»[7].

2. RESULTADOS DE LAS CONSULTAS CON LAS PARTES INTERESADAS Y DE LAS EVALUACIONES DE IMPACTO

Consulta con las partes interesadas

En abril de 2012, la Comisión adoptó un informe sobre la aplicación de la Directiva 2005/60/CE y solicitó observaciones a todos los interesados[8]. El anexo de ese informe abordaba, en particular, las transferencias electrónicas transfronterizas y, más en concreto, las dos nuevas obligaciones de incluir en ellas información sobre el beneficiario y adoptar las medidas de congelación que se deriven de las Resoluciones de Naciones Unidas.

La Comisión recibió solo cuatro aportaciones que se referían expresamente al anexo del informe. En las observaciones enviadas se pedía que se consultara a los interesados de todos los países y territorios afectados por el Reglamento relativo a la transferencia de fondos, y se subrayaba la necesidad de que toda nueva exigencia u obligación impuesta a los proveedores de servicios de pago fuera proporcionada y fácil de cumplir.

En el contexto del estudio externo[9] realizado por encargo de la Comisión Europea, se llevaron a cabo extensas consultas entre 108 interesados, que incluyeron entrevistas telefónicas y la cumplimentación de un cuestionario estructurado.

Utilización de asesoramiento técnico

En el curso de 2012, se realizó un estudio externo por encargo de la Comisión, dirigido a recopilar información sobre el funcionamiento del Reglamento relativo a las transferencias de fondos en los Estados miembros y los problemas que hayan surgido[10].

El estudio contiene, en particular, una serie de recomendaciones, a saber:

– introducir la obligación de que los proveedores de servicios de pagos garanticen que junto a las transferencias electrónicas se conserve toda la información relativa al ordenante y al beneficiario;

– determinar qué información del beneficiario ha de verificarse, y quién debe hacerlo;

– estudiar la posibilidad de introducir un régimen «simplificado» para las transferencias electrónicas transfronterizas cuyo importe no exceda de 1 000 EUR, salvo cuando existan sospechas de blanqueo de capitales o financiación del terrorismo;

– aclarar más las obligaciones de información de los proveedores de servicios de pago;

– prohibir explícitamente la ejecución de las transferencias electrónicas que no reúnan los requisitos necesarios (exhaustividad y exactitud de la información);

– que los proveedores de servicios de pago beneficiarios apliquen políticas y procedimientos efectivos, basados en el riesgo, con el fin de determinar las oportunas medidas de actuación;

– que se tengan en cuenta las consecuencias en lo referente a la protección de datos.

Evaluación de impacto

La presente propuesta va acompañada de una evaluación de impacto en la que se indican los principales problemas detectados en el vigente marco normativo de la UE en materia de lucha contra el blanqueo de capitales y la financiación del terrorismo[11]: i) falta de coherencia con las normas internacionales recientemente revisadas; ii) diferentes interpretaciones de las normas en los distintos Estados miembros; y iii) deficiencias y lagunas por lo que respecta a los nuevos riesgos de blanqueo de capitales y financiación del terrorismo. Ello trae como consecuencia una

6 COM(2012) 10 final y COM(2012) 11 final.
7 COM(2010) 716 final.
8 El informe de la Comisión, las respuestas de los interesados y una síntesis de las aportaciones están disponibles en http://ec.europa.eu/internal_market/company/financial-crime/index_en.htm
9 El estudio está disponible en la siguiente dirección http://ec.europa.eu/internal_market/company/financial-crime/index_en.htm
10 *Ibidem*.
11 La evaluación de impacto está disponible en la siguiente dirección http://ec.europa.eu/internal_market/company/financial-crime/index_en.htm

reducción de la eficacia de los regímenes de lucha contra el blanqueo de capitales y la financiación del terrorismo, lo que tiene efectos negativos por lo que atañe a la reputación, así como en el orden económico y financiero.

La evaluación de impacto analiza los tres escenarios siguientes:

(1) un escenario de base, consistente en que la Comisión no adopta ninguna medida;

(2) un escenario de ajuste, que comporta cambios limitados del Reglamento relativo a las transferencias de fondos, necesarios para: i) adaptar el texto legislativo a las normas internacionales revisadas, o ii) garantizar un grado suficiente de coherencia entre las disposiciones nacionales, o iii) solucionar las deficiencias más importantes en relación con las nuevas amenazas; y

(3) un escenario de plena armonización, que conlleva importantes cambios de política y elementos de armonización adicionales, en reconocimiento de posibles especificidades de la UE.

El análisis efectuado en la evaluación de impacto ha demostrado que el segundo escenario es el más equilibrado, ya que, a la vez que adapta el Reglamento relativo a las transferencias de fondos a las normas internacionales revisadas, garantiza un grado de coherencia suficiente entre las normas nacionales y deja margen de maniobra para su aplicación.

Asimismo, la evaluación de impacto analizó los efectos de las propuestas legislativas sobre los derechos fundamentales. En consonancia con la Carta de los Derechos Fundamentales, las propuestas persiguen, en particular, garantizar la protección de los datos personales (artículo 8 de la Carta) por lo que atañe a su almacenamiento y transferencia.

3. ASPECTOS JURÍDICOS DE LA PROPUESTA

Base jurídica

Artículo 114 del Tratado de Funcionamiento de la Unión Europea.

Subsidiariedad y proporcionalidad

Existe consenso en general entre todos los interesados (en particular los Estados miembros y el sector de servicios de pago) en cuanto a que los objetivos de la propuesta no pueden ser alcanzados de manera suficiente por los Estados miembros y, por consiguiente, pueden alcanzarse mejor con la intervención de la UE.

La actuación descoordinada de los Estados miembros en el ámbito de las transferencias de fondos transfronterizas podría incidir significativamente en el buen funcionamiento de los sistemas de pago a escala de la UE y, en consecuencia, afectar negativamente al mercado interior de servicios financieros (véase el considerando 2 del Reglamento relativo a la transferencia de fondos).

Por la escala de su intervención, la Unión garantizará la transposición uniforme de la nueva Recomendación 16 del GAFI en toda la UE, y, en particular, garantizará que no exista discriminación entre los pagos nacionales, dentro de un Estado miembro, y los pagos transfronterizos, entre Estados miembros.

La propuesta se atiene, pues, al principio de subsidiariedad.

En cuanto al principio de proporcionalidad, de acuerdo con el análisis efectuado en la evaluación de impacto, la propuesta transpone la Recomendación revisada del GAFI sobre las transferencias electrónicas, introduciendo los requisitos mínimos que garanticen el seguimiento de las transferencias, limitándose a lo estrictamente necesario para alcanzar sus objetivos.

4. REPERCUSIONES PRESUPUESTARIAS

La presente propuesta no tiene repercusiones para el presupuesto de la Unión.

5. INFORMACIÓN ADICIONAL

Explicación detallada de la propuesta

Conforme a la nueva Recomendación 16 del GAFI sobre las transferencias electrónicas, y a la Nota Interpretativa que la acompaña, los cambios propuestos están destinados a abordar aspectos en los que aún existen lagunas en materia de transparencia.

Se trata de mejorar el seguimiento mediante los siguientes requisitos principales:

– incluir información sobre el beneficiario;

– con respecto al ámbito de aplicación del Reglamento, especificar que las tarjetas de crédito o de débito, los dispositivos de telefonía móvil o cualquier otro dispositivo digital o de tecnología de la información estén sujetos a lo dispuesto en el Reglamento cuando se utilicen para efectuar transferencias de fondos entre

particulares; asimismo, especificar que en importes inferiores a 1 000 euros, en el caso de transferencias fuera de la UE, es de aplicación un régimen simplificado en el que la información sobre el ordenante y el beneficiario no se verifica (frente a posibles exenciones del ámbito de aplicación como en el Reglamento (CE) nº 1781/2006);

– en cuanto a las obligaciones del proveedor de servicios de pago (PSP) del beneficiario, la obligación de verificar la identidad de este último (si no ha sido identificado previamente) en el caso de pagos procedentes de fuera de la UE y de un importe superior a 1 000 EUR; por lo que atañe al PSP del beneficiario y al PSP intermediario, la obligación de establecer procedimientos basados en el riesgo y destinados a determinar cuándo debe ejecutarse, rechazarse o suspenderse una transferencia de fondos que carezca de la información necesaria, así como determinar las medidas oportunas que deban adoptarse;

– en relación con la protección de datos, adaptar los requisitos de conservación de la información a las normas del GAFI, de acuerdo con el nuevo régimen previsto en la Directiva [xxxx/yyyy];

– en relación con las sanciones, reforzar las facultades sancionadoras de las autoridades competentes y establecer la obligación de coordinar las actuaciones en los casos transfronterizos; la obligación de publicar las sanciones impuestas por infracciones cometidas; y la obligación de establecer mecanismos eficaces que alienten a notificar las infracciones de las disposiciones del Reglamento.

Espacio Económico Europeo

El acto propuesto es pertinente a efectos del Espacio Económico Europeo y, por consiguiente, debe hacerse extensivo a su territorio.

2013/0024 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativo a la información que acompaña a las transferencias de fondos

(Texto pertinente a efectos del EEE)

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, su artículo 114,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de acto legislativo a los parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo[12],

Visto el dictamen del Banco Central Europeo[13],

Previa consulta al Supervisor Europeo de Protección de Datos[14]:

De conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

(1) Los flujos de dinero negro a través de transferencias de fondos pueden dañar la estabilidad y reputación del sector financiero y amenazar el mercado interior. El terrorismo quebranta las bases mismas de nuestra sociedad. La solidez, la integridad y la estabilidad del sistema de transferencias de fondos y la confianza en el sistema financiero en su conjunto podrían verse seriamente comprometidas por los esfuerzos de los delincuentes y de sus cómplices por encubrir el origen de sus ingresos delictivos o por transferir fondos con propósitos terroristas.

12 DO C … de …, p. ….
13 DO C … de …, p. ….
14 DO C … de …, p. ….

(2) Si no se adoptan medidas de coordinación en el ámbito de la Unión, los blanqueadores de capitales y los financiadores del terrorismo podrían aprovechar la libre circulación de capitales que trae consigo un espacio financiero integrado para facilitar sus actividades delictivas. Por su escala, la acción de la Unión garantizará que la Recomendación 16 sobre transferencias electrónicas del Grupo de Acción Financiera Internacional (GAFI) sea transpuesta de manera uniforme en toda la Unión Europea y, en especial, que no haya ninguna discriminación entre los pagos nacionales, en un Estado miembro, y los pagos transfronterizos entre Estados miembros. Una actuación no coordinada de los Estados miembros por sí solos en el ámbito de las transferencias transfronterizas de fondos podría afectar significativamente al buen funcionamiento de los sistemas de pagos a nivel de la UE y, por lo tanto, perjudicar al mercado interior en el ámbito de los servicios financieros.

(3) En la revisión de la Estrategia revisada de la Unión sobre la financiación del terrorismo, de 17 de julio de 2008, se indica que han de proseguir los esfuerzos dirigidos a impedir la financiación del terrorismo y el uso por las personas sospechosas de terrorismo de sus propios recursos financieros. Se reconoce que el GAFI persigue constantemente la mejora de sus Recomendaciones y se esfuerza por llegar a una interpretación común de cómo deben aplicarse. Asimismo, en la citada Estrategia revisada de la Unión se señala que la aplicación de esas Recomendaciones por los miembros del GAFI y los miembros de organismos regionales similares al GAFI se evalúa periódicamente y que, en este sentido, es importante que los Estados miembros adopten un mismo enfoque.

(4) Para prevenir la financiación del terrorismo, se han adoptado medidas dirigidas a la congelación de fondos y recursos económicos de determinadas personas, grupos y entidades, concretamente el Reglamento (CE) nº 2580/2001, de 27 de diciembre de 2001, sobre medidas restrictivas específicas dirigidas a determinadas personas y entidades con el fin de luchar contra el terrorismo[15] y el Reglamento (CE) nº 881/2002 del Consejo, de 27 de mayo de 2002, por el que se imponen determinadas medidas restrictivas específicas dirigidas contra determinadas personas y entidades asociadas con la red Al-Qaida[16]. Con ese mismo objeto, se han adoptado medidas encaminadas a proteger el sistema financiero contra la canalización de fondos y recursos económicos con fines terroristas. La Directiva [xxxx/yyyy] del Parlamento Europeo y del Consejo, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo[17], contiene una serie de esas medidas. Sin embargo, dichas medidas no impiden del todo que los terroristas y otros delincuentes tengan acceso a los sistemas de pago para hacer circular sus fondos.

(5) Para estimular un planteamiento coherente en el contexto internacional en el ámbito de la lucha contra el blanqueo de capitales y la financiación del terrorismo, las nuevas medidas comunitarias deben tener en cuenta la evolución a ese respecto, más concretamente las normas internacionales sobre la lucha contra el blanqueo de capitales y la financiación del terrorismo y la proliferación, adoptadas en 2012, y en especial la Recomendación 16 y la nota interpretativa revisada para su aplicación.

(6) La capacidad de seguimiento total de las transferencias de fondos puede ser una herramienta particularmente importante y valiosa en la prevención, investigación y detección del blanqueo de capitales o de la financiación del terrorismo. Resulta, por lo tanto, pertinente para asegurar la transmisión de la información a lo largo de la cadena de pago establecer un sistema que imponga la obligación a los proveedores de servicios de pago de acompañar las transferencias de fondos de información sobre el ordenante y el beneficiario.

(7) Las disposiciones del presente Reglamento se establecen sin perjuicio de lo dispuesto en la legislación nacional de transposición de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[18]. Por ejemplo, lo datos personales recogidos a efectos del cumplimiento del presente Reglamento no deben ser tratados posteriormente de forma que resulte incompatible con lo dispuesto en la citada Directiva 95/46/CE. En especial, debe estar terminantemente prohibido todo tratamiento posterior con fines comerciales. La lucha contra el blanqueo de capitales y la financiación del terrorismo se reconoce como un importante motivo de interés general en todos los Estados miembros. Por consiguiente, en la aplicación del presente Reglamento, la transferencia de datos personales a un tercer país que no garantice un nivel adecuado de protección en el sentido de lo dispuesto en el artículo 25 de la Directiva 95/46/CE debe autorizarse de acuerdo con el artículo 26, letra d), de esa misma Directiva.

(8) Las personas que se limitan a convertir documentos en soporte papel en datos electrónicos y que actúan con arreglo a un contrato celebrado con un proveedor de servicios de pago no están incluidas en el ámbito de aplicación del presente Reglamento; esto mismo es válido en lo que atañe a las personas físicas o jurídicas que solo proporcionan a los proveedores de servicios de pago un sistema de mensajería u otros sistemas de apoyo para la transmisión de fondos, o sistemas de compensación y liquidación.

---

15 DO L 344 de 28.12.2001, p. 70.
16 DO L 139 de 29.5.2002, p. 9.
17 DO L… de …, p. … .
18 DO L 281 de 23.11.1995, p. 31.

(9) Es adecuado excluir del ámbito de aplicación del presente Reglamento las transferencias de fondos que representen un bajo riesgo de blanqueo de capitales o de financiación del terrorismo. Estas exclusiones deben comprender las tarjetas de crédito y de débito, los teléfonos móviles u otros dispositivos digitales o de tecnología de la información, las retiradas de efectivo en cajeros automáticos, los pagos en concepto de impuestos, multas u otros gravámenes, y las transferencias de fondos en las que tanto el ordenante como el beneficiario sean proveedores de servicios de pago que actúen por cuenta propia. Además, a fin de tener en cuenta las características especiales de los sistemas de pago nacionales, los Estados miembros deben poder establecer exenciones para las transferencias electrónicas siempre que sea posible realizar un seguimiento de las transferencias de fondos hasta localizar al ordenante. No obstante, no debe otorgarse exención alguna cuando una tarjeta de débito o de crédito, un teléfono móvil u otro dispositivo digital o de tecnología de la información, de prepago o postpago, se utilice para efectuar una transferencia entre particulares.

(10) Con el fin de no obstaculizar la eficiencia de los sistemas de pago, deben diferenciarse los requisitos de verificación aplicables a las transferencias de fondos efectuadas a partir de cuentas de los aplicables a las transferencias no efectuadas a partir de cuentas. Para contrarrestar el riesgo de que se realicen operaciones fuera de los cauces reglamentarios por la aplicación de unas exigencias de identificación demasiado estrictas con respecto a la potencial amenaza del uso de las pequeñas transferencias de fondos para fines terroristas, en caso de transferencias de fondos no realizadas a partir de una cuenta, la obligación de verificar que la información sobre el ordenante sea exacta debe aplicarse únicamente a las transferencias individuales que superen los 1 000 EUR. En el caso de las transferencias de fondos efectuadas a partir de cuentas, no debe requerirse que los proveedores de servicios de pago verifiquen la información sobre el ordenante que acompañe a cada transferencia de fondos, cuando se cumplan las obligaciones que establece la Directiva [xxxx/yyyy]..

(11) En el contexto de la legislación de la Unión en materia de pagos –Reglamento (CE) nº 924/2009 del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, relativo a los pagos transfronterizos en la Comunidad[19], Reglamento (UE) nº 260/2012 del Parlamento Europeo y del Consejo, de 14 de marzo de 2012, por el que se establecen requisitos técnicos y empresariales para las transferencias y los adeudos domiciliados en euros[20] y Directiva 2007/64/CE del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, sobre servicios de pago en el mercado interior[21]– resulta suficiente prever que las transferencias de fondos efectuadas en la Unión vayan acompañadas de información simplificada sobre el ordenante

(12) Con el fin de que las autoridades responsables de combatir el blanqueo de capitales o la financiación del terrorismo en terceros países puedan localizar el origen de los fondos utilizados para dichos propósitos, las transferencias de fondos desde la Comunidad al exterior de la Unión deben llevar información completa sobre el ordenante y el beneficiario. Dichas autoridades deben tener acceso a información completa sobre el ordenante solo a efectos de prevenir, investigar y detectar el blanqueo de capitales o la financiación del terrorismo.

(13) Para que las transferencias de fondos de un solo ordenante a varios beneficiarios se envíen de forma poco costosa en ficheros que contengan lotes de transferencias individuales desde la Unión al exterior de la Unión, estas deben poder llevar únicamente el número de cuenta del ordenante o su identificador único de operación, a condición de que el fichero correspondiente al lote de transferencias contenga información completa sobre el ordenante y el beneficiario o beneficiarios.

(14) Para comprobar si la información requerida sobre el ordenante y el beneficiario acompaña a las transferencias de fondos, y ayudar a identificar las operaciones sospechosas, el proveedor de servicios de pago del beneficiario y el proveedor de servicios de pago intermediario deben contar con procedimientos efectivos para detectar la falta de información sobre el ordenante y el beneficiario.

(15) Dada la potencial amenaza de financiación del terrorismo planteada por las transferencias anónimas, resulta oportuno exigir que los proveedores de servicios de pago soliciten información sobre el ordenante y el beneficiario. En consonancia con el enfoque basado en el riesgo desarrollado por el GAFI, resulta oportuno determinar qué ámbitos presentan mayor y menor riesgo, al objeto de responder mejor a los riesgos de blanqueo de capitales y financiación del terrorismo. De este modo, el proveedor de servicios de pago del beneficiario y el proveedor de servicios de pago intermediario deben establecer procedimientos eficaces, basados en el riesgo, para aquellos casos en que las transferencias de fondos no contengan la información requerida sobre el ordenante y el beneficiario, con el fin de decidir si se ejecuta, se rechaza o se suspende la transferencia y qué medidas consiguientes resulta oportuno adoptar. En el caso de que el proveedor de servicios de pago del ordenante esté situado fuera del territorio de la Unión, debe reforzarse la diligencia debida con respecto al cliente, de conformidad con la Directiva [xxxx/yyyy], por lo que se refiere a las relaciones transfronterizas de corresponsalía bancaria con ese proveedor de servicios de pago.

---

19 DO L 266 de 9.10.2009, p. 11.
20 DO L 94 de 30.3.2012, p. 22.
21 DO L 319 de 5.12.2007, p. 1.

(16) El proveedor de servicios de pago del beneficiario y el proveedor de servicios de pago intermediario deben ejercer una vigilancia especial, evaluando los riesgos, cuando constaten que la información sobre el ordenante falta o está incompleta, y deben informar sobre las operaciones sospechosas a las autoridades competentes, de acuerdo con las obligaciones en materia de información establecidas en la Directiva [xxxx/yyyy] y en las medidas de ejecución nacionales.

(17) Las disposiciones aplicables a las transferencias de fondos en las que falte información sobre el ordenante o el beneficiario o esta sea incompleta deben aplicarse sin perjuicio de las obligaciones de los proveedores de servicios de pago y los proveedores de servicios de pago intermediarios de suspender y/o rechazar las transferencias de fondos que incumplan disposiciones de Derecho civil, administrativo o penal.

(18) Hasta que se eliminen las limitaciones técnicas que pueden impedir que los proveedores de servicios de pago intermediarios cumplan la obligación de transmitir toda la información recibida sobre el ordenante, dichos proveedores de servicios de pago intermediarios deben guardar constancia de esa información. Estas limitaciones técnicas deben desaparecer tan pronto como se actualicen los sistemas de pago.

(19) Dado que, en las investigaciones penales, puede no ser posible determinar los datos requeridos o los individuos implicados hasta muchos meses o incluso años después de la transferencia original de fondos, y a fin de poder tener acceso a elementos de prueba esenciales en el contexto de investigaciones, los proveedores de servicios de pago deben guardar constancia de la información sobre el ordenante para prevenir, investigar y detectar el blanqueo de capitales o la financiación del terrorismo.. Este período debe ser limitado.

(20) Para acelerar las intervenciones en el marco de la lucha contra el terrorismo, los proveedores de servicios de pago deben responder rápidamente a las peticiones de información sobre el ordenante de las autoridades responsables de la lucha contra el blanqueo de capitales o la financiación del terrorismo en el Estado miembro donde estén establecidos.

(21) El número de días para responder a las solicitudes de información sobre el ordenante viene determinado por el número de días hábiles en el Estado miembro del proveedor de servicios de pago del ordenante.

(22) A fin de promover el cumplimiento de lo dispuesto en el presente Reglamento, y con arreglo a la Comunicación de la Comisión de 9 de diciembre de 2010 titulada «Regímenes sancionadores más rigurosos en el sector de servicios financieros»[22], se deben reforzar las facultades de las autoridades competentes para adoptar medidas de supervisión, así como sus facultades sancionadoras. Resulta oportuno prever sanciones administrativas y, dada la importancia de la lucha contra el blanqueo de capitales y la financiación del terrorismo, los Estados miembros deben establecer sanciones que resulten eficaces, proporcionadas y disuasorias. Los Estados miembros deben notificar a la Comisión, así como a la Autoridad Europea de Supervisión (Autoridad Bancaria Europea, en lo sucesivo «ABE»), creada por el Reglamento (UE) nº 1093/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Bancaria Europea), se modifica la Decisión nº 716/2009/CE y se deroga la Decisión 2009/78/CE de la Comisión; a la Autoridad Europea de Supervisión (Autoridad Europea de Seguros y Pensiones de Jubilación, en lo sucesivo «AESPJ»), creada por el Reglamento (UE) nº 1094/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Europea de Seguros y Pensiones de Jubilación), se modifica la Decisión nº 716/2009/CE y se deroga la Decisión 2009/79/CE de la Comisión; y la Autoridad Europea de Supervisión (Autoridad Europea de Valores y Mercados, en lo sucesivo, «AEVM»), creada por el Reglamento (UE) nº 1095/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Europea de Valores y Mercados), se modifica la Decisión nº 716/2009/CE y se deroga la Decisión 2009/77/CE.

(23) A fin de garantizar condiciones uniformes de ejecución de los artículos XXX del presente Reglamento, deben conferirse a la Comisión competencias de ejecución. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) nº 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión[23].

(24) Varios países y territorios que no forman parte del territorio de la Unión comparten una unión monetaria con un Estado miembro, forman parte de la zona monetaria de un Estado miembro o han firmado un convenio monetario con la Unión representada por un Estado miembro, y tienen proveedores de servicios de pago que intervienen, directa o indirectamente, en los sistemas de pagos y liquidación de ese Estado miembro. Para evitar todo efecto negativo de importancia sobre las economías de esos países o territorios que pudiera resultar de la aplicación del presente Reglamento a transferencias de fondos entre los Estados miembros de que se trate y esos países o territorios, resulta oportuno prever la posibilidad de que esas transferencias de fondos sean tratadas como transferencias de fondos dentro de esos Estados miembros.

22 COM(2010) 716 final.
23 DO L 55 de 28.2.2011, p. 13.

(25) Vistas las modificaciones que sería necesario introducir en el Reglamento (CE) nº 1781/2006, de 15 de noviembre de 2006, relativo a la información sobre los ordenantes que acompaña a las transferencias de fondos, resulta oportuno derogarlo en aras de la claridad.

(26) Dado que los objetivos del presente Reglamento no pueden ser alcanzados de manera suficiente por los Estados miembros y, por consiguiente, debido a las dimensiones o los efectos de la acción, pueden lograrse mejor a nivel de la Unión, la Unión puede adoptar medidas, de acuerdo con el principio de subsidiariedad consagrado en el artículo 5 del Tratado. De conformidad con el principio de proporcionalidad enunciado en dicho artículo, el presente Reglamento no excede de lo necesario para alcanzar dichos objetivos.

(27) El presente Reglamento respeta los derechos fundamentales y observa los principios reconocidos por la Carta de los Derechos Fundamentales de la Unión Europea, en particular el derecho al respeto de la vida privada y familiar (artículo 7), el derecho a la protección de datos de carácter personal (artículo 8) y el derecho a la tutela judicial efectiva y a un juez imparcial (artículo 47), así como el principio *ne bis in idem*.

(28) A fin de facilitar la introducción del nuevo marco sobre el blanqueo de capitales y la financiación del terrorismo, procede que la fecha de aplicación del presente Reglamento coincida con el final del plazo de transposición de la Directiva [xxxx/yyyy].

HAN ADOPTADO EL PRESENTE REGLAMENTO:

CAPÍTULO I

OBJETO, DEFINICIONES Y ÁMBITO DE APLICACIÓN

Artículo 1

Objeto

El presente Reglamento establece normas sobre la información que debe acompañar a las transferencias de fondos, en lo referente a los ordenantes y beneficiarios de las mismas, a efectos de la prevención, detección e investigación del blanqueo de capitales y la financiación del terrorismo.

Artículo 2

Definiciones

A efectos del presente Reglamento, se entenderá por:

(1) «financiación del terrorismo»: financiación del terrorismo tal y como se define en el artículo 1, apartado 4, de la Directiva [xxxx/yyyy];

(2) «blanqueo de capitales»: las actividades de blanqueo de capitales a que se refiere el artículo 1, apartados 2 o 3, de la Directiva [xxxx/yyyy];

(3) «ordenante»: toda persona física o jurídica que efectúa una transferencia de fondos desde su propia cuenta o da una orden para que se efectúe una transferencia de fondos;

(4) «beneficiario»: toda persona física o jurídica que sea el destinatario previsto de los fondos transferidos;

(5) «proveedor de servicios de pago»: toda persona física o jurídica que preste servicios de transferencia de fondos a título profesional;

(6) «proveedor de servicios de pago intermediario»: todo proveedor de servicios de pago, que no sea ni el del ordenante ni el del beneficiario, que reciba y transmita una transferencia de fondos por cuenta del proveedor de servicios de pago del ordenante o del beneficiario o de otro proveedor de servicios de pago intermediario;

(7) «transferencia de fondos»: toda operación efectuada por cuenta de un ordenante, a través de un proveedor de servicios de pago y por medios electrónicos, con objeto de poner fondos a disposición de un beneficiario a través de un proveedor de servicios de pago, con independencia de que el ordenante y el beneficiario sean o no la misma persona.

(8) «transferencia por lotes»: varias transferencias de fondos individuales que se agrupan para su transmisión;

(9) «identificador único de operación»: una combinación de letras o símbolos determinada por el proveedor de servicios de pago, con arreglo a los protocolos del sistema de pago y liquidación o del sistema de mensajería utilizados para realizar la transferencia de fondos, que permite rastrear la operación hasta identificar al ordenante y al beneficiario.

(10) «transferencia entre particulares»: toda operación de transferencia de fondos que tenga lugar entre dos personas físicas.

Artículo 3

Ámbito de aplicación

1. El presente Reglamento se aplicará a las transferencias de fondos en cualquier moneda enviadas o recibidas por un proveedor de servicios de pago establecido en la Unión.

2. El presente Reglamento no se aplicará a las transferencias de fondos efectuadas utilizando una tarjeta de crédito o de débito o un teléfono móvil o cualquier otro dispositivo digital o de tecnología de la información, a condición de que:

   (a) la tarjeta o dispositivo se utilice para el pago de bienes y servicios;

   (b) el número de la citada tarjeta o dispositivo se indique en todas las transferencias que se deriven de la operación.

   No obstante, el presente Reglamento será de aplicación cuando una tarjeta de crédito o de débito o un teléfono móvil o cualquier otro dispositivo digital o de tecnología de la información se utilice para efectuar una transferencia de fondos entre particulares.

3. El presente Reglamento no se aplicará a las transferencias de fondos cuando:

   (a) la transferencia de fondos implique que el ordenante tenga que retirar efectivo de su propia cuenta;

   (b) los fondos se transfieran a autoridades públicas en concepto de pago de impuestos, multas u otros gravámenes dentro de un Estado miembro;

   (c) tanto el ordenante como el beneficiario sean proveedores de servicios de pago que actúen en nombre propio.

CAPÍTULO II

OBLIGACIONES DE LOS PROVEEDORES DE SERVICIOS DE PAGO

Sección 1

OBLIGACIONES DEL PROVEEDOR DE SERVICIOS DE PAGO DEL ORDENANTE

Artículo 4

Información que debe acompañar a las transferencias de fondos

1. Los proveedores de servicios de pago se asegurarán de que las transferencias de fondos vayan acompañadas de la siguiente información sobre el ordenante:

   (a) el nombre del ordenante;

   (b) el número de cuenta del ordenante, cuando esta se utilice para realizar la transferencia de fondos, o un identificador único de operación cuando no se utilice tal cuenta a esos efectos;

   (c) la dirección del ordenante, o el número nacional de identidad, o el número de identificación de cliente, o su fecha y lugar de nacimiento.

2. Los proveedores de servicios de pago se asegurarán de que las transferencias de fondos vayan acompañadas de la siguiente información sobre el beneficiario:

   (a) el nombre del beneficiario; y

   (b) el número de cuenta del beneficiario, cuando esta cuenta se utilice para realizar la operación, o un identificador único de operación cuando no se utilice tal cuenta a esos efectos.

3. Antes de transferir los fondos, el proveedor de servicios de pago del ordenante verificará la exactitud de la información a que se refiere el apartado 1 por medio de documentos, datos o información obtenidos de una fuente fiable e independiente.

4. Cuando los fondos se transfieran desde la cuenta del ordenante, la verificación a que se refiere el apartado 3 se dará por efectuada siempre que:

(a) la identidad del ordenante haya sido verificada con ocasión de la apertura de la cuenta, de conformidad con el artículo 11 de la Directiva [xxxx/yyyy], y la información recopilada en dicha verificación se haya almacenado con arreglo a lo establecido en el artículo 39 de esa Directiva;

o

(b) al ordenante le sean aplicables las disposiciones del artículo 12, apartado 5, de la Directiva [xxxx/yyyy].

5. No obstante, sin perjuicio de lo dispuesto en el apartado 3, en el caso de transferencias de fondos no efectuadas a partir de una cuenta, el proveedor de servicios de pago del ordenante no verificará la información a que se refiere el apartado 1 cuando el importe no sobrepase los 1 000 EUR y no parezca relacionada con otras transferencias de fondos que, junto con la transferencia considerada, sobrepasen los 1 000 EUR.

Artículo 5

Transferencias de fondos dentro de la Unión

1. No obstante lo dispuesto en el artículo 4, apartados 1 y 2, cuando tanto el proveedor de servicios de pago del ordenante como el proveedor de servicios de pago del beneficiario estén establecidos en la Unión, solo se exigirá que las transferencias de fondos vayan acompañadas del número de cuenta del ordenante o su identificador único de operación.

2. No obstante lo dispuesto en el apartado 1, cuando así lo solicite el proveedor de servicios de pago del beneficiario o el proveedor de servicios de pago intermediario, el proveedor de servicios de pago del ordenante facilitará la información sobre el ordenante o el beneficiario conforme al articulo 4, en el plazo de tres días hábiles desde la recepción de esa petición.

Artículo 6

Transferencias de fondos al exterior de la Unión

1. En el caso de las transferencias por lotes procedentes de un solo ordenante en las que los proveedores de servicios de pago de los beneficiarios estén establecidos fuera de la Unión, el artículo 4, apartados 1 y 2, no será aplicable a las transferencias individuales que formen parte del lote, a condición de que el fichero correspondiente al lote contenga esa información y que las transferencias individuales lleven el número de cuenta del ordenante o su identificador único de operación.

2. No obstante lo dispuesto en el artículo 4, apartados 1 y 2, cuando el proveedor de servicios de pago del beneficiario esté establecido fuera de la Unión, las transferencias de fondos que no sobrepasen los 1 000 EUR irán acompañadas de lo siguiente:

(a) el nombre del ordenante;

(b) el nombre del beneficiario;

(c) el número de cuenta del ordenante y del beneficiario o el identificador único de operación.

Solo se verificará la exactitud de esta información cuando existan sospechas de blanqueo de capitales o financiación del terrorismo.

SECCIÓN 2

OBLIGACIONES DEL PROVEEDOR DE SERVICIOS DE PAGO DEL BENEFICIARIO

Artículo 7

Detección de la falta de información sobre el ordenante y el beneficiario

1. El proveedor de servicios de pago del beneficiario verificará, en lo que respecta a la información sobre el ordenante y el beneficiario, si los campos del sistema de mensajería o de pagos y liquidación utilizado para efectuar la transferencia de fondos han sido rellenados mediante los caracteres o entradas admisibles en el marco de los protocolos de dicho sistema.

2. Dicho proveedor deberá contar con procedimientos efectivos para detectar la falta de la siguiente información sobre el ordenante y el beneficiario:

   (a) en relación con las transferencias de fondos en las que el proveedor de servicios de pago del ordenante esté establecido en la Unión, la información exigida de conformidad con el artículo 5;

   (b) en relación con las transferencias de fondos en las que el proveedor de servicios de pago del ordenante esté establecido fuera de la Unión, la información completa sobre el ordenante y el beneficiario mencionada en el artículo 4, apartados 1 y 2, y, si procede, la información exigida en el artículo 14;

   y

   (c) en relación con las transferencias por lotes en las que el proveedor de servicios de pago del ordenante esté establecido fuera de la Unión, la información mencionada en el artículo 4, apartados 1 y 2, sobre la transferencia por lotes.

3. En las transferencias de fondos que sobrepasen los 1 000 EUR, en las que el proveedor de servicios de pago del ordenante esté establecido fuera de la Unión, el proveedor de servicios de pago del beneficiario verificará la identidad de este último cuando dicha identidad no haya sido ya verificada.

4. En las transferencias de fondos que no sobrepasen los 1 000 EUR, en las que el proveedor de servicios de pago del ordenante esté establecido fuera de la Unión, el proveedor de servicios de pago del beneficiario no tendrá que verificar la información relativa al beneficiario, salvo cuando existan sospechas de blanqueo de capitales o financiación del terrorismo.

Artículo 8

Transferencias de fondos a las que falte información o con información incompleta sobre el ordenante y el beneficiario

1. El proveedor se servicios de pago del beneficiario implantará procedimientos eficaces, basados en el riesgo, destinados a determinar cuándo ha de ejecutarse, rechazarse o suspenderse una transferencia de fondos que no contenga la información requerida sobre el ordenante y el beneficiario, así como las consiguientes medidas que deban adoptarse.

   Si, al recibir transferencias de fondos, el proveedor de servicios de pago del beneficiario constata que falta la información sobre el ordenante y el beneficiario exigida en el artículo 4, apartados 1 y 2, el artículo 5, apartado 1, y el artículo 6, o de que esta es incompleta, deberá, o bien rechazar la transferencia, o pedir información completa sobre el ordenante y el beneficiario.

2. Cuando, de forma reiterada, un proveedor de servicios de pago no facilite la información requerida sobre el ordenante, el proveedor de servicios de pago del beneficiario tomará medidas que pueden ir desde, inicialmente, emitir una advertencia o fijar un plazo, antes de rechazar toda futura transferencia de fondos de dicho proveedor de servicios de pago, hasta decidir si restringe o pone fin a la relación comercial con ese proveedor de servicios de pago.

   El proveedor de servicios de pago del beneficiario informará de ese hecho a las autoridades responsables de la lucha contra el blanqueo de capitales o la financiación del terrorismo.

Artículo 9

Evaluación y notificación

El proveedor de servicios de pago del beneficiario considerará que la falta de información sobre el ordenante y el beneficiario, o el hecho de que esta sea incompleta, constituye un factor para evaluar si la transferencia de fondos, o cualquier operación relacionada con ella, resulta sospechosa, y si debe informarse de ello a la Unidad de Información Financiera.

SECCIÓN 3

OBLIGACIONES DE LOS PROVEEDORES DE SERVICIOS DE PAGO INTERMEDIARIOS

Artículo 10

Conservación de la información sobre el ordenante y el beneficiario con la transferencia

Los proveedores de servicios de pago intermediarios se asegurarán de que toda la información recibida sobre el ordenante y el beneficiario que acompaña a una transferencia de fondos se conserve con la misma.

Artículo 11

Detección de la falta de información sobre el ordenante y el beneficiario

1. El proveedor de servicios de pago intermediario verificará, en lo que respecta a la información sobre el ordenante y el beneficiario, si los campos del sistema de mensajería o de pagos y liquidación utilizado para efectuar la transferencia de fondos han sido rellenados mediante los caracteres o entradas admisibles en el marco de los protocolos de dicho sistema.

2. Dicho proveedor deberá contar con procedimientos efectivos para detectar la falta de la siguiente información sobre el ordenante y el beneficiario:

   (a) en relación con las transferencias de fondos en las que el proveedor de servicios de pago del ordenante esté establecido en la Unión, la información exigida de conformidad con el artículo 5;

   (b) en relación con las transferencias de fondos en las que el proveedor de servicios de pago del ordenante esté establecido fuera de la Unión, la información completa sobre el ordenante y el beneficiario mencionada en el artículo 4, apartados 1 y 2, o, si procede, la información exigida en el artículo 14;

   y

   (c) en relación con las transferencias por lotes en las que el proveedor de servicios de pago del ordenante esté establecido fuera de la Unión, la información mencionada en el artículo 4, apartados 1 y 2, sobre la transferencia por lotes.

Artículo 12

Transferencias de fondos a las que falte información o con información incompleta sobre el ordenante y el beneficiario

1. El proveedor se servicios de pago intermediario implantará procedimientos eficaces, basados en el riesgo, destinados a determinar cuándo ha de ejecutarse, rechazarse o suspenderse una transferencia de fondos que no contenga la información requerida sobre el ordenante y el beneficiario, así como las consiguientes medidas que deban adoptarse.

   Si, al recibir transferencias de fondos, el proveedor de servicios de pago intermediario constata que falta la información sobre el ordenante y el beneficiario exigida por el artículo 4, apartados 1 y 2, el artículo 5, apartado 1, y el artículo 6, o de que esta es incompleta, deberá, o bien rechazar la transferencia, o pedir información completa sobre el ordenante y el beneficiario.

2. Cuando, de forma reiterada, un proveedor de servicios de pago no facilite la información requerida sobre el ordenante, el proveedor de servicios de pago intermediario tomará medidas que pueden ir desde, inicialmente, emitir una advertencia o fijar un plazo, antes de rechazar toda futura transferencia de fondos de dicho proveedor de servicios de pago, hasta decidir si restringe o pone fin a la relación comercial con ese proveedor de servicios de pago.

El proveedor de servicios de pago intermediario informará de ese hecho a las autoridades responsables de la lucha contra el blanqueo de capitales o la financiación del terrorismo.

Artículo 13

Evaluación y notificación

El proveedor de servicios de pago intermediario considerará que la falta de información sobre el ordenante y el beneficiario, o el hecho de que esta sea incompleta, constituye un factor para evaluar si la transferencia de fondos, o cualquier operación relacionada con ella, resulta sospechosa, y si debe informarse de ello a la Unidad de Información Financiera.

Artículo 14

Limitaciones técnicas

1. El presente artículo se aplicará en los casos en que el proveedor de servicios de pago del ordenante esté establecido fuera de la Unión y el proveedor de servicios de pago intermediario esté establecido en la Unión.

2. El proveedor de servicios de pago intermediario, cuando reciba una transferencia de fondos, salvo que constate que la información sobre el ordenante, necesaria con arreglo al presente Reglamento, falta o es incompleta, podrá, al enviar las transferencias de fondos al proveedor de servicios de pago del beneficiario, utilizar un sistema de pago con limitaciones técnicas que evite que la información sobre el ordenante acompañe a las transferencias de fondos.

3. El proveedor de servicios de pago intermediario, cuando reciba una transferencia de fondos, salvo que constate que la información sobre el ordenante, necesaria con arreglo al presente Reglamento, falta o es incompleta, solo utilizará un sistema de pago con limitaciones técnicas en caso de que pueda informar de este hecho al proveedor de servicios de pago del beneficiario, bien través de un sistema de mensajería o de pago que permita comunicar este hecho o mediante otro procedimiento, siempre que el modo de comunicación haya sido aceptado o acordado por ambos proveedores de servicios de pago.

4. Cuando el proveedor de servicios de pago intermediario utilice un sistema de pago con limitaciones técnicas, dicho proveedor de servicios de pago intermediario, a solicitud del proveedor de servicios de pago del beneficiario, pondrá a disposición de este toda la información que haya recibido sobre el ordenante, esté o no completa, en el plazo de tres días hábiles desde la recepción de dicha solicitud.

CAPÍTULO III

COOPERACIÓN Y CONSERVACIÓN DE LA INFORMACIÓN

Artículo 15

Obligación de cooperar

Los proveedores de servicios de pago responderán plenamente y sin demora, de conformidad con los requisitos de procedimiento previstos en el Derecho nacional del Estado miembro en el que estén establecidos, a las indagaciones de las autoridades responsables de la lucha contra el blanqueo de capitales o la financiación del terrorismo de dicho Estado miembro en lo relativo a la información exigida por el presente Reglamento.

Artículo 16

Conservación de la información

El proveedor de servicios de pago del ordenante y el proveedor de servicios de pago del beneficiario conservarán durante cinco años la información a que se refieren los artículos 4, 5, 6 y 7. En los supuestos a que se refiere el artículo 14, apartados 2 y 3, el proveedor de servicios de pago intermediario conservará toda la información recibida durante cinco años. Una vez transcurrido ese plazo, deberán eliminarse los datos personales, salvo disposición en contrario del Derecho nacional, que deberá especificar en qué circunstancias los proveedores de servicios de pago podrán o deberán conservar datos. Los Estados miembros podrán autorizar o exigir un plazo mayor de conservación únicamente si fuera

necesario a efectos de la prevención, detección o investigación del blanqueo de capitales y la financiación del terrorismo. El plazo máximo de conservación tras la realización de la transferencia de fondos no podrá exceder de diez años.

CAPÍTULO IV

SANCIONES Y SEGUIMIENTO

Artículo 17

Sanciones

1. Los Estados miembros establecerán las normas en materia de medidas y sanciones administrativas aplicables en caso de incumplimiento de las disposiciones del presente Reglamento y adoptarán todas las medidas necesarias para garantizar su aplicación. Las sanciones establecidas deberán ser eficaces, proporcionadas y disuasorias.

2. Los Estados miembros velarán por que cuando los proveedores de servicios de pago estén sujetos a obligaciones, puedan aplicarse sanciones, en caso de incumplimiento, a los miembros del órgano de dirección y a las demás personas físicas responsables de la infracción con arreglo al Derecho nacional.

3. El [*24 meses después de la entrada en vigor del presente Reglamento*] a más tardar, los Estados miembros notificarán las normas a que se refiere el apartado 1 a la Comisión y al Comité Mixto de la ABE, la AESPJ y la AEVM. Notificarán a la Comisión y al Comité Mixto de la ABE, la AESPJ y la AEVM sin demora cualquier modificación ulterior de las mismas.

4. Se otorgarán a las autoridades competentes todas las facultades de investigación necesarias para el ejercicio de sus funciones. Al ejercer sus facultades sancionadoras, las autoridades competentes cooperarán estrechamente para garantizar que las sanciones o medidas ofrezcan los resultados deseados, y coordinarán su actuación en el ámbito transfronterizo .

Artículo 18

Disposiciones específicas

1. El presente artículo se aplicará en los siguientes casos:

   (a) la reiterada omisión de información obligatoria sobre el ordenante y el beneficiario, en contravención de lo dispuesto en los artículos 4, 5, y 6;

   (b) el incumplimiento grave de los proveedores de servicios de pago a la hora de garantizar la conservación de la información conforme al artículo 16;

   (c) el incumplimiento del proveedor de servicios de pago en lo que atañe a la obligación de implantar políticas y procedimientos eficaces, basados en el riesgo, conforme a lo dispuesto en los artículos 8 y 12.

2. En los casos a que se refiere el apartado 1, entre las sanciones y medidas administrativas aplicables figurarán como mínimo las siguientes:

   (a) una declaración pública que indique la persona física o jurídica y la naturaleza de la infracción;

   (b) un requerimiento dirigido a la persona física o jurídica para que ponga fin a su conducta y se abstenga de repetirla;

   (c) en el caso de un proveedor de servicios de pago, retirada de la autorización;

   (d) la imposición de una prohibición temporal de ejercer funciones en el proveedor de servicios de pago a cualquiera de los miembros del órgano de dirección o cualquier otra persona física que se considere responsable;

   (e) si se trata de una persona jurídica, sanciones pecuniarias administrativas de hasta el 10 % de su volumen de negocios total anual en el ejercicio anterior; cuando la persona jurídica sea una filial de una empresa matriz, el volumen de negocios total anual pertinente será el volumen de negocios total anual resultante de las cuentas consolidadas de la empresa matriz última en el ejercicio anterior;

(f) si se trata de una persona física, sanciones pecuniarias administrativas de hasta 5 000 000 EUR, o, en los Estados miembros en los que el euro no es la moneda oficial, el valor correspondiente en la moneda nacional en la fecha de entrada en vigor de la presente Directiva;

(g) sanciones pecuniarias administrativas de hasta el doble del importe de los beneficios obtenidos o de las pérdidas evitadas gracias al incumplimiento, en caso de que puedan determinarse.

Artículo 19

Publicación de las sanciones

Las sanciones y medidas administrativas impuestas en los casos a que se refiere el artículo 17 y el artículo 18, apartado 1, se publicarán sin demora injustificada, en particular información sobre el tipo y la naturaleza del incumplimiento y la identidad de las personas responsables del mismo, a menos que dicha publicación pueda comprometer gravemente la estabilidad de los mercados financieros.

Cuando la publicación pueda causar un daño desproporcionado a las partes implicadas, las autoridades competentes publicarán las sanciones de manera anónima.

Artículo 20

Aplicación de las sanciones por las autoridades competentes

A la hora de determinar el tipo de sanciones o medidas administrativas y el nivel de las sanciones pecuniarias administrativas, las autoridades competentes tendrán en cuenta todas las circunstancias pertinentes, entre ellas:

(a) la gravedad y duración de la infracción;

(b) el grado de responsabilidad de la persona física o jurídica responsable;

(c) la solidez financiera de la persona física o jurídica responsable, reflejada en el volumen de negocios total de la persona jurídica responsable o en los ingresos anuales de la persona física responsable;

(d) la importancia de los beneficios obtenidos o las pérdidas evitadas por la persona física o jurídica responsable, en la medida en que puedan determinarse;

(e) las pérdidas para terceros causadas por la infracción, en la medida en que puedan determinarse;

(f) el nivel de cooperación de la persona física o jurídica responsable con la autoridad competente;

(g) las infracciones anteriores de la persona física o jurídica responsable.

Artículo 21

Notificación de incumplimientos

1. Los Estados miembros establecerán mecanismos eficaces para alentar la notificación del incumplimiento del presente Reglamento a las autoridades competentes.

2. Los mecanismos contemplados en el apartado 1 incluirán, como mínimo:

(a) procedimientos específicos para la recepción de informes sobre incumplimientos y su seguimiento;

(b) protección adecuada de los denunciantes de incumplimientos potenciales o reales;

(c) protección de los datos personales relativos tanto a las personas que notifican un incumplimiento como a la persona física presuntamente responsable del mismo, de conformidad con los principios establecidos en la Directiva 95/46/CE.

3. Los proveedores de servicios de pago establecerán procedimientos adecuados para que sus empleados puedan comunicar incumplimientos a nivel interno a través de un cauce específico.

Artículo 22

Seguimiento

Los Estados miembros exigirán a las autoridades competentes que supervisen de forma efectiva y tomen las medidas necesarias para garantizar el cumplimiento de lo dispuesto en el presente Reglamento.

CAPÍTULO V

PODERES DE EJECUCIÓN

Artículo 23

Procedimiento de comité

1. La Comisión estará asistida por el Comité sobre Prevención del Blanqueo de Capitales y Financiación del Terrorismo, en lo sucesivo denominado «el Comité». Dicho comité será un comité a tenor de lo dispuesto en el Reglamento (UE) nº 182/2011.

2. En los casos en que se haga referencia al presente apartado será de aplicación el artículo 5 del Reglamento (UE) nº 182/2011.

CAPÍTULO VI

EXENCIONES

Artículo 24

Acuerdos con los territorios o países mencionados en el artículo 355 del Tratado

1. La Comisión podrá autorizar a cualquier Estado miembro a celebrar acuerdos, en el marco de disposiciones nacionales, con un país o territorio que no forme parte del territorio de la Unión definido en el artículo 355 del Tratado, que prevean excepciones al presente Reglamento, con el fin de permitir que las transferencias de fondos entre ese país o territorio y el Estado miembro correspondiente sean tratadas como transferencias de fondos realizadas en ese Estado miembro.

   Estos acuerdos sólo podrán autorizarse si se cumplen todas las condiciones siguientes:

   (a) que el país o el territorio en cuestión comparta una unión monetaria con el Estado miembro de que se trate, forme parte de la zona monetaria de ese Estado miembro o haya firmado un convenio monetario con la Unión representada por un Estado miembro;

   (b) que los proveedores de servicios de pago del país o territorio en cuestión participen, directa o indirectamente, en los sistemas de pago y liquidación de dicho Estado miembro,

   y

   (c) que el país o el territorio en cuestión exija que los proveedores de servicios de pago bajo su jurisdicción apliquen las mismas normas que se establecen en el presente Reglamento.

2. Todo Estado miembro que desee celebrar un acuerdo según lo mencionado en el apartado 1 enviará una petición a la Comisión y le facilitará toda la información necesaria.

   Cuando la Comisión reciba una petición de un Estado miembro, las transferencias de fondos entre ese Estado miembro y el país o territorio correspondiente se tratarán provisionalmente como transferencias de fondos realizadas en ese Estado miembro hasta que se alcance una decisión de conformidad con el procedimiento establecido en el presente artículo.

   Si la Comisión considera que no cuenta con toda la información necesaria, se pondrá en contacto con el Estado miembro de que se trate en el plazo de dos meses desde el momento en que reciba la petición y especificará la información adicional que necesita.

   Una vez que la Comisión cuente con toda la información que considere necesaria para valorar la petición, se lo notificará debidamente al Estado miembro solicitante en el plazo de un mes y transmitirá la petición a los demás Estados miembros.

3. En el plazo de tres meses desde la notificación mencionada en apartado 2, párrafo cuarto, la Comisión decidirá, de conformidad con el procedimiento mencionado en el artículo 23, apartado 2, si autorizar al Estado miembro correspondiente a celebrar el acuerdo mencionado en el apartado 1 del presente artículo.

   En cualquier caso, la decisión a que se refiere el párrafo primero se adoptará en el plazo de dieciocho meses a contar desde el momento en que la Comisión reciba la petición.

CAPÍTULO VII

DISPOSICIONES FINALES.

Artículo 25

Derogación

Queda derogado el Reglamento (CE) nº 1781/2006.

Las referencias al Reglamento derogado se entenderán hechas al presente Reglamento y se leerán con arreglo a la tabla de correspondencias que figura en el anexo.

Artículo 26

Entrada en vigor

El presente Reglamento entrará en vigor el vigésimo día siguiente al de su publicación en el *Diario Oficial de la Unión* Europea.

Será aplicable a partir del [*fecha de transposición de la Directiva xxxx/yyyy*].

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Estrasburgo, el

Por el Parlamento Europeo
El Presidente

Por el Consejo
El Presidente

N. de la R.: La documentació que acompanya aquesta proposta pot ésser consultada a l'Arxiu del Parlament.

Tramesa a la Comissió

Comissió competent: Comissió d'Economia, Finances i Pressupost.
Acord: Presidència del Parlament, 13.02.2013.

Termini de formulació d'observacions

Termini: 4 dies hàbils (del 19.02.2013 al 22.02.2013).
Finiment del termini: 25.02.2013; 09:30 h.
Acord: Presidència del Parlament, 13.02.2013.

Control del principi de subsidiarietat amb relació a la Proposta de directiva del Parlament Europeu i del Consell relativa a les mesures per a garantir un alt nivell comú de seguretat de les xarxes i de la informació a la Unió
Tram. 295-00017/10

Text presentat
Tramesa de la Secretaria de la Comissió Mixta de la Unió Europea del 13.02.2013
Reg. 2624 / Admissió a tràmit: Presidència del Parlament, 13.02.2013

Asunto: Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión [COM(2013) 48 final] [2013/0027 (COD)] {SWD(2013) 31 final} {SWD(2013) 32 final}

En aplicación del artículo 6.1 de la Ley 8/1994, de 19 de mayo, la Comisión Mixta para la Unión Europea remite a su Parlamento, por medio del presente correo electrónico, la iniciativa legislativa de la Unión Europea que se acompaña, a efectos de su conocimiento y para que, en su caso, remita a las Cortes Generales un dictamen motivado que exponga las razones por las que considera que la referida iniciativa de la Unión Europea no se ajusta al principio de subsidiariedad.

Aprovecho la ocasión para recordarle que, de conformidad con el artículo 6.2 de la mencionada Ley 8/1994, el dictamen motivado que, en su caso, apruebe su Institución debería ser recibido por las Cortes Generales en el plazo de cuatro semanas a partir de la remisión de la iniciativa legislativa europea.

Con el fin de agilizar la transmisión de los documentos en relación con este procedimiento de control del principio de subsidiariedad, le informo que se ha habilitado el siguiente correo electrónico de la Comisión Mixta para la Unión Europea: cmue@congreso.es

Secretaría de la Comisión Mixta para la Unión Europea

Bruselas, 7.2.2013
COM(2013) 48 final
2013/0027 (COD)

Propuesta de

DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión

{SWD(2013) 31 final}
{SWD(2013) 32 final}

EXPOSICIÓN DE MOTIVOS

El objetivo de la Directiva propuesta es garantizar un elevado nivel común de seguridad de las redes y de la información (SRI). Para ello es preciso aumentar la seguridad de Internet y de las redes y los sistemas de información privados que sustentan el funcionamiento de nuestras sociedades y economías. A fin de alcanzar dicho objetivo, es necesario, por una parte, instar a los Estados miembros a estar más preparados e incrementar la cooperación entre ellos, y, por otra, exigir a los operadores de infraestructuras críticas tales como la energía o los transportes, a los proveedores clave de servicios de la sociedad de la información (plataformas de comercio electrónico, redes sociales, etc.) y a las administraciones públicas que adopten las medidas oportunas para gestionar los riesgos de seguridad y notificar los incidentes graves a las autoridades nacionales competentes.

Esta propuesta se presenta en relación con la Comunicación conjunta de la Comisión y la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad sobre una estrategia europea de ciberseguridad. La finalidad de dicha estrategia es garantizar un entorno digital seguro y fiable, sin olvidar la promoción y la protección de los derechos fundamentales y otros valores esenciales de la UE. La presente propuesta es el principal instrumento de la estrategia, que en este ámbito incluye asimismo otras medidas centradas en la concienciación, el desarrollo de un mercado interior de productos y servicios de ciberseguridad, y el fomento de las inversiones en I+D. Estas medidas se complementarán con otras destinadas a intensificar la lucha contra la ciberdelincuencia y elaborar una política internacional de ciberseguridad para la UE.

1.1. Motivación y objetivos de la propuesta

La SRI está adquiriendo una importancia creciente para nuestra economía y nuestra sociedad. También es un requisito previo imprescindible para crear un entorno fiable para el comercio mundial de servicios. Los sistemas de información, empero, pueden verse afectados por incidentes relacionados con la seguridad tales como errores humanos, fenómenos naturales, fallos técnicos o ataques malintencionados. La envergadura, frecuencia y complejidad de estos incidentes es cada vez mayor. Según la consulta pública en línea de la Comisión sobre la mejora de la seguridad de las redes y de la información en la UE[1], el 57 % de los participantes en ella habían sufrido a lo largo del año anterior incidentes de SRI que habían tenido graves consecuencias en sus actividades. La falta de SRI puede llegar a comprometer servicios vitales que dependen de la integridad de las redes y los sistemas de información, interrumpiendo las actividades de las empresas, generando cuantiosas pérdidas financieras para la economía de la UE e incidiendo negativamente en el bienestar de la sociedad.

Por otra parte, al tratarse de instrumentos de comunicación sin fronteras, los sistemas de información digitales —y en particular Internet— están interconectados entre los Estados miembros y contribuyen decisivamente a facilitar la circulación transfronteriza de bienes, servicios y personas. Un problema grave de estos sistemas en un Estado miembro puede afectar a otros Estados miembros y a la UE en su conjunto. Por consiguiente, la resiliencia y la estabilidad de las redes y los sistemas de información revisten suma importancia para la realización del mercado único digital y el buen funcionamiento del mercado interior. La mayor probabilidad o frecuencia de los incidentes y la incapacidad de ofrecer protección suficiente minan asimismo la confianza de los ciudadanos en los servicios de red e información. Así, por ejemplo, el Eurobarómetro de 2012 sobre ciberseguridad señalaba que al 38 % de los usuarios de Internet en la UE le preocupa la seguridad de los pagos en línea y ha modificado su comportamiento en consecuencia: probablemente un 18 % comprará menos en Internet y un 15 % no utilizará tanto los servicios bancarios en línea[2].

La situación actual en la UE es reflejo del planteamiento meramente voluntario seguido hasta el momento, que no ofrece protección suficiente frente a incidentes y riesgos relacionados con la SRI en la UE. Las capacidades y mecanismos de SRI actuales son sencillamente insuficientes para seguir el ritmo de unas amenazas en rápida mutación y garantizar un nivel elevado de protección igual en todos los Estados miembros.

Pese a las iniciativas emprendidas, los niveles de capacidad y preparación de los Estados miembros son muy distintos y dan lugar a enfoques fragmentados en la UE. Al estar redes y sistemas interconectados, la SRI global de la UE se ve perjudicada por esos Estados miembros cuyo nivel de protección es insuficiente. Esta situación dificulta asimismo la creación de lazos de confianza entre homólogos, requisito previo para la cooperación y el intercambio de información. Como consecuencia de ello, solamente mantienen relaciones de cooperación unos pocos Estados miembros con elevado nivel de capacidades.

Actualmente no existe, por tanto, un mecanismo efectivo a escala de la UE que haga posible una labor de cooperación y colaboración eficaz y un intercambio de información de confianza sobre incidentes y riesgos de SRI entre los Estados miembros. Estas carencias pueden dar lugar a intervenciones reglamentarias no coordinadas, estrategias incoherentes y normas divergentes, que a su vez llevan aparejada una protección insuficiente ante los problemas de SRI en toda la UE. Pueden incluso surgir obstáculos al mercado interior que generen gastos de observancia a las empresas que operan en más de un Estado miembro.

Por último, a los agentes que gestionan infraestructuras críticas o prestan servicios esenciales para el funcionamiento de nuestras sociedades no se les han impuesto las oportunas obligaciones de adoptar medidas de gestión de riesgos ni de intercambiar información con las autoridades competentes. Así pues, por una parte, no se ofrecen a las empresas incentivos reales para proceder a una gestión de riesgos como es debido, con una evaluación del riesgo y la adopción de medidas adecuadas para garantizar la SRI. Por otra parte, un elevado porcentaje de incidentes no llega a conocimiento de las autoridades competentes y pasa desapercibido. Y, sin embargo, la información sobre los incidentes es esencial para que las autoridades públicas reaccionen, adopten las medidas de atenuación apropiadas y fijen las prioridades estratégicas oportunas en materia de SRI.

El actual marco regulador solamente obliga a las empresas de telecomunicaciones a adoptar medidas de gestión de riesgos y a notificar los incidentes graves que ponen en peligro la SRI. No obstante, hay muchos otros sectores cuyo

1 La consulta pública en línea sobre la mejora de la seguridad de las redes y de la información en la UE se desarrolló del 23 de julio al 15 de octubre de 2012.

2 Eurobarómetro 390/2012.

desarrollo depende de las TIC y que, por ende, deberían también prestar la debida atención a la SRI. Algunos proveedores de infraestructuras y servicios específicos son especialmente vulnerables al ser muy dependientes del correcto funcionamiento de las redes y los sistemas de información. Tales sectores desempeñan una función primordial, pues prestan servicios de apoyo cruciales para nuestra economía y nuestra sociedad, y la seguridad de sus sistemas reviste especial importancia para el funcionamiento del mercado interior. Entre estos sectores cabe citar la banca, la bolsa, la generación, el transporte y la distribución de energía, los transportes (aéreo, ferroviario y marítimo), la sanidad, los servicios de Internet y las administraciones públicas.

Así pues, en la UE hay que abordar la SRI de forma radicalmente distinta. Es necesario imponer obligaciones reglamentarias para establecer condiciones uniformes y colmar las actuales lagunas jurídicas. A fin de hacer frente a estos problemas e incrementar el nivel de SRI en toda la Unión Europea, la Directiva propuesta fija los objetivos que a continuación se exponen.

En primer lugar, la propuesta impone a todos los Estados miembros la obligación de velar por que exista un nivel mínimo de capacidades nacionales mediante la designación de autoridades competentes en materia de SRI, la creación de equipos de respuesta a emergencias informáticas (CERT) y la adopción de estrategias y planes de cooperación nacionales en el ámbito de la SRI.

En segundo lugar, las autoridades nacionales competentes deberán cooperar dentro de una red que garantice una coordinación segura y eficaz y, en particular, un intercambio coordinado de información y unas labores de detección y respuesta a escala de la UE. A través de esta red, los Estados miembros deberán intercambiar información y cooperar para hacer frente a las amenazas e incidentes que puedan poner en peligro la SRI sobre la base del plan de cooperación europeo en materia de SRI.

En tercer lugar, siguiendo el modelo de la Directiva Marco sobre las comunicaciones electrónicas, la propuesta pretende implantar una cultura de gestión de riesgos y garantizar el intercambio de información entre los sectores público y privado. Las empresas de los sectores críticos concretos antes citados y las administraciones públicas deberán evaluar los riesgos a que se enfrentan y adoptar medidas adecuadas y proporcionadas para garantizar la SRI. Estas empresas deberán notificar a las autoridades competentes todos los incidentes que supongan un peligro grave para el funcionamiento de sus redes y sistemas de información y comprometan de forma significativa la continuidad de los servicios críticos y el suministro de mercancías.

1.2. Contexto general

Ya en su Comunicación de 2001 titulada *Seguridad de las redes y de la información: Propuesta para un enfoque político europeo*, la Comisión destacaba la creciente importancia de la SRI[3]. Posteriormente, en 2006 se adoptó una estrategia para una sociedad de la información segura[4], que tenía como objetivo desarrollar una cultura de SRI en Europa. Sus principales aspectos fueron aprobados en una Resolución del Consejo[5].

El 30 de marzo de 2009, la Comisión adoptó una Comunicación sobre protección de infraestructuras críticas de información (PICI)[6], cuya finalidad era proteger a Europa de las ciberperturbaciones impulsando una mayor seguridad. En dicha Comunicación se presentaba un plan de acción para respaldar a los Estados miembros en sus esfuerzos de prevención y respuesta. El plan de acción se aprobó en las Conclusiones de la Presidencia de la Conferencia Ministerial sobre PICI celebrada en Tallin en 2009. El 18 de diciembre de 2009, el Consejo adoptó una Resolución relativa a un planteamiento de colaboración en materia de seguridad de las redes y de la información[7].

La Agenda Digital para Europa (ADE)[8], adoptada en mayo de 2010, y las conclusiones del Consejo correspondientes[9] ponían de relieve la convicción común de que la confianza y la seguridad son condiciones previas fundamentales para la adopción a gran escala de las TIC y, por ende, para el logro de los objetivos de una de las dimensiones de la Estrategia Europa 2020, la denominada «crecimiento inteligente»[10]. En su capítulo dedicado a la confianza y la seguridad, la ADE insistía en la necesidad de que todas las partes interesadas se unieran en un esfuerzo conjunto para garantizar la seguridad y la resiliencia de las infraestructuras de las TIC, centrándose en la prevención, la preparación y la sensibilización al objeto de desarrollar unos mecanismos de seguridad eficaces y coordinados. En particular, la acción clave 6 de la Agenda Digital para Europa instaba a adoptar medidas encaminadas a conseguir una política de SRI reforzada y de alto nivel.

En su Comunicación de marzo de 2011 sobre la protección de infraestructuras críticas de información titulada *Logros y próximas etapas: hacia la ciberseguridad global*[11], la Comisión hacía balance de los resultados logrados desde la

3 COM(2001) 298.
4 COM(2006) 251 http://eur-lex.europa.eu/LexUriServ/site/es/com/2006/com2006_0251es01.pdf.
5 2007/068/01.
6 COM(2009) 149.
7 2009/C 321/01.
8 COM(2010) 245.
9 Conclusiones del Consejo de 31 de mayo de 2010 sobre la Agenda Digital para Europa (10130/10).
10 COM(2010) 2020 y Conclusiones del Consejo Europeo de 25 y 26 de marzo de 2010 (EUCO 7/10).
11 COM(2011) 163.

adopción del plan de acción sobre la PICI en 2009 y concluía que la aplicación del plan demostraba que los enfoques puramente nacionales no bastaban para abordar cuestiones de seguridad y resiliencia y que Europa debía seguir esforzándose por construir una estrategia coherente y cooperativa para toda la UE. En la Comunicación sobre la PICI de 2011 se anunciaba una serie de medidas y la Comisión instaba a los Estados miembros a crear capacidades y mantener una cooperación transfronteriza en materia de SRI. La mayor parte de esas medidas tenía que haberse completado en 2012, pero aún no se ha llevado a la práctica.

En sus conclusiones de 27 de mayo de 2011 sobre la PICI, el Consejo de la Unión Europea subrayaba la acuciante necesidad de contar con unos sistemas y redes de TIC resilientes y seguros frente a todas las perturbaciones posibles, accidentales o intencionadas, lograr en toda la UE un nivel elevado de preparación, seguridad y resiliencia, mejorar las competencias técnicas a fin de que Europa pueda responder a los desafíos en materia de protección de las redes y las infraestructuras de información, e impulsar la cooperación entre los Estados miembros mediante el establecimiento de mecanismos de cooperación ante incidentes.

1.3. Disposiciones internacionales y de la Unión Europea existentes en este ámbito

En virtud del Reglamento (CE) nº 460/2004, la Comunidad Europea creó en 2004 la Agencia Europea de Seguridad de las Redes y de la Información (ENISA)[12] con el fin de contribuir a garantizar un elevado nivel de SRI y desarrollar una cultura en este ámbito en toda la UE. El 30 de septiembre de 2010 se adoptó una propuesta para modernizar el mandato de la ENISA[13], que se está debatiendo actualmente en el Consejo y el Parlamento Europeo. El marco regulador revisado de los servicios de comunicaciones electrónicas[14], en vigor desde noviembre de 2009, impone obligaciones en materia de seguridad a los proveedores de servicios de comunicaciones electrónicas[15]. Dichas obligaciones tenían que estar incorporadas a los ordenamientos jurídicos nacionales en mayo de 2011.

El marco regulador de protección de datos[16] obliga a todos los agentes que actúan como responsables del tratamiento de los datos (por ejemplo, bancos u hospitales) a implantar medidas de seguridad para proteger los datos personales. Asimismo, la propuesta de Reglamento general de protección de datos[17], presentada por la Comisión en 2012, establece que los responsables del tratamiento deben notificar los casos de violación de datos personales a las autoridades nacionales de control. Así pues, una violación de la SRI que afectara a la prestación de un servicio sin comprometer datos personales (por ejemplo, una avería de las TIC en una compañía eléctrica que ocasionara la interrupción del servicio) no debería notificarse.

Al amparo de la Directiva 2008/114/CE sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, el Programa Europeo de Protección de Infraestructuras Críticas (PEPIC)[18] establece el marco global para la protección de las infraestructuras críticas en la UE. Los objetivos del PEPIC coinciden plenamente con los de la presente propuesta y la Directiva debería aplicarse sin perjuicio de la Directiva 2008/114/CE. El PEPIC no obliga a los operadores a notificar violaciones significativas de la seguridad ni establece mecanismos para que los Estados miembros cooperen y respondan ante los incidentes que se produzcan.

Los colegisladores están examinando actualmente la propuesta de Directiva de la Comisión relativa a los ataques contra los sistemas de información[19], que tiene como objetivo armonizar la tipificación como delitos de determinados tipos de conducta. Dicha propuesta abarca solamente la tipificación de determinados tipos de conducta y no aborda la prevención de riesgos e incidentes de SRI, la respuesta a los incidentes de SRI ni la atenuación de sus efectos. La presente Directiva debe aplicarse sin perjuicio de la Directiva relativa a los ataques contra los sistemas de información.

El 28 de marzo de 2012, la Comisión adoptó una Comunicación sobre la creación de un centro europeo de ciberdelincuencia (EC3)[20]. Este Centro, creado el 11 de enero de 2013, está integrado en la Oficina Europea de Policía (Europol) y funcionará como punto central en la lucha contra la ciberdelincuencia en la UE. El EC3 está destinado a aunar los conocimientos sobre ciberdelincuencia europeos para contribuir a la capacitación de los Estados miembros, a prestar apoyo a los Estados miembros en investigaciones de ciberdelincuencia y, en estrecha cooperación con Eurojust, a ser la voz colectiva de los investigadores de ciberdelincuencia europeos ante los organismos de orden público y el estamento judicial.

Las instituciones, agencias y organismos europeos han creado su propio equipo de respuesta a emergencias informáticas, denominado CERT-UE.

---

12 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:ES:HTML.

13 COM(2010) 521.

14 Véase http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf.

15 Artículos 13 *bis* y 13 *ter* de la Directiva Marco.

16 Directiva 2002/58/CE de 12 de julio de 2002.

17 COM(2012) 11.

18 COM(2006) 786, http://eur-lex.europa.eu/LexUriServ/site/es/com/2006/com2006_0786es01.pdf.

19 COM(2010) 517, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:ES:PDF.

20 COM(2012) 140 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:ES:PDF.

A escala internacional, la UE desarrolla actividades bilaterales y multilaterales en el ámbito de la ciberseguridad. Con motivo de la Cumbre UE-EE.UU. de 2010[21], se creó el Grupo de Trabajo UE-EE.UU. sobre Ciberseguridad y Ciberdelincuencia. La UE también participa en otros foros multilaterales tales como la Organización de Cooperación y Desarrollo Económicos (OCDE), la Asamblea General de las Naciones Unidas (AGNU), la Unión Internacional de Telecomunicaciones (UIT), la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Cumbre Mundial sobre la Sociedad de la Información (CMSI) y el Foro para la Gobernanza de Internet (IGF).

2. RESULTADOS DE LAS CONSULTAS CON LAS PARTES INTERESADAS Y DE LAS EVALUACIONES DE IMPACTO

2.1. Consulta con las partes interesadas y utilización de asesoramiento técnico

Del 23 de julio al 15 de octubre de 2012 estuvo abierta en línea una consulta pública sobre la mejora de la SRI en la UE. La Comisión recibió un total de 160 respuestas al cuestionario en línea.
La principal conclusión que puede extraerse de esas respuestas es el reconocimiento generalizado de la necesidad de aumentar la SRI en toda la UE. Más concretamente, el 82,8 % de los participantes en la consulta señala que los Gobiernos de la UE deberían adoptar más medidas para garantizar un elevado nivel de SRI; también el 82,8 % opina que los usuarios de sistemas de información no son conscientes de las amenazas e incidentes de SRI existentes; el 66,3 % estaría, en principio, a favor de la introducción de requisitos reglamentarios para gestionar los riesgos de SRI; y el 84,8 % afirma que tales requisitos se han de establecer a escala de la UE. Muchas respuestas indican que sería importante adoptar requisitos de SRI en los siguientes sectores específicos: banca y finanzas (91,1 %), energía (89,4 %), transportes (81,7 %), sanidad (89,4 %), servicios de Internet (89,1 %) y administraciones públicas (87,5 %). Los participantes en la consulta también consideran que, de introducirse la obligación de notificar violaciones de la SRI a la autoridad nacional competente, sería preciso hacerlo a escala de la UE (65,1 %) y estiman que las administraciones públicas también han de estar sujetas a esa obligación (93,5 %). Por último, afirman que la obligación de proceder a la gestión de riesgos de SRI de acuerdo con los conocimientos tecnológicos actuales no les supondría costes adicionales significativos (63,4 %), como tampoco se los supondría la obligación de notificar violaciones de la seguridad (72,3 %).
Se consultó a los Estados miembros en varias formaciones del Consejo, en el contexto del Foro Europeo de Estados Miembros (EFMS) en la Conferencia sobre Ciberseguridad organizada por la Comisión y el Servicio Europeo de Acción Exterior el 6 de julio de 2012, así como en reuniones bilaterales dedicadas a este tema que se convocaron a petición de algunos Estados miembros.

También se entablaron conversaciones con el sector privado en el marco de la Asociación público-privada europea de resiliencia[22] y a través de reuniones bilaterales. En cuanto al sector público, la Comisión mantuvo contactos con la ENISA y el CERT de las instituciones de la UE.

2.2. Evaluación de impacto

La Comisión ha efectuado una evaluación de impacto con respecto a tres opciones de actuación:

1ª opción: Mantenimiento del enfoque actual (hipótesis de referencia).

2ª opción: Enfoque reglamentario, con la presentación de una propuesta legislativa que establezca un marco jurídico común en materia de SRI para toda la UE y abarque las capacidades de los Estados miembros, los mecanismos de cooperación a escala de la UE y los requisitos que han de cumplir los principales agentes del sector privado y las administraciones públicas.

3ª opción: Enfoque mixto que combine las iniciativas de carácter voluntario en lo que respecta a las capacidades de los Estados miembros en el ámbito de la SRI y los mecanismos de cooperación a escala de la UE con requisitos reglamentarios aplicables a los principales agentes del sector privado y las administraciones públicas.

En opinión de la Comisión, la 2ª opción es la que puede tener mayores efectos positivos, pues incrementaría considerablemente la protección de consumidores, empresas y administraciones de la UE frente a los incidentes de SRI. Más concretamente, las obligaciones impuestas a los Estados miembros garantizarían la debida preparación a escala nacional y contribuirían a lograr un clima de confianza mutua, que es condición previa para una cooperación eficaz en la UE. La creación de mecanismos de cooperación a escala de la UE a través de una red facilitaría la adopción de medidas de prevención y respuesta coherentes y coordinadas ante incidentes y riesgos de SRI de carácter transfronterizo. Imponer a las administraciones públicas y a los principales agentes del sector privado la obligación de aplicar medidas de gestión de riesgos en el ámbito de la SRI supondría un poderoso incentivo para hacer frente con eficacia a los riesgos de seguridad. La obligación de notificar los incidentes de SRI con efectos significativos mejoraría la capacidad de respuesta a incidentes y fomentaría la transparencia. Por lo demás, al poner sus propios asuntos en orden, la UE podría ampliar su influencia internacional y convertirse en un socio todavía más fiable en las labores de

21 http://europa.eu/rapid/press-release_MEMO-10-597_en.htm.

22 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r.

cooperación bilateral y multilateral. Así pues, la UE se encontraría mejor situada para promover los derechos fundamentales y los valores esenciales de la Unión en el exterior.

La evaluación cuantitativa muestra que la 2ª opción no impondría una carga desproporcionada a los Estados miembros. Los costes que generaría para el sector privado también serían limitados por cuanto muchas de las entidades en cuestión ya están obligadas a cumplir los requisitos de seguridad existentes (los responsables del tratamiento de datos deben adoptar medidas técnicas y de organización, entre ellas medidas de SRI, para proteger los datos personales). También se han tomado en consideración los gastos de seguridad actuales en el sector privado.

La presente propuesta observa los principios reconocidos por la Carta de los Derechos Fundamentales de la Unión Europea y, en particular, el derecho al respeto de la vida privada y las comunicaciones, el derecho a la protección de los datos de carácter personal, el derecho a la libertad de empresa, el derecho a la propiedad, el derecho a una tutela judicial efectiva y el derecho a ser oído. La presente Directiva se deberá aplicar de acuerdo con estos derechos y principios.

3. ASPECTOS JURÍDICOS DE LA PROPUESTA

3.1. Base jurídica

La Unión Europea posee competencias para adoptar medidas destinadas a establecer el mercado interior o garantizar su funcionamiento, de conformidad con las disposiciones pertinentes de los Tratados (artículo 26 del Tratado de Funcionamiento de la Unión Europea — TFUE). En virtud del artículo 114 del TFUE, la UE puede adoptar «medidas relativas a *la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros* que tengan por objeto el establecimiento o el funcionamiento del mercado interior».

Como ya se ha indicado, las redes y los sistemas de información contribuyen de forma decisiva a facilitar la circulación transfronteriza de bienes, servicios y personas. A menudo están interconectados y huelga decir que la Internet tiene carácter global. Dada su dimensión transnacional intrínseca, una perturbación en un Estado miembro puede afectar también a otros Estados miembros y a la UE en su conjunto. Por consiguiente, la resiliencia y la estabilidad de las redes y los sistemas de información son esenciales para el buen funcionamiento del mercado interior.

El legislador de la UE ya ha reconocido la necesidad de armonizar las normas de SRI para asegurar el desarrollo del mercado interior. Cabe destacar a este respecto el Reglamento (CE) nº 460/2004 por el que se crea la ENISA[23], basado en el artículo 114 del TFUE.

Las grandes diferencias entre Estados miembros en lo que a capacidades, políticas y niveles de protección en materia de SRI se refiere han dado lugar a disparidades que representan un obstáculo para el mercado interior y justifican la actuación de la UE.

3.2. Subsidiariedad

La intervención europea en el campo de la SRI está justificada por el principio de subsidiariedad.

En primer lugar, dado el carácter transfronterizo de la SRI, de no intervenir la UE, cada Estado miembro actuaría por su cuenta, haciendo caso omiso de las interdependencias entre las redes y los sistemas de información de la UE. Un grado suficiente de coordinación entre los Estados miembros garantizaría una gestión correcta de los riesgos de SRI en el contexto transfronterizo en que surgen. Las divergencias entre las normativas sobre SRI representan una barrera para las empresas que quieren desarrollar sus actividades en varios países y para la consecución de economías de escala a nivel mundial.

En segundo lugar, es preciso imponer obligaciones reglamentarias a escala de la UE para lograr condiciones uniformes y colmar las lagunas jurídicas. Se ha demostrado que los planteamientos de carácter meramente voluntario dan lugar a una cooperación limitada a una minoría de Estados miembros con elevado nivel de capacidades. Para conseguir la participación de todos los Estados miembros, es necesario cerciorarse de que todos ellos poseen el nivel mínimo de capacidades requerido. Las medidas adoptadas por los Gobiernos para garantizar la SRI han de guardar coherencia unas con otras y estar coordinadas de modo que sea posible contener y reducir al mínimo las consecuencias de incidentes que pongan en peligro la SRI. En el marco de la red, a través del intercambio de las mejores prácticas y de la colaboración permanente de la ENISA, las autoridades competentes y la Comisión cooperarán para facilitar una aplicación convergente de la Directiva en toda la UE. Además, las intervenciones concertadas en defensa de la SRI pueden contribuir de forma muy positiva a la protección efectiva de los derechos fundamentales, y en especial del derecho a la protección de los datos de carácter personal y a la intimidad. Una actuación a escala de la UE aumentaría por tanto la eficacia de las políticas nacionales vigentes y facilitaría su desarrollo.

Las medidas propuestas también quedan justificadas por el principio de proporcionalidad. Las obligaciones que han de cumplir los Estados miembros se fijan en el nivel mínimo necesario para lograr una preparación adecuada y posibilitar

[23] Reglamento (CE) n° 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información (DO L 77 de 13.3.2004, p. 1).

una cooperación basada en la confianza. Ello permite a los Estados miembros tomar debidamente en consideración las particularidades nacionales y garantiza la aplicación de los principios comunes de la UE de forma proporcionada. Gracias al amplio alcance de la Directiva, los Estados miembros podrán aplicarla en función de los riesgos reales que existan a escala nacional, expuestos en la estrategia nacional de SRI. La gestión de riesgos obligatoria solamente es aplicable a las entidades críticas e impone medidas proporcionales a los riesgos. En la consulta pública se destacaba la importancia de garantizar la seguridad de esas entidades críticas. Las obligaciones en materia de notificación únicamente se impondrían con respecto a los incidentes con efectos significativos. Como ya se ha señalado anteriormente, las medidas no ocasionarían gastos desproporcionados, ya que muchas de esas entidades que actúan como responsables del tratamiento ya están obligadas a asegurar la protección de los datos personales por la normativa de protección de datos vigente.

Para no imponer una carga desproporcionada a los pequeños operadores, y en especial a las pymes, los requisitos son proporcionales a los riesgos que presentan la red o el sistema de información de que se trate y no son aplicables a las microempresas. Las entidades sujetas a esas obligaciones deberán, en primer lugar, determinar los riesgos existentes y, a continuación, decidir las medidas que deban adoptarse para atenuarlos.

Los objetivos señalados pueden alcanzarse mejor a escala de la UE que de los Estados miembros, habida cuenta de los aspectos transfronterizos de los riesgos e incidentes de SRI. Por tanto, la UE puede adoptar medidas con arreglo al principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad, la Directiva propuesta no excede de lo necesario para alcanzar esos objetivos.

Para alcanzar los objetivos, la Comisión debe ser autorizada a adoptar actos delegados, de conformidad con el artículo 290 del Tratado de Funcionamiento de la Unión Europea, al objeto de completar o modificar determinados elementos no esenciales del acto de base. Con la propuesta de la Comisión también se pretende respaldar un proceso de proporcionalidad en la aplicación de las obligaciones impuestas a los operadores públicos y privados.

A fin de garantizar condiciones uniformes de aplicación del acto de base, deben conferirse a la Comisión competencias para adoptar actos de ejecución con arreglo al artículo 291 del Tratado de Funcionamiento de la Unión Europea.

Teniendo presentes, en particular, el amplio alcance de la Directiva propuesta, el hecho de que afecta a ámbitos fuertemente regulados y las obligaciones jurídicas que se derivan de su capítulo IV, se considera necesario que se adjunten documentos explicativos a la notificación de las medidas de transposición. De conformidad con la Declaración política conjunta de los Estados miembros y de la Comisión sobre los documentos explicativos de 28 de septiembre de 2011, los Estados miembros se han comprometido a adjuntar a la notificación de sus medidas de transposición, cuando esté justificado, uno o varios documentos que expliquen la relación entre los elementos de una directiva y las partes correspondientes de los instrumentos nacionales de transposición. Por lo que respecta a la presente Directiva, el legislador considera que la transmisión de tales documentos está justificada.

4. REPERCUSIONES PRESUPUESTARIAS

La cooperación y el intercambio de información entre los Estados miembros precisan infraestructuras seguras. La propuesta solamente tendrá repercusiones en el presupuesto de la UE si los Estados miembros optan por adaptar las infraestructuras existentes (por ejemplo,s-TESTA) y encomiendan las labores de ejecución a la Comisión dentro del MFP para el período 2014-2020. Se calcula que el coste único ascenderá a 1 250 000 EUR y se imputará al presupuesto de la UE, en la línea presupuestaria 09.03.02 (promover la interconexión y la interoperabilidad de los servicios públicos nacionales en línea, así como el acceso a estas redes — Capítulo 09.03, Mecanismo «Conectar Europa» — redes de telecomunicaciones), siempre que existan fondos disponibles en dicho Mecanismo. Los Estados miembros pueden compartir el coste único de adaptar las infraestructuras existentes o decidir crear nuevas infraestructuras y correr con los gastos de las mismas, que se estiman en unos 10 millones EUR anuales.

2013/0027 (COD)

Propuesta de

DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, su artículo 114,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de acto legislativo a los parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo[24],

Previa consulta al Supervisor Europeo de Protección de Datos,

De conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

(1) Las redes y los sistemas y servicios de información desempeñan un papel crucial en la sociedad. Su fiabilidad y seguridad son esenciales para la actividad económica y el bienestar social y, en particular, para el funcionamiento del mercado interior.

(2) La magnitud y la frecuencia de los incidentes de seguridad, ya sean deliberados o accidentales, se están incrementando y representan una grave amenaza para el funcionamiento de las redes y los sistemas de información. Tales incidentes pueden interrumpir las actividades económicas, generar considerables pérdidas financieras, minar la confianza del usuario y causar grandes daños a la economía de la Unión.

(3) Al ser instrumentos de comunicación sin fronteras, los sistemas de información digitales —y sobre todo Internet— contribuyen decisivamente a facilitar la circulación transfronteriza de bienes, servicios y personas. Dado su carácter transnacional, una perturbación grave de esos sistemas en un Estado miembro puede afectar también a otros Estados miembros y a la Unión en su conjunto. Por consiguiente, la resiliencia y la estabilidad de las redes y los sistemas de información son fundamentales para el correcto funcionamiento del mercado interior.

(4) Es conveniente crear a escala de la Unión un mecanismo de cooperación que propicie el intercambio de información y una detección y respuesta coordinadas en relación con la seguridad de las redes y de la información (en lo sucesivo, «SRI»). Para que dicho mecanismo sea eficaz e integrador, es esencial que todos los Estados miembros posean unas capacidades mínimas y una estrategia que aseguren un elevado nivel de SRI en su territorio. Asimismo, procede imponer a las administraciones públicas y a los operadores de infraestructuras críticas de información requisitos mínimos en materia de seguridad para fomentar una cultura de gestión de riesgos y garantizar la notificación de los incidentes más graves.

(5) Para abarcar todos los incidentes y riesgos pertinentes, la presente Directiva debe aplicarse a todas las redes y a todos los sistemas de información. No obstante, las obligaciones impuestas a las administraciones públicas y a los operadores del mercado no deberían ser aplicables a las empresas que suministran redes públicas de comunicaciones o prestan servicios de comunicaciones electrónicas disponibles para el público con arreglo a la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva Marco)[25], que están sujetas a los requisitos específicos de seguridad e integridad establecidos en el artículo 13 *bis* de dicha Directiva, ni tampoco a los proveedores de servicios de confianza.

(6) Las capacidades existentes no bastan para garantizar un elevado nivel de SRI en la Unión. Los niveles de preparación de los Estados miembros son muy distintos, lo que da lugar a enfoques fragmentarios en la Unión. Esta situación engendra desiguales niveles de protección de los consumidores y las empresas, comprometiendo el nivel general de SRI de la Unión. A su vez, la inexistencia de requisitos mínimos

[24] DO C […] de […], p. […].
[25] DO L 108 de 24.4.2002, p. 33.

comunes para las administraciones públicas y los operadores del mercado imposibilita la creación de un mecanismo global y efectivo de cooperación en la Unión.

(7) Para responder con eficacia a los problemas de seguridad de las redes y los sistemas de información es, pues, necesario un planteamiento global a escala de la Unión que integre requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, actividades de intercambio de información y coordinación de medidas, así como requisitos mínimos comunes de seguridad para todos los operadores del mercado interesados y las administraciones públicas.

(8) Las disposiciones de la presente Directiva no han de obstar para que los Estados miembros adopten las medidas necesarias para asegurar la protección de sus intereses esenciales en materia de seguridad, salvaguardar el orden público y la seguridad pública, y permitir la investigación, detección y represión de delitos. De conformidad con el artículo 346 del TFUE, ningún Estado miembro debe estar obligado a facilitar información cuya divulgación considere contraria a los intereses esenciales de su seguridad.

(9) A fin de alcanzar y mantener un elevado nivel común de seguridad de las redes y los sistemas de información, los Estados miembros deben disponer de sendas estrategias nacionales de SRI que fijen los objetivos estratégicos y las medidas concretas que haya que aplicar. Deben elaborarse a escala nacional planes de cooperación en el ámbito de la SRI que cumplan los requisitos esenciales para así lograr niveles de capacidad de respuesta que hagan posible una cooperación efectiva y eficaz a escala nacional y de la Unión ante los incidentes que se produzcan.

(10) Con miras a una aplicación efectiva de las disposiciones adoptadas de conformidad con la presente Directiva, procede crear o designar en cada uno de los Estados miembros un organismo que coordine las cuestiones relacionadas con la SRI y actúe como centro de referencia nacional a efectos de cooperación transfronteriza a escala de la Unión. Estos organismos deben disponer de recursos técnicos, financieros y humanos suficientes para poder desempeñar efectiva y eficazmente las tareas que se les encomienden y alcanzar de este modo los objetivos de la presente Directiva.

(11) Todos los Estados miembros deben disponer de capacidades técnicas y de organización suficientes para poder adoptar las medidas de prevención, detección, respuesta y atenuación oportunas ante los incidentes y riesgos que puedan afectar a las redes y los sistemas de información. Por consiguiente, procede crear en todos los Estados miembros equipos de respuesta a emergencias informáticas que funcionen correctamente y cumplan los requisitos esenciales para así disponer de capacidades efectivas y compatibles que permitan hacer frente a incidentes y riesgos y garantizar una cooperación eficaz a escala de la Unión.

(12) Sobre la base de los significativos avances logrados en el marco del Foro Europeo de Estados Miembros («EFMS») merced a los debates e intercambios sobre mejores prácticas, incluida la elaboración de principios de cooperación europea ante crisis cibernéticas, los Estados miembros y la Comisión deberían crear una red que los mantuviera en comunicación permanente y respaldara su cooperación. Se espera que este mecanismo seguro y efectivo de comunicación permita estructurar y coordinar a escala de la Unión las labores de intercambio de información, detección y respuesta.

(13) Es conveniente que la Agencia Europea de Seguridad de las Redes y de la Información («ENISA») preste asistencia a los Estados miembros y a la Comisión ofreciéndoles su experiencia, conocimientos y asesoramiento y facilitando el intercambio de mejores prácticas. En particular, la Comisión debe consultar a la ENISA a la hora de aplicar la presente Directiva. A fin de facilitar información eficaz y oportuna a los Estados miembros y la Comisión, deben lanzarse alertas tempranas sobre incidentes y riesgos en el marco de la red de cooperación. Al objeto de desarrollar capacidades y conocimientos entre los Estados miembros, la red de cooperación debe servir también de instrumento para el intercambio de mejores prácticas, ayudando a sus miembros a desarrollar capacidades y dirigiendo la organización de revisiones por homólogos y ejercicios de SRI.

(14) Es oportuno crear infraestructuras seguras para el intercambio de información delicada y confidencial en el marco de la red de cooperación. Sin perjuicio de la obligación de notificar a la red de cooperación los incidentes y riesgos que afecten a toda la Unión, el acceso a la información confidencial de otros Estados miembros solo debe permitirse a los Estados miembros que demuestren que sus recursos técnicos, financieros y humanos y sus procedimientos, así como sus infraestructuras de comunicación, garantizan su participación efectiva, eficiente y segura en la red.

(15) La cooperación entre los sectores público y privado reviste importancia esencial por cuanto la mayor parte de las redes y sistemas de información es de titularidad privada. Conviene alentar a los operadores del mercado a crear sus propios mecanismos de cooperación informal para garantizar la SRI. Asimismo, los operadores deben cooperar con el sector público e intercambiar información y mejores prácticas a cambio de obtener apoyo operativo en caso de que se produzcan incidentes.

(16) Para garantizar la transparencia e informar debidamente a los ciudadanos y operadores del mercado de la UE, conviene que las autoridades competentes creen un sitio web común para publicar información no confidencial sobre incidentes y riesgos.

(17) Cuando la información se considere confidencial de conformidad con las normas nacionales y de la Unión en materia de secreto comercial, debe mantenerse ese carácter confidencial a la hora de desarrollar las actividades y cumplir los objetivos establecidos en la presente Directiva.

(18) Basándose ante todo en las experiencias nacionales en materia de gestión de crisis y en cooperación con la ENISA, la Comisión y los Estados miembros deben elaborar un plan de cooperación de la Unión en materia de SRI que establezca mecanismos de cooperación para hacer frente a riesgos e incidentes. Dicho plan debe tomarse debidamente en consideración a la hora de lanzar alertas tempranas en el marco de la red de cooperación.

(19) Las alertas tempranas solamente deben notificarse en el marco de la red cuando la dimensión y gravedad del incidente o riesgo en cuestión sean o puedan llegar a ser de tal envergadura que requieran medidas de información o coordinación de la respuesta a escala de la Unión. Por tanto, las alertas tempranas se deberían limitar a los incidentes o riesgos reales o potenciales que se extiendan rápidamente, superen la capacidad nacional de respuesta o afecten a más de un Estado miembro. Para poder proceder a un análisis adecuado, debe comunicarse a la red de cooperación toda la información pertinente para la evaluación del riesgo o incidente.

(20) Tras haber recibido y evaluado una alerta temprana, las autoridades competentes deben acordar una respuesta coordinada en el marco del plan de cooperación de la Unión en materia de SRI. Tanto las autoridades competentes como la Comisión deben estar informadas de las medidas adoptadas a escala nacional como resultado de la respuesta coordinada.

(21) El alcance mundial de los problemas de SRI hace necesaria una mayor cooperación internacional con miras a mejorar las normas de seguridad y el intercambio de información, y promover un planteamiento mundial común con respecto a las cuestiones de SRI.

(22) La responsabilidad de velar por la SRI recae en gran medida en las administraciones públicas y los operadores del mercado. Debe fomentarse una cultura de gestión de riesgos que entrañe una evaluación del riesgo y la aplicación de medidas de seguridad proporcionales a los riesgos existentes y que habrá de desarrollarse a través de requisitos reglamentarios adecuados y prácticas voluntarias del sector. Asimismo, son necesarias condiciones uniformes para garantizar el funcionamiento efectivo de la red de cooperación y, por ende, una colaboración eficaz de todos los Estados miembros.

(23) La Directiva 2002/21/CE establece que las empresas que suministran redes públicas de comunicaciones o prestan servicios de comunicaciones electrónicas disponibles para el público deben adoptar medidas adecuadas para salvaguardar su integridad y seguridad e introduce requisitos de notificación de las violaciones de la seguridad y las pérdidas de integridad. La Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)[26] exige que los proveedores de servicios de comunicaciones electrónicas accesibles para el público tomen las medidas técnicas y de organización necesarias para velar por la seguridad de sus servicios.

(24) Estas obligaciones no solo han de imponerse al sector de las comunicaciones electrónicas, sino también a los principales proveedores de servicios de la sociedad de la información, tal y como se definen en la Directiva 98/34/CE del Parlamento Europeo y del Consejo, de 22 de junio de 1998, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas y de las reglas relativas a los servicios de la sociedad de la información[27], que sirven de apoyo a los servicios de la sociedad de la información derivados o a las actividades en línea, tales como las plataformas de comercio electrónico, las pasarelas de pago por Internet, las redes sociales, los motores de búsqueda, los servicios de computación en nube o las tiendas de aplicaciones. La interrupción de estos servicios de apoyo a la sociedad de la información impide la prestación de otros servicios de la sociedad de la información que dependen de ellos. Los desarrolladores de programas informáticos y los fabricantes de equipos físicos no son proveedores de servicios de la sociedad de la información y quedan, por tanto, excluidos. Procede imponer asimismo esas obligaciones a las administraciones públicas y a los operadores de infraestructuras críticas, que son muy dependientes de las tecnologías de la información y la comunicación y desempeñan un papel esencial en el mantenimiento de funciones económicas o sociales vitales, tales como el gas y la electricidad, los transportes, las entidades de crédito, las bolsas y la sanidad. Los trastornos que puedan sufrir tales redes y sistemas de información afectan al mercado interior.

---

[26] DO L 201 de 31.7.2002, p. 37.
[27] DO L 204 de 21.7.1998, p. 37.

(25) Las medidas técnicas y de organización impuestas a las administraciones públicas y a los operadores del mercado no requerirán que se diseñe, se desarrolle o fabrique de una manera especial un determinado producto comercial de tecnología de la información y la comunicación.

(26) Las administraciones públicas y los operadores del mercado deben velar por la seguridad de las redes y sistemas que se hallan bajo su control. Se trata fundamentalmente de redes y sistemas privados gestionados por el personal de TI interno o cuya seguridad se ha encomendado a empresas externas. Las obligaciones en materia de seguridad y notificación han de aplicarse a los operadores del mercado y a las administraciones públicas pertinentes, independientemente de si se encargan ellos mismos del mantenimiento de sus redes y sistemas de información o lo subcontratan.

(27) Para no imponer una carga financiera y administrativa desproporcionada a los pequeños operadores y a los usuarios, los requisitos han de ser proporcionales a los riesgos que presenta la red o el sistema de información en cuestión, habida cuenta del estado de la técnica. Dichos requisitos no deben aplicarse a las microempresas.

(28) Las autoridades competentes deben procurar que se mantengan los canales de intercambio de información informales y de confianza entre los operadores del mercado y entre los sectores público y privado. Antes de dar publicidad a los incidentes notificados a las autoridades competentes, es preciso sopesar debidamente el interés de los ciudadanos en ser informados sobre las amenazas existentes y los perjuicios que en términos comerciales y de reputación puedan sufrir las administraciones públicas y los operadores del mercado que notifican los incidentes. A la hora de cumplir sus obligaciones de notificación, las autoridades competentes han de tener muy en cuenta la necesidad de mantener estrictamente confidencial la información sobre los puntos vulnerables del producto antes de dar a conocer las soluciones de seguridad adecuadas.

(29) Es preciso que las autoridades competentes dispongan de los medios necesarios para desempeñar su cometido y, en particular, de competencias para obtener información suficiente de los operadores del mercado y las administraciones públicas a fin de evaluar el nivel de seguridad de las redes y los sistemas de información, así como datos fidedignos y exhaustivos sobre incidentes reales que hayan repercutido en el funcionamiento de las redes y los sistemas de información.

(30) Los incidentes suelen estar causados por actividades delictivas. Cabe suponer el carácter delictivo de los incidentes aun cuando las pruebas para demostrarlo no sean lo suficientemente claras desde el principio. A este respecto, una cooperación adecuada entre las autoridades competentes y los cuerpos de seguridad debería formar parte de una respuesta efectiva y global ante la amenaza de que se produzcan incidentes de seguridad. En particular, para promover un entorno protegido, seguro y más resiliente es preciso notificar sistemáticamente los incidentes de carácter supuestamente delictivo a los cuerpos de seguridad. La naturaleza delictiva grave de los incidentes debe evaluarse a la luz de la normativa de la UE sobre ciberdelincuencia.

(31) En numerosas ocasiones los datos de carácter personal se ven comprometidos a raíz de incidentes. En este contexto, las autoridades competentes y las autoridades responsables de la protección de datos han de cooperar e intercambiar la información pertinente ante las violaciones de datos personales derivadas de incidentes. Los Estados miembros deben imponer la obligación de notificar los incidentes de seguridad de modo que se reduzca al mínimo la carga administrativa en caso de que el incidente de seguridad constituya también una violación de datos personales con arreglo al Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[28]. En colaboración con las autoridades competentes y las autoridades responsables de la protección de datos, la ENISA podría contribuir a elaborar mecanismos de intercambio de información y modelos que evitaran la necesidad de contar con dos modelos de notificación. Este modelo único de notificación facilitaría la comunicación de incidentes que comprometan los datos personales, aliviando de este modo la carga administrativa para empresas y administraciones públicas.

(32) La normalización de los requisitos en materia de seguridad es un proceso impulsado por el mercado. Al objeto de garantizar una aplicación convergente de las normas de seguridad, es oportuno que los Estados miembros fomenten el cumplimiento de normas específicas o la conformidad con ellas para así lograr un elevado nivel de seguridad en la Unión. A tal fin, puede ser necesario elaborar normas armonizadas, de acuerdo con las disposiciones del Reglamento (UE) nº 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión nº 1673/2006/CE del Parlamento Europeo y del Consejo[29].

(33) La Comisión debe revisar periódicamente las disposiciones contenidas en la presente Directiva, en particular con vistas a determinar si es preciso modificarlas a la luz de la cambiante situación de la tecnología o el mercado.

---

[28] SEC(2012) 72 final.

[29] DO L 316 de 14.11.2012, p. 12.

(34) En aras del correcto funcionamiento de la red de cooperación, procede delegar en la Comisión poderes para adoptar actos de conformidad con el artículo 290 del Tratado de Funcionamiento de Unión Europea en relación con la determinación de los criterios que debe reunir un Estado miembro para poder ser autorizado a participar en el sistema de intercambio seguro de información, con la especificación de los hechos que activan la alterta temprana y con la definición de las circunstancias en que los operadores del mercado y las administraciones públicas están obligados a notificar incidentes.

(35) Reviste primordial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos. Al preparar y elaborar actos delegados, la Comisión debe garantizar que los documentos pertinentes se transmitan al Parlamento Europeo y al Consejo de manera simultánea, oportuna y adecuada.

(36) A fin de garantizar condiciones uniformes de ejecución de la presente Directiva, procede conferir competencias de ejecución a la Comisión en lo que respecta a la cooperación entre las autoridades competentes y la Comisión en el marco de la red de cooperación, el acceso a las infraestructuras seguras de intercambio de información, el plan de cooperación de la Unión en materia de SRI, los formatos y procedimientos aplicables a la hora de informar a los ciudadanos sobre incidentes y las normas o especificaciones técnicas en materia de SRI. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) nº 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión[30].

(37) Es conveniente que, a la hora de aplicar la presente Directiva, la Comisión colabore, cuando proceda, con los comités sectoriales y organismos pertinentes establecidos a escala de la UE, especialmente en los ámbitos de la energía, los transportes y la sanidad.

(38) La información que una autoridad competente considere confidencial de acuerdo con las normas nacionales y de la Unión sobre secreto comercial únicamente debe intercambiarse con la Comisión y otras autoridades competentes cuando tal intercambio sea estrictamente necesario a los efectos de la aplicación de la presente Directiva. El intercambio se debe limitar a la información que resulte pertinente y proporcional a la finalidad perseguida.

(39) El intercambio de información sobre riesgos e incidentes en el marco de la red de cooperación y el cumplimiento de la obligación de notificar los incidentes a las autoridades nacionales competentes pueden hacer necesario el tratamiento de datos personales. Dicho tratamiento es necesario para alcanzar los objetivos de interés público perseguidos por la presente Directiva y es por tanto legítimo en virtud del artículo 7 de la Directiva 95/46/CE. No constituye, en relación con esos objetivos legítimos, una intervención desmesurada e intolerable que afecte a la propia esencia del derecho a la protección de los datos personales garantizado por el artículo 8 de la Carta de los Derechos Fundamentales. Al llevar a la práctica la presente Directiva, se debe aplicar, cuando proceda, el Reglamento (CE) nº 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión[31]. Cuando las instituciones y órganos de la Unión procedan al tratamiento de datos a los efectos de la aplicación de la presente Directiva, dicho tratamiento deberá efectuarse de conformidad con los dispuesto en el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

(40) Dado que el objetivo de la presente Directiva, a saber, garantizar un elevado nivel de SRI en la Unión, no puede ser alcanzado de manera suficiente por los Estados miembros de manera individual y, por consiguiente, debido a los efectos de la acción, puede lograrse mejor a nivel de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad enunciado en dicho artículo, la presente Directiva no excede de lo necesario para alcanzar estos objetivos.

(41) La presente Directiva observa los derechos fundamentales y los principios reconocidos por la Carta de los Derechos Fundamentales de la Unión Europea y, en particular, el derecho al respeto de la vida privada y las comunicaciones, el derecho a la protección de los datos de carácter personal, el derecho a la libertad de empresa, el derecho a la propiedad, el derecho a una tutela judicial efectiva y el derecho a ser oído. La presente Directiva debe aplicarse de acuerdo con estos derechos y principios.

30 DO L 55 de 28.2.2011, p. 13.
31 DO L 145 de 31.5.2001, p. 43.

HAN ADOPTADO LA PRESENTE DIRECTIVA:

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1

Objeto y ámbito de aplicación

1. La presente Directiva establece medidas para garantizar un elevado nivel común de seguridad de las redes y de la información (denominada en lo sucesivo «SRI») en la Unión.

2. A tal fin, la presente Directiva:

a) establece las obligaciones que han de cumplir todos los Estados miembros en materia de prevención, gestión y respuesta a riesgos e incidentes que afecten a las redes y los sistemas de información;

b) establece un mecanismo de cooperación entre los Estados miembros con el fin de garantizar la aplicación uniforme de la presente Directiva en la Unión y, en su caso, una gestión y una respuesta eficaces y coordinadas ante los riesgos e incidentes que afecten a las redes y los sistemas de información;

c) establece requisitos en materia de seguridad para los operadores del mercado y las administraciones públicas.

3. Los requisitos de seguridad previstos en el artículo 14 no serán aplicables a las empresas que suministran redes públicas de comunicaciones o prestan servicios de comunicaciones electrónicas disponibles para el público con arreglo a la Directiva 2002/21/CE, que están sujetas a los requisitos específicos de seguridad e integridad establecidos en los artículos 13 *bis* y 13 *ter* de dicha Directiva, ni tampoco a los proveedores de servicios de confianza.

4. La presente Directiva se entenderá sin perjuicio de la normativa sobre ciberdelincuencia de la UE y de la Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección[32].

5. Asimismo, la presente Directiva se entenderá sin perjuicio de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[33], de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, y del Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[34].

6. El intercambio de información en el marco de la red de cooperación a que se hace referencia en el capítulo III y las notificaciones de incidentes de SRI contempladas en el artículo 14 pueden requerir el tratamiento de datos personales. Dicho tratamiento, que es necesario para alcanzar los objetivos de interés público perseguidos por la presente Directiva, será autorizado por el Estado miembro interesado de acuerdo con el artículo 7 de la Directiva 95/46/CE y con la Directiva 2002/58/CE según su adopción en el Derecho interno.

Artículo 2

Armonización mínima

No se impedirá que los Estados miembros adopten o mantengan disposiciones que garanticen un nivel de seguridad más elevado, sin perjuicio de las obligaciones que les impone la normativa de la Unión.

32 DO L 345 de 23.12.2008, p. 75.
33 DO L 281 de 23.11.1995, p. 31.
34 SEC(2012) 72 final.

Artículo 3

Definiciones

A los efectos de la presente Directiva, se entenderá por:

1) «redes y sistemas de información»:

   a) una red de comunicaciones electrónicas en la acepción de la Directiva 2002/21/CE,

   b) todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos,

   c) los datos informáticos almacenados, tratados, recuperados o transmitidos por los elementos contemplados en las letras a) y b) para su funcionamiento, utilización, protección y mantenimiento;

2) «seguridad»: la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de confianza, a acciones accidentales o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos;

3) «riesgo»: toda circunstancia o hecho que pueda tener efectos adversos en la seguridad;

4) «incidente»: toda circunstancia o hecho que tenga efectos adversos en la seguridad;

5) «servicio de la sociedad de la información»: un servicio en la acepción del artículo 1, número 2, de la Directiva 98/34/CE;

6) «plan de cooperación en materia de SRI»: un plan que constituye el marco para las funciones, responsabilidades y procedimientos de organización a fin de mantener o restablecer el funcionamiento de las redes y los sistemas de información en caso de que se vean afectados por un riesgo o incidente;

7) «gestión de incidentes»: todos los procedimientos seguidos para analizar, limitar y responder a un incidente;

8) «operador del mercado»:

   a) un proveedor de servicios de la sociedad de la información que posibilitan la prestación de otros servicios de la sociedad de la información, una lista no exhaustiva de los cuales figura en el anexo II;

   b) un operador de infraestructuras críticas esenciales para el mantenimiento de actividades económicas y sociales vitales en los sectores de la energía, los transportes, la banca, la bolsa y la sanidad, una lista no exhaustiva de los cuales figura en el anexo II.

9) «norma»: una norma en la acepción del Reglamento (UE) nº 1025/2012;

10) «especificación»: una especificación en la acepción del Reglamento (UE) nº 1025/2012;

11) «proveedor de servicios de confianza»: una persona física o jurídica que presta un servicio electrónico consistente en la creación, verificación, validación, gestión y conservación de firmas electrónicas, sellos electrónicos, marcas de tiempo electrónicas, documentos electrónicos, servicios de entrega electrónica, autenticación de sitios web y certificados electrónicos, incluidos los certificados de firma electrónica y de sello electrónico.

CAPÍTULO II

MARCOS NACIONALES DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN

Artículo 4

Principio

Los Estados miembros garantizarán un elevado nivel común de seguridad de las redes y los sistemas de información en sus territorios de conformidad con lo dispuesto en la presente Directiva.

Artículo 5

Estrategia nacional de SRI y plan de cooperación nacional en materia de SRI

1. Cada Estado miembro adoptará una estrategia nacional de SRI que establezca los objetivos estratégicos y las medidas estratégicas y reglamentarias concretas para alcanzar y mantener un elevado nivel de seguridad de las redes y de la información. La estrategia nacional de SRI abordará, en particular, las cuestiones siguientes:

a) Determinación de los objetivos y prioridades de la estrategia sobre la base de un análisis actualizado de riesgos e incidentes.

b) Marco de gobernanza para lograr los objetivos y las prioridades de la estrategia, con una definición clara de las funciones y responsabilidades de las instituciones públicas y los demás agentes pertinentes.

c) Determinación de las medidas generales sobre preparación, respuesta y recuperación, incluidos los mecanismos de cooperación entre los sectores público y privado.

d) Indicación de los programas de educación, concienciación y formación.

e) Planes de investigación y desarrollo y explicación de la manera en que reflejan las prioridades establecidas.

2. La estrategia nacional de SRI incluirá un plan de cooperación nacional en materia de SRI que contemple como mínimo los siguientes aspectos:

a) Plan de evaluación de riesgos que permita determinarlos y evaluar los efectos de incidentes potenciales.

b) Determinación de las funciones y responsabilidades de los diversos agentes que participan en la ejecución del plan.

c) Determinación de los procedimientos de cooperación y comunicación necesarios para garantizar la prevención, detección, respuesta, reparación y recuperación, adaptados en función del nivel de alerta.

d) Hoja de ruta sobre ejercicios y actividades de formación en el ámbito de la SRI para reforzar, validar y someter a ensayo el plan. La experiencia adquirida se deberá documentar e incorporar a las actualizaciones del plan.

3. La estrategia nacional de SRI y el plan de cooperación nacional en materia de SRI se deberán remitir a la Comisión en el plazo de un mes a partir de su adopción.

Artículo 6

Autoridad nacional competente en materia de seguridad de las redes y los sistemas de información

1. Cada Estado miembro designará una autoridad nacional competente en materia de seguridad de las redes y los sistemas de información («la autoridad competente»).

2. Las autoridades competentes supervisarán la aplicación de la presente Directiva a escala nacional y contribuirán a una aplicación coherente de la misma en toda la Unión.

3. Los Estados miembros velarán por que las autoridades competentes dispongan de suficientes recursos técnicos, financieros y humanos para llevar a cabo las tareas a ellas asignadas de forma eficiente y eficaz y cumplir así los objetivos de la presente Directiva. Los Estados miembros garantizarán una cooperación eficiente, eficaz y segura entre las autoridades competentes a través de la red a que se hace referencia en el artículo 8.

4. Los Estados miembros velarán por que las autoridades competentes reciban las notificaciones de incidentes de las administraciones públicas y los operadores del mercado con arreglo al artículo 14, apartado 2, y se les confieran las competencias de aplicación a que se refiere el artículo 15.

5. Las autoridades competentes llevarán a cabo consultas y cooperarán, cuando proceda, con las fuerzas de seguridad nacionales y las autoridades responsables de la protección de datos.

6. Los Estados miembros notificarán sin demora a la Comisión la autoridad competente que hayan designado, su cometido y cualquier cambio posterior que se introduzca en él. Los Estados miembros harán pública la designación de la autoridad competente.

Artículo 7

Equipo de respuesta a emergencias informáticas

1. Cada Estado miembro creará un equipo de respuesta a emergencias informáticas (en lo sucesivo, «CERT») responsable de la gestión de incidentes y riesgos de acuerdo con un procedimiento claramente definido, que se ajustará a los requisitos establecidos en el anexo I, punto 1. Podrá crearse un CERT en el marco de la autoridad competente.

2. Los Estados miembros velarán por que los CERT cuenten con suficientes recursos técnicos, financieros y humanos para llevar a cabo efectivamente las tareas que les correspondan, establecidas en el anexo I, punto 2.

3. Los Estados miembros velarán por que los CERT dispongan a escala nacional de infraestructuras de comunicación e información seguras y resilientes, que serán compatibles e interoperables con el sistema seguro de intercambio de información a que se hace referencia en el artículo 9.

4. Los Estados miembros informarán a la Comisión de los recursos, el mandato y el procedimiento de gestión de incidentes de los CERT.

5. Los CERT actuarán bajo la supervisión de la autoridad competente, que comprobará periódicamente la adecuación de sus recursos, su mandato y la eficacia de su procedimiento de gestión de incidentes.

CAPÍTULO III

COOPERACIÓN ENTRE LAS AUTORIDADES COMPETENTES

Artículo 8

Red de cooperación

1. Las autoridades competentes y la Comisión crearán una red («red de cooperación») para colaborar contra los riesgos e incidentes que afecten a las redes y los sistemas de información.

2. La Comisión y las autoridades competentes mantendrán una comunicación constante en el marco de la red de cooperación. Cuando así se le solicite, la Agencia Europea de Seguridad de las Redes y de la Información («ENISA») asistirá a la red de cooperación ofreciéndole su experiencia, conocimientos y asesoramiento.

3. En el marco de la red de cooperación, las autoridades competentes:

   a) difundirán alertas tempranas sobre riesgos e incidentes de conformidad con el artículo 10;

   b) ofrecerán una respuesta coordinada de conformidad con el artículo 11;

   c) publicarán periódicamente en un sitio web común información no confidencial sobre las alertas tempranas y las respuestas coordinadas en curso;

   d) examinarán y evaluarán conjuntamente, a petición de un Estado miembro o de la Comisión, uno o varios planes de cooperación nacionales en materia de SRI y estrategias nacionales de SRI, contemplados en el artículo 5, en el marco de la presente Directiva;

   e) examinarán y evaluarán conjuntamente, a petición de un Estado miembro o de la Comisión, la eficacia de los CERT, especialmente cuando los ejercicios de SRI se realicen a escala de la Unión;

   f) cooperarán e intercambiarán información sobre todas las cuestiones pertinentes con el Centro Europeo de Ciberdelincuencia de Europol y con otros organismos europeos pertinentes, en particular en los sectores de la protección de datos, la energía, los transportes, la banca, la bolsa y la sanidad;

   g) intercambiarán información y mejores prácticas entre sí y con la Comisión, y se ayudarán mutuamente con el fin de crear capacidades en materia de SRI;

   h) organizarán revisiones por homólogos periódicas sobre capacidades y preparación;

   i) organizarán ejercicios de SRI a escala de la Unión y participarán, en su caso, en ejercicios de SRI internacionales.

4. La Comisión establecerá mediante actos de ejecución las disposiciones necesarias para facilitar la cooperación entre las autoridades competentes y la Comisión a que se hace referencia en los apartados 2 y

3. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de consulta contemplado en el artículo 19, apartado 2.

Artículo 9

Sistema seguro de intercambio de información

1. El intercambio de información delicada y confidencial dentro de la red de cooperación se efectuará a través de una infraestructura segura.

2. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 18 a fin de fijar los criterios que ha de reunir un Estado miembro para ser autorizado a participar en el sistema seguro de intercambio de información, en relación con:

   a) la disponibilidad a escala nacional de infraestructuras de comunicación e información seguras y resilientes que sean compatibles e interoperables con la infraestructura segura de la red de cooperación de conformidad con el artículo 7, apartado 3, y

   b) la existencia de recursos y procedimientos técnicos, financieros y humanos adecuados para su autoridad competente y el CERT, de modo que sea posible una participación eficiente, eficaz y segura en el sistema seguro de intercambio de información contemplado en el artículo 6, apartado 3, el artículo 7, apartado 2, y el artículo 7, apartado 3.

3. La Comisión adoptará mediante actos de ejecución decisiones sobre el acceso de los Estados miembros a esta infraestructura segura, con arreglo a los criterios mencionados en los apartados 2 y 3. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 19, apartado 3.

Artículo 10

Alertas tempranas

1. Las autoridades competentes o la Comisión difundirán alertas tempranas en el marco de la red de cooperación en relación con los riesgos e incidentes que cumplan como mínimo una de las condiciones siguientes:

   a) riesgos e incidentes cuya magnitud aumente o pueda aumentar rápidamente;

   b) riesgos e incidentes que sobrepasen o puedan sobrepasar la capacidad nacional de respuesta;

   c) riesgos e incidentes que afecten o puedan afectar a más de un Estado miembro.

2. Las autoridades competentes y la Comisión incluirán en sus alertas tempranas toda la información pertinente que obre en su poder y pueda ser de utilidad para evaluar el riesgo o incidente.

3. A petición de un Estado miembro o por iniciativa propia, la Comisión podrá solicitar a un Estado miembro que proporcione la información pertinente sobre un riesgo o incidente concreto.

4. Cuando se sospeche que el riesgo o incidente objeto de una alerta temprana es de carácter delictivo, las autoridades competentes o la Comisión informarán de ello al Centro Europeo de Ciberdelincuencia de Europol.

5. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 18 con el fin de especificar los riesgos e incidentes que pueden activar la alerta temprana mencionada en el apartado 1.

Artículo 11

Respuesta cordinada

1. Cuando reciban la alerta temprana a que se refiere el artículo 10, las autoridades competentes evaluarán la información pertinente y acordarán una respuesta coordinada de conformidad con el plan de cooperación de la Unión en materia de SRI contemplado en el artículo 12.

2. Las diversas medidas adoptadas a escala nacional a raíz de la respuesta coordinada se notificarán a la red de cooperación.

Artículo 12

Plan de cooperación de la Unión en materia de SRI

1. La Comisión estará facultada para adoptar mediante actos de ejecución un plan de cooperación de la Unión en materia de SRI. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 19, apartado 3.

2. El plan de cooperación de la Unión en materia de SRI establecerá:

a) a los efectos del artículo 10:

– el formato y los procedimientos de recopilación e intercambio de información compatible y comparable sobre riesgos e incidentes por parte de las autoridades competentes,

– los procedimientos y criterios de evaluación de riesgos e incidentes por parte de la red de cooperación;

b) los procedimientos que se han de seguir para ofrecer las respuestas coordinadas previstas en el artículo 11, entre ellos el reparto de funciones y responsabilidades y los procedimientos de cooperación;

c) una hoja de ruta sobre ejercicios y actividades de formación en el ámbito de la SRI para reforzar, validar y someter a ensayo el plan;

d) un programa de transferencia de conocimientos entre los Estados miembros en materia de desarrollo de capacidades y aprendizaje entre homólogos;

e) un programa de concienciación y formación entre los Estados miembros.

3. El plan de cooperación de la Unión en materia de SRI deberá adoptarse dentro del año siguiente a la entrada en vigor de la presente Directiva y se revisará periódicamente.

Artículo 13

Cooperación internacional

Sin perjuicio de la posibilidad de que la red de cooperación mantenga relaciones informales de colaboración a escala internacional, la Unión podrá concluir acuerdos internacionales con terceros países u organizaciones internacionales que hagan posible y organicen su participación en algunas actividades de la red de cooperación. En tales acuerdos se tendrá en cuenta la necesidad de deparar una protección adecuada a los datos personales que circulen en la red de cooperación.

CAPÍTULO IV

SEGURIDAD DE LAS REDES Y SISTEMAS DE INFORMACIÓN DE LAS ADMINISTRACIONES PÚBLICAS Y LOS OPERADORES DEL MERCADO

Artículo 14

Requisitos en materia de seguridad y notificación de incidentes

1. Los Estados miembros velarán por que las administraciones públicas y los operadores del mercado tomen las medidas técnicas y de organización apropiadas para gestionar los riesgos existentes para la seguridad de las redes y los sistemas de información que controlan y utilizan en sus operaciones. Habida cuenta del estado de la técnica, dichas medidas garantizarán un nivel de seguridad adecuado en relación con el riesgo existente. En particular, adoptarán medidas para prevenir y reducir al mínimo los efectos de los incidentes que afecten a sus redes y sistemas de información en los servicios básicos que prestan, garantizando de este modo la continuidad de los servicios que dependen de tales redes y sistemas de información.

2. Los Estados miembros velarán por que las administraciones públicas y los operadores del mercado notifiquen a la autoridad competente los incidentes que tengan efectos significativos en la seguridad de los servicios básicos que prestan.

3. Los requisitos establecidos en los apartados 1 y 2 serán aplicables a todos los operadores del mercado que prestan servicios en la Unión Europea.

4. Cuando estime que la divulgación de un incidente redunda en el interés público, la autoridad competente podrá informar de él a los ciudadanos o pedir a las administraciones públicas y los operadores del mercado

que lo hagan. Una vez al año, la autoridad competente presentará a la red de cooperación un informe resumido sobre las notificaciones recibidas y las medidas adoptadas de acuerdo con el presente apartado.

5. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 18 con el fin de determinar las circunstancias en que las administraciones públicas y los operadores del mercado estarán obligados a notificar incidentes.

6. A reserva de cualesquiera actos delegados adoptados en virtud del apartado 5, las autoridades competentes podrán adoptar directrices y, en caso necesario, impartir instrucciones sobre las circunstancias en que las administraciones públicas y los operadores del mercado estarán obligados a notificar incidentes.

7. La Comisión estará facultada para determinar mediante actos de ejecución los formatos y procedimientos aplicables a los efectos del apartado 2. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 19, apartado 3.

8. Los apartados 1 y 2 no serán aplicables a las microempresas, según la definición que recoge la Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas[35].

Artículo 15

Aplicación y observancia

1. Los Estados miembros velarán por que las autoridades competentes dispongan de todas las competencias necesarias para investigar los casos de incumplimiento por parte de las administraciones públicas o los operadores del mercado de las obligaciones que les impone el artículo 14 y los efectos que tengan en la seguridad de las redes y los sistemas de información.

2. Los Estados miembros velarán por que las autoridades competentes estén facultadas para exigir a los operadores del mercado y a las administraciones públicas:

   a) que proporcionen la información necesaria para evaluar la seguridad de sus redes y sistemas de información, incluida la documentación sobre las políticas de seguridad;

   b) que se sometan a una auditoría de seguridad practicada por un organismo independiente o una autoridad nacional cualificados y pongan los resultados en conocimiento de la autoridad competente.

3. Los Estados miembros velarán por que las autoridades competentes estén facultadas para impartir instrucciones vinculantes a los operadores del mercado y a las administraciones públicas.

4. Las autoridades competentes notificarán los incidentes de carácter grave y supuestamente delictivo a los cuerpos de seguridad.

5. Las autoridades competentes cooperarán estrechamente con las autoridades responsables de la protección de datos personales a la hora de hacer frente a incidentes que den lugar a violaciones de datos personales.

6. Los Estados miembros garantizarán que cualesquiera obligaciones impuestas a las administraciones públicas y a los operadores del mercado en virtud del presente capítulo puedan estar sujetas a control judicial.

Artículo 16

Normalización

1. A fin de garantizar una aplicación convergente de lo dispuesto en el artículo 14, apartado 1, los Estados miembros fomentarán la utilización de las normas y especificaciones pertinentes en materia de seguridad de las redes y la información.

2. La Comisión elaborará mediante actos de ejecución una lista de las normas mencionadas en el apartado 1. Dicha lista se publicará en el *Diario Oficial de la Unión Europea*.

[35] DO L 124 de 20.5.2003, p. 36.

CAPÍTULO V

DISPOSICIONES FINALES

Artículo 17

Sanciones

1. Los Estados miembros establecerán normas sobre las sanciones aplicables a las infracciones de las disposiciones nacionales adoptadas en virtud de la presente Directiva y tomarán todas las medidas necesarias para garantizar su aplicación. Las sanciones adoptadas deberán ser eficaces, proporcionadas y disuasorias. Los Estados miembros notificarán esas disposiciones a la Comisión a más tardar en la fecha de transposición de la presente Directiva, y le notificarán además sin demora cualquier modificación posterior que les afecte.

2. Los Estados miembros garantizarán que, en caso de que un incidente de seguridad afecte a datos personales, las sanciones previstas guarden coherencia con las sanciones establecidas en el Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[36].

Artículo 18

Ejercicio de la delegación

1. Se otorgan a la Comisión poderes para adoptar actos delegados de acuerdo con las condiciones establecidas en el presente artículo.

2. Se otorgan a la Comisión los poderes para adoptar los actos delegados a que se refieren el artículo 9, apartado 2, el artículo 10, apartado 5, y el artículo 14, apartado 5. La Comisión elaborará un informe sobre los poderes delegados a más tardar nueve meses antes de que finalice el período de cinco años. La delegación de poderes se prorrogará automáticamente por períodos de idéntica duración, excepto si el Parlamento Europeo o el Consejo se oponen a dicha prórroga a más tardar tres meses antes del final de cada período.

3. La delegación de poderes a que se refieren el artículo 9, apartado 2, el artículo 10, apartado 5, y el artículo 14, apartado 5, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. Surtirá efecto al día siguiente de la publicación de la decisión en el *Diario Oficial de la Unión Europea* o en una fecha posterior que se precisará en dicha decisión. No afectará a la validez de los actos delegados que ya estén en vigor.

4. En cuanto la Comisión adopte un acto delegado, lo notificará simultáneamente al Parlamento Europeo y al Consejo.

5. Los actos delegados adoptados en virtud del artículo 9, apartado 2, del artículo 10, apartado 5, y del artículo 14, apartado 5, entrarán en vigor únicamente si, en un plazo de dos meses desde su notificación al Parlamento Europeo y al Consejo, ni el Parlamento Europeo ni el Consejo formulan objeciones o si, antes del vencimiento de dicho plazo, tanto el uno como el otro informan a la Comisión de que no las formularán. Este plazo se prorrogará dos meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 19

Procedimiento de comité

1. La Comisión estará asistida por un comité (el Comité de Seguridad de las Redes y de la Información). Dicho comité será un comité en la acepción del Reglamento (UE) nº 182/2011.

2. En los casos en que se haga referencia al presente apartado, será de aplicación el artículo 4 del Reglamento (UE) nº 182/2011.

3. En los casos en que se haga referencia al presente apartado, será de aplicación el artículo 5 del Reglamento (UE) nº 182/2011.

[36] SEC(2012) 72 final.

Artículo 20

Revisión

La Comisión revisará periódicamente el funcionamiento de la presente Directiva e informará al Parlamento Europeo y al Consejo. El primer informe se presentará a más tardar tres años después de la fecha de transposición mencionada en el artículo 21. A tal fin, la Comisión podrá solicitar a los Estados miembros que faciliten información sin demoras injustificadas.

Artículo 21

Transposición

1. Los Estados miembros adoptarán y publicarán, a más tardar [un año y medio después de la fecha de adopción], las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva. Comunicarán inmediatamente a la Comisión el texto de dichas disposiciones.

   Aplicarán esas medidas a partir del [un año y medio después de la fecha de adopción].

   Cuando los Estados miembros adopten dichas disposiciones, estas harán referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia.

2. Los Estados miembros comunicarán a la Comisión el texto de las disposiciones básicas de Derecho interno que adopten en el ámbito regulado por la presente Directiva.

Artículo 22

Entrada en vigor

La presente Directiva entrará en vigor el [vigésimo] día siguiente al de su publicación en el *Diario Oficial de la Unión Europea.*

Artículo 23

Destinatarios

Los destinatarios de la presente Directiva serán los Estados miembros.

Hecho en Bruselas, el

Por el Parlamento Europeo
El Presidente

Por el Consejo
El Presidente

N. de la R.: La documentació que acompanya aquesta proposta pot ésser consultada a l'Arxiu del Parlament.

Tramesa a la Comissió

Comissió competent: Comissió d'Interior.
Acord: Presidència del Parlament, 13.02.2013.

Termini de formulació d'observacions

Termini: 4 dies hàbils (del 19.02.2013 al 22.02.2013).
Finiment del termini: 25.02.2013; 09:30 h.
Acord: Presidència del Parlament, 13.02.2013.