

ES

ES

ES



COMISIÓN DE LAS COMUNIDADES EUROPEAS

Bruselas,
COM(2009) 538

**COMUNICACIÓN DE LA COMISIÓN AL CONSEJO, AL PARLAMENTO
EUROPEO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE
LAS REGIONES**

Hacia la integración de la vigilancia marítima:

Entorno común de intercambio de información sobre cuestiones marítimas de la UE

{SEC(2009) 1341}

HACIA LA INTEGRACIÓN DE LA VIGILANCIA MARÍTIMA: ENTORNO COMÚN DE INTERCAMBIO DE INFORMACIÓN SOBRE CUESTIONES MARÍTIMAS DE LA UE

1. INTRODUCCIÓN

En su Comunicación sobre una política marítima integrada para la Unión Europea, la Comisión Europea se comprometió a avanzar *«hacia un sistema más integrado de vigilancia que aúne los sistemas de supervisión y seguimiento existentes utilizados a efectos de la seguridad marítima, la protección del medio ambiente marino, el control de la pesca, el control de las fronteras exteriores y otras actividades dirigidas al cumplimiento de la ley.»*¹

El Consejo de Asuntos Generales de 8 de diciembre de 2008 animó a la Comisión a trabajar hacia la interoperabilidad entre los sistemas nacionales y comunitarios para incrementar la rentabilidad de las actividades de vigilancia marítima. Este enfoque orientado hacia una mayor integración de la vigilancia marítima fue confirmado en la hoja de ruta para la creación de un sistema europeo de vigilancia de fronteras (EUROSUR), que prevé la creación gradual de un entorno común en el que se comparta la información en el ámbito marítimo de la UE,² así como en la reciente actualización del sistema comunitario de seguimiento y de información sobre el tráfico marítimo³.

El objetivo de la vigilancia marítima integrada es ofrecer un conocimiento de la situación (situational awareness) de las actividades realizadas en el mar con repercusiones en la seguridad y protección marítima, el control de las fronteras, el medio ambiente marino, el control de la pesca, los intereses comerciales y económicos de la Unión Europea, así como en la aplicación de la normativa general y en la defensa, con el fin de facilitar la toma de decisiones apropiada.

El conocimiento de la situación marítima consiste en la comprensión real de las actividades relacionadas con el sector marítimo que pueden tener consecuencias en la seguridad, la protección, la economía o el medio ambiente de la Unión Europea y sus Estados miembros. Establecido sobre la base de exigencias y derechos de los usuarios claramente definidos, dicho conocimiento ayuda a las autoridades responsables de las actividades de control y vigilancia a prevenir y gestionar de manera global todas las situaciones, acontecimientos y medidas relacionadas con el sector marítimo de la UE.

El sector marítimo de la UE comprende las aguas territoriales de los Estados miembros de la UE, las zonas económicas exclusivas y las plataformas continentales, definidas en la Convención de las Naciones Unidas sobre el Derecho del Mar de 1982, así como todas las actividades marítimas desarrolladas en esas zonas, ya sea en el fondo del mar, debajo de la superficie, en la superficie o sobre el mar, como las realizadas por instalaciones, cargueros, pequeñas embarcaciones y buques abanderados en la UE o relacionados de algún modo con la

¹ COM(2007) 575 final de 10.10.2007.

² COM(2008) 68 final de 13.2.2008, p. 9.

³ Directiva 2009/17/CE por la que se modifica la Directiva 2002/59/CE relativa al establecimiento de un sistema comunitario de seguimiento y de información sobre el tráfico marítimo, DO L 131 de 28.5.2009, p. 101. También es relevante el Reglamento (CE) n° 725/2004, de 31 de marzo de 2004, relativo a la mejora de la protección de los buques y las instalaciones portuarias, DO L 129 de 29.4.2004, p. 6.

UE mediante vínculos de propiedad o de gestión. A lo anterior se añade cualquier zona de búsqueda y salvamento y todas las zonas de operaciones que hayan sido designadas para una operación marítima de la UE por una autoridad civil o militar⁴.

Existe una clara necesidad de compartir información sobre vigilancia marítima. Autoridades de sectores diferentes que realizan actividades de control y vigilancia en el mar recopilan datos e información operativa para obtener la mejor imagen posible del conocimiento marítimo para su propio uso. En muchas comunidades de usuarios, actualmente, esta imagen no incluye la información complementaria recopilada por otros usuarios del sector debido a la falta de intercambio mutuo. Si se desarrollan los medios necesarios para permitir el intercambio de datos e información, la imagen del conocimiento marítimo de los distintos usuarios mejorará y esas imágenes aumentarán a su vez la eficacia de las autoridades de los Estados miembros y mejorará la rentabilidad.

El objetivo de la presente Comunicación es establecer los principios que han de presidir la creación de un entorno común de intercambio de información sobre cuestiones marítimas de la UE e iniciar el procedimiento para su instauración. Para conseguir ese objetivo, debe reforzarse la coordinación y la coherencia entre la Comisión Europea, los Estados miembros y los interlocutores que la comunidad europea de defensa indique con ese fin.

2. RETOS

Los retos que se plantean actualmente en cuanto a la creación de un entorno común de intercambio de información sobre cuestiones marítimas de la UE son los siguientes:

Múltiples comunidades de usuarios y operadores: Tanto a escala nacional como comunitaria, las autoridades nacionales responsables de la defensa, el control de las fronteras, las aduanas, la contaminación marítima, el control de la pesca, la protección y la seguridad marítima, la gestión del tráfico de buques, la reacción a los accidentes y catástrofes, la búsqueda y el salvamento, así como de la aplicación de la normativa, recopilan información destinada a su uso propio.

A pesar de que existen medios tecnológicos para compartir toda esa información de forma provechosa, la mayor parte de la información necesaria para adquirir el conocimiento de la situación marítima todavía se recoge mediante numerosos sistemas sectoriales a escala nacional, comunitaria e internacional.

Aunque en algunos casos las autoridades responsables desconocen que una información similar está siendo recogida por otras autoridades y otros sistemas, en otros casos son conscientes de ello pero también son incapaces de compartir esa información debido a que solo determinadas comunidades de usuarios disponen actualmente de normas, acuerdos o políticas de intercambio de información.

Marcos jurídicos diferentes: Las diferentes actividades de vigilancia marítima se llevan a cabo en el marco de los tres pilares de la UE. Los sistemas de vigilancia se han elaborado sobre la base de la legislación internacional y comunitaria específica del sector.

⁴ Si bien todos los ámbitos incluidos en el «sector marítimo de la UE» tienen una repercusión directa o indirecta en la política y en los intereses comunitarios, no todos ellos son competencia de la UE.

Independientemente del marco comunitario existente, nada debería impedir a los Estados miembros integrar sus actividades de vigilancia marítima.

Amenazas transfronterizas: En la mayoría de los casos, las amenazas a las que se enfrentan los Estados miembros en el sector marítimo de la UE precisan tratamiento transnacional, o incluso a veces transectorial, de más envergadura, especialmente en alta mar.

Disposiciones jurídicas específicas: Las actividades de vigilancia marítima en alta mar están reglamentadas por la legislación internacional y la normativa comunitaria, que también regulan el tratamiento de datos personales, confidenciales o clasificados.

3. ÁMBITO DE APLICACIÓN

Teniendo en cuenta los retos mencionados, el éxito del proceso de definición y aplicación para el establecimiento del entorno común de intercambio de información solo se alcanzará con la consulta generalizada y la coordinación total con todas las comunidades de usuarios y operadores interesados y en pleno cumplimiento del principio de subsidiariedad. Cuando se considere oportuno, participarán también los terceros países vecinos.

Los diferentes elementos del concepto de «entorno común de intercambio de información» se entenderán del siguiente modo:

- **«Entorno»:** los sistemas de información sectoriales interconectados que permiten a los usuarios elaborar sus imágenes específicas del conocimiento de la situación y, por lo tanto, determinar tendencias y detectar anomalías y amenazas.
- **«Común»:** los datos de los que se nutre la información deben recogerse solamente una vez, ya que el destino de esa información es ser compartida entre las diferentes comunidades de usuarios.
- **«Intercambio»:** cada comunidad recibe y facilita información en cumplimiento de las normas y procedimientos previamente acordados.
- **«Información»:** debe permitir al usuario elaborar su propio conocimiento de la situación. Aunque proceda de comunidades de usuarios heterogéneas, la información debe ser identificable, accesible, comprensible y utilizable. El tratamiento de la información se realizará con las adecuadas medidas de seguridad.

La creación de un entorno común de intercambio de información aportará las siguientes ventajas:

Interoperabilidad: Es necesario encontrar el modo de permitir el intercambio de información entre los sistemas sectoriales que ya son operativos⁵ y los que están siendo desarrollados por la Unión Europea y sus Estados miembros, que cuentan con el respaldo de agencias comunitarias como la AESM, la ACCP, FRONTEX y la AED⁶. Eso supone el desarrollo de

⁵ Por ejemplo, SafeSeaNet, CleanseaNet, centro de datos LRIT de la UE, gestionados por la AESM.

⁶ La presente Comunicación va acompañada de un documento de trabajo de los servicios de la Comisión en el que se incluye un glosario de términos y acrónimos.

normas, interconexiones, procesos y procedimientos no técnicos existentes, y la creación de nuevos, que permitan el intercambio y la protección de la información compartida sobre la base de derechos de acceso acordados. También mejorará la interoperabilidad entre sistemas sectoriales dentro de un único Estado miembro.

Mejorar el conocimiento de la situación: La información obtenida en dicho entorno debe mejorar considerablemente el conocimiento de la situación dentro de la UE y los Estados miembros.

Eficacia: Por otra parte, este entorno común debería también contribuir a unir los esfuerzos de las diferentes entidades con intereses marítimos y evitar que los mismos datos sean recogidos varias veces, reduciendo así considerablemente los costes financieros de todos los interesados. A su debido tiempo, puede contemplarse un enfoque polivalente cuando se utilicen los instrumentos y recursos de vigilancia de las diferentes comunidades de usuarios.

Subsidiariedad: La gran mayoría de las actividades de control y vigilancia en el mar se realizan bajo la responsabilidad de los Estados miembros. Según el principio de subsidiariedad, los Estados miembros son responsables de coordinar la recogida y la comprobación de la información de todas sus agencias, administraciones y operadores nacionales, preferentemente a través de un mecanismo nacional único de coordinación. Los Estados miembros también deben gestionar, en su caso, los derechos de acceso de terceras partes, calificar los niveles de seguridad de la información y los datos, y aprobar y controlar los mecanismos de difusión selectiva y seguridad de los datos.

4. PRINCIPIOS RECTORES DE LA CREACIÓN DE UN ENTORNO COMÚN DE INTERCAMBIO DE INFORMACIÓN EN EL ÁMBITO MARÍTIMO DE LA UE

4.1. Principio 1: Un enfoque que vincule a todas las comunidades de usuarios

El entorno común de intercambio de información debe permitir a las autoridades de los Estados miembros utilizar de manera más eficaz la información sobre vigilancia marítima. Es preciso que las reglas y normas comunes sean establecidas a escala comunitaria para que el intercambio de información entre las diferentes comunidades de usuarios sea lo más perfecto posible. Cada una de las comunidades debe tener la posibilidad de facilitar y/o recibir a escala nacional información procedente de sistemas y mecanismos de seguridad internacionales⁷, regionales⁸, comunitarios⁹, militares¹⁰ e internos¹¹, a medida que la necesiten, de acuerdo con las condiciones de utilización y los derechos de acceso definidos de los usuarios, para poder elaborar su propia imagen de la situación.

4.1.1. Cuestiones que deberán estudiarse

- (1) *Entorno flexible de intercambio de información:* El entorno común de intercambio de información debe reunir las condiciones de seguridad necesarias, pero también debe ser lo suficientemente flexible para adaptarse a las necesidades y situaciones de los nuevos usuarios. Este aspecto pone de relieve la necesidad de permitir que las

⁷ Por ejemplo, AIS, LRIT.

⁸ Por ejemplo, BSRBCC, BSBC.

⁹ Por ejemplo, SafeSeaNet, centro de datos LRIT de la UE, CleanSeaNet, VMS, EUROSUR.

¹⁰ Por ejemplo, MSSIS, VR-MTC, SUCBAS.

¹¹ Por ejemplo, MAOC-N, CeCLAD, FRONTEx.

comunidades de usuarios que participen en el entorno común de intercambio de información tengan acceso a la mayor información posible para que puedan elaborar su propia imagen de la situación, acorde con sus exigencias operativas. Esa necesidad se determinó, por ejemplo, en las operaciones conjuntas de la agencia FRONTEX para prevenir las actividades ilegales en las fronteras exteriores meridionales de la UE.

- (2) Facilitar una información completa para mejorar el proceso de toma de decisiones: La capacidad de toma de decisiones solo puede mejorarse con la participación de todas las comunidades. Por ejemplo, el intercambio de información entre las autoridades civiles y las fuerzas de defensa debe hacerse en los dos sentidos, respetando las normas relativas a la seguridad de la información.

4.1.2. Recomendaciones

- (1) Evitar la duplicación de los datos: Los datos de seguimiento del tráfico solo deberán difundirse una vez a través del sistema Safe-Sea-Net¹². Esos datos podrán después ponerse a disposición de todos los usuarios reconocidos, incluido el sector de la defensa, de acuerdo con el marco jurídico existente a escala comunitaria o sus modificaciones, si procede.
- (2) Interoperabilidad entre las comunidades de usuarios de la UE: El apoyo de las fuerzas militares de la UE al sector civil en el ámbito de la protección y la seguridad marítimas, incluidas las misiones de respuesta a las catástrofes, exige mejorar la interoperabilidad y conectividad de todos los participantes a escala nacional.
- (3) Coordinación nacional: En primer lugar, es preciso mejorar la gobernanza de los aspectos relacionados con la vigilancia marítima a escala nacional. Con ese fin, se recomienda que las autoridades que ya constituyen plataformas de información sectoriales sirvan de interfaz en el entorno común de intercambio de información.
- (4) Cooperación internacional y regional: Además de la creación de interfaces entre los diferentes sistemas de vigilancia marítima dentro de la UE, hay que prestar atención a la posibilidad de compartir determinados elementos de información con terceros países. En este caso, también deberán tenerse en cuenta cuestiones de seguridad y reciprocidad de la información. Las cinco cuencas marítimas regionales (Mar Báltico, Mar del Norte, Océano Atlántico, Mar Mediterráneo y Mar Negro) y las regiones ultraperiféricas constituyen una amplia zona expuesta a amenazas específicas y para responder a ellas es preciso añadir más esfuerzos.

4.2. Principio 2: Elaborar un marco técnico par la interoperabilidad y la futura integración

La mejor manera de crear un «entorno común de intercambio de información en el ámbito marítimo de la UE» consiste en establecer un marco técnico sin carácter jerárquico aplicable a los sistemas de control y vigilancia marítimos. La arquitectura de ese marco técnico debe concebirse como un espacio de interacción rentable entre los diferentes niveles de información que permita a los usuarios mejorar las imágenes de la situación. La arquitectura del sistema debe permitir, entre otras cosas, recopilar, unir, analizar, divulgar y gestionar los datos al nivel adecuado de descentralización, en función de los requisitos de seguridad (por

¹² Directiva 2002/59/CE del Consejo, modificada por el artículo 22 bis de la Directiva 2009/17/CE.

ejemplo, de información) y en cumplimiento de la normativa sobre protección de datos, las normas internacionales y los requisitos de funcionamiento. Los sistemas existentes deben utilizarse de la manera más eficaz posible.

4.2.1. Cuestiones que deberán estudiarse

- (1) Interoperabilidad e interconexión de los sistemas: En lugar de reunir toda la información en una base de datos única, cada comunidad de usuarios debe hacer que sus datos sean accesibles a las demás comunidades de usuarios que los necesiten y estén autorizadas a recibirlos. De ese modo, cada comunidad de usuarios se convertirá en el editor de su propia información y en el destinatario de la información publicada por las demás comunidades de usuarios en la medida en que la necesite. La arquitectura del sistema debe permitir que la información se utilice mediante normas comunes, que sea fiable para todos los usuarios que la reciben y que solo puedan acceder a ella los usuarios autorizados.
- (2) Utilización de un sistema comunitario: Para algunas categorías de información, es más fácil y más rentable recoger y divulgar los datos de forma centralizada. Todas las comunidades de usuarios interesadas deben utilizar el sistema comunitario SafeSeaNet, que debe desarrollarse para poder funcionar como plataforma principal de intercambio de información en el ámbito marítimo de la UE en lo que respecta a las notificaciones de llegada a puerto o de salida del puerto, información sobre mercancías peligrosas, notificaciones sobre seguridad marítima, información sobre incidentes y accidentes, información procedente de los sistemas AIS y LRIT y datos sobre el control de la contaminación. La Comisión, asistida por el grupo de gestión de alto nivel de SafeSeaNet, llevará a cabo la gestión y seguirá la futura evolución de este sistema, tal como se define en la Directiva 2002/59/CE.
- (3) Utilización de los sistemas sectoriales para compartir información clasificada: Sin embargo, en el caso de determinadas categorías de información como información clasificada, información confidencial sobre seguridad (por ejemplo, los datos relacionados con la seguridad interior y la defensa), es preciso aplicar un enfoque sectorial para salvaguardar los intereses en materia de seguridad de las comunidades de usuarios o de los destinatarios. En principio, dicha información se intercambiará en la medida en que se necesite solamente dentro de la comunidad de usuarios interesada. En caso necesario y si procede, esa información podrá compartirse con otras comunidades de usuarios o destinatarios a escala nacional de acuerdo con la legislación vigente, así como con otros Estados miembros que utilicen los mismos sistemas comunitarios.
- (4) Enfoques regionales: Los Estados miembros considerarán la posibilidad de desarrollar los medios para obtener un conocimiento conjunto de la situación en lo que respecta a las actividades legales e ilegales en el mar que contribuya a mejorar la capacidad de reacción a escala regional.

4.2.2. Recomendaciones

- (1) Marco técnico: La arquitectura del sistema, que tendrá plenamente en cuenta las competencias de las autoridades nacionales establecidas por la legislación nacional y la normativa comunitaria, debe concebirse como una interconexión de diferentes niveles de información basados en la interoperabilidad y en normas comunes que

resulte rentable desde el punto de vista económico. Los distintos niveles deben ofrecer al usuario la mejor solución técnica para acceder a la información, instrumentos eficaces para la extracción de datos, procesos de correlación y criterios armonizados para la detección de modelos normales y anormales. Con este propósito, habrán de acordarse modelos de interoperabilidad y normas sobre la manipulación de datos y deberán establecerse líneas de comunicación seguras entre los usuarios de datos interesados basadas en los derechos de acceso previamente definidos.

Ejemplo de niveles de información (no jerárquicos):



La recogida, fusión, análisis y difusión de la información puede realizarse de la siguiente manera:

- **Recogida:** la utilización por parte de los diferentes usuarios (por ejemplo, autoridades civiles y militares) de los mismos instrumentos (equipos terrestres, satélites, sensores) puede impedir que la misma información sea recopilada varias veces.
- **Fusión:** la fusión de los datos puede colmar lagunas de la información y reducir la incertidumbre provocada por información procedente de diferentes fuentes.
- **Análisis:** los análisis sobre la sensibilidad de los datos desde el punto de vista de la seguridad debe efectuarse por separado.
- **Difusión:** la información adecuada debe transmitirse al responsable de la toma de decisiones en el momento oportuno. Para acceder a la información es preciso disponer de los permisos correspondientes.

- (2) Interoperabilidad y normas comunes: La estructura del sistema exige también la mejor solución técnica para la sincronización de los servicios, la calidad de los datos y metodologías comunes para el intercambio de terminología y datos, sobre la base de las mejores prácticas. Garantizar la coherencia entre las medidas de la UE y las emprendidas por los países vecinos, especialmente en las zonas marítimas regionales compartidas, reviste una importancia fundamental.
- (3) Agencias de la UE: Las agencias de la UE relevantes en este ámbito desempeñan un papel de apoyo y de coordinación muy importante dentro de su comunidad de usuarios. También pueden, en caso necesario, servir de plataforma para el intercambio de información.

4.3. Principio 3: Intercambio de información entre autoridades civiles y militares

La información sobre vigilancia debe compartirse entre las autoridades civiles y militares para evitar duplicidades y para que sea rentable económicamente. Aunque tienen finalidades y mandatos diferentes, es preciso que ambas autoridades dispongan de normas y procedimientos comunes para tener acceso a la información y a su utilización con el fin de efectuar el intercambio de información en dos direcciones.

4.3.1. Cuestiones que deberán estudiarse

- (1) En lo que respecta a las funciones y competencias de las autoridades nacionales, regionales o internacionales, establecidas por la legislación nacional y la normativa comunitaria, el apoyo de las fuerzas armadas de los Estados miembros en las intervenciones civiles de seguridad marítima y de seguridad interna es importante y exige una mayor interoperabilidad y conectividad entre todos los interesados. Igualmente, los datos procedentes del sector civil pueden revelarse útiles para operaciones militares.
- (2) El cumplimiento de la legislación nacional y de la normativa comunitaria exige normas y capacidad para operar en alta mar. Tecnologías como la recopilación y análisis de imágenes satélite de alta resolución, patrullas aéreas, la explotación de plataformas deshabitadas, la detección y el análisis de sonidos submarinos, que han constituido hasta ahora competencias típicas de defensa, se están considerando cada vez más válidas para su uso civil. Las comunidades de usuarios civiles, por su parte, pueden aportar a la comunidad militar una amplia contribución en forma de información obtenida a partir del entorno común de intercambio de información para elaborar una imagen marítima reconocida (*Recognized Maritime Picture*).

4.3.2. Recomendaciones

- (1) Mayor coordinación: Para conseguir los objetivos mencionados mediante la creación de un entorno común de intercambio de información debe aumentarse la coordinación entre la Comisión Europea, los Estados miembros y los interlocutores que el sector europeo de la defensa indique. Esta mayor coordinación puede traducirse en orientaciones políticas, respetando plenamente el marco jurídico de cada comunidad de usuarios.
- (2) Mejor utilización de los instrumentos de vigilancia en todas las comunidades: Los usuarios civiles y militares autorizados deberán tener la posibilidad de solicitar y recibir información de los instrumentos europeos de vigilancia con fines de vigilancia

marítima. A escala técnica, esto implica normas comunes para compartir, recopilar y presentar la información a usuarios individuales, en su caso.

- (3) Datos de origen espacial: Europa se ha comprometido a desarrollar su propia capacidad operativa para la observación de la Tierra a través del programa de Vigilancia Mundial del Medio Ambiente y la Seguridad (GMES). Mediante la utilización de elementos de origen espacial para mejorar el conocimiento de la situación marítima será posible aportar ayuda a las operaciones llevadas a cabo por autoridades civiles y militares, como el control del tráfico marítimo, el seguimiento de la contaminación marina y la lucha contra las actividades ilegales en el mar. Actualmente, la utilización de la observación espacial para el seguimiento de la contaminación marina ya forma parte del sistema CleanSeaNet aplicado por la AESM. Estas cuestiones también están siendo tratadas por el GMES, ya que contribuyen a la elaboración de las aplicaciones de seguridad en los ámbitos de la vigilancia de las fronteras marítimas exteriores de la UE y del apoyo a la acción exterior de la UE.

4.4. Principio 4: Disposiciones jurídicas específicas

Es preciso detectar en la legislación nacional y la normativa comunitaria los obstáculos al intercambio de datos sobre control y vigilancia para el establecimiento de un entorno común de intercambio de información. Al suprimirlos, convendrá conceder la debida atención al respeto de la confidencialidad de los datos, a las cuestiones relativas a los derechos de propiedad intelectual y a la protección de los datos personales, así como a la propiedad de los datos de conformidad con las leyes nacionales e internacionales.

4.4.1. Cuestiones que deberán estudiarse

- (4) Tratamiento de datos personales: Las diversas actividades mencionadas en las anteriores secciones pueden implicar el tratamiento de datos personales. En el marco del entorno común de intercambio de información deben observarse los principios de la normativa relativa a la protección de los datos personales, aplicable en la Unión Europea¹³. Los datos personales deben recogerse con fines legítimos y utilizarse y transferirse con objetivos compatibles con aquellos con los que se recogieron inicialmente.
- (5) Requisitos de confidencialidad: Se observa que una cantidad significativa de datos de comunicación y vigilancia en el sector marítimo se clasifican como confidenciales (en el ámbito comercial) y/o deben considerarse como tales. En lo que respecta a la confidencialidad, el obstáculo principal es la naturaleza explícita de las disposiciones sobre confidencialidad de algunos instrumentos fundamentales pertenecientes al control y la vigilancia. Por consiguiente, para el tratamiento y la posterior transferencia de este tipo de datos será preciso comprobar que los destinatarios de los datos estén igualmente vinculados por obligaciones de confidencialidad y secreto profesional, como ya ocurre actualmente con las disposiciones del LRIT.

13 Directiva 95/46/CE 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 (DO L 281 de 23.11.1995, p. 31) y las disposiciones nacionales que la aplican. Reglamento (CE) n° 45/2001 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 (DO L 8 de 12.1.2001, p. 1); Convenio del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal de 28 de enero de 1981 (ETS 108). Dicho Convenio está completado por el Protocolo adicional relativo a las autoridades de control y los tránsitos transfronterizos de datos (ETS 181 de 8 de noviembre de 2001) y por la Recomendación n° R(87) 15, de 17 de septiembre de 1987, del Consejo de Europa dirigida a regular el uso de los datos de carácter personal en el sector de la policía.

- (6) Intercambio de datos civiles/militares: En relación con el posible intercambio de información y datos entre las diferentes autoridades (incluidas las autoridades militares), es preciso estudiar la forma de garantizar la integridad de la información clasificada, de los datos comerciales confidenciales y de la información relativa a las investigaciones penales y la protección de los datos personales.

4.4.2. Recomendaciones

- (1) En aras de la seguridad jurídica de todos los interesados, se propone que cualquier mecanismo destinado a permitir el intercambio transfronterizo de datos procedentes de diferentes bases de datos se someta a un marco jurídico preciso, en función de la necesidad de información, que defina al menos la naturaleza de los datos de que se trate, la competencia de los suministradores de datos, la finalidad (y los métodos) del intercambio y los destinatarios potenciales de los datos, y que incorpore las medidas de salvaguardia necesarias con respecto a la confidencialidad y la seguridad de los (o algunos) datos y la protección de los datos personales, cuando sea relevante y habida cuenta de las disposiciones legales y los sistemas operativos existentes a escala comunitaria.
- (2) El tratamiento de datos personales con fines militares y para la seguridad del Estado y la aplicación del derecho penal queda excluido actualmente del marco jurídico general de la protección de datos. No obstante, la cuestión de la protección de datos puede considerarse en cada caso particular mediante los instrumentos jurídicos específicos en esos ámbitos, tanto a escala comunitaria como nacional¹⁴. Por consiguiente, serán necesarias medidas de salvaguardia adicionales en caso de que esté previsto compartir datos personales entre autoridades pertenecientes al ámbito de aplicación del marco jurídico existente para la protección de datos (por ejemplo, autoridades de pesca) y autoridades (actualmente) excluidas de dicho ámbito (por ejemplo, autoridades militares o de la seguridad del Estado).

5. PERSPECTIVAS

El objetivo de los *principios rectores de la creación de un entorno común de intercambio de información en el ámbito marítimo de la UE* es, como ya se ha explicado, suscitar un proceso de reflexión a escala nacional y comunitaria. Esta labor exigirá la participación de todas las comunidades de usuarios para determinar claramente sus necesidades y las medidas para responder a ellas. Con ese fin, los servicios de la Comisión cooperarán con el equipo de redactores expertos de la Agencia Europea de Defensa en el marco del mandato que les ha sido confiado de publicar un informe sobre la vigilancia marítima.

En este marco, se propone establecer una cooperación permanente y estructurada entre los diferentes interesados europeos en los ámbitos civil y militar de los Estados miembros para encontrar soluciones innovadoras dentro del marco jurídico vigente. La coordinación puede contribuir a mejorar la interoperabilidad y la conectividad entre los sistemas civiles y militares existentes.

¹⁴ Decisión marco 2006/XX/JAI del Consejo relativa a la protección de los datos personales tratados en el marco de la cooperación policial y judicial en materia penal, DO L 350 de 30.12.2008, p. 60.

Se propone también que la labor de creación de un entorno común de intercambio de información se lleve a cabo en el marco del grupo de expertos de los Estados miembros de la Comisión sobre la integración de la vigilancia marítima, de forma compatible con otros trabajos en curso en grupos sectoriales y en comités de acuerdo con sus competencias respectivas. El grupo de expertos se ocupará principalmente de la arquitectura del sistema de intercambio de información entre los diferentes sistemas sectoriales, teniendo en cuenta los marcos jurídicos existentes y examinando las barreras de procedimiento y tecnológicas para compartir información.

La constitución de un entorno común para compartir información no debería, en ningún caso, entorpecer el desarrollo de sistemas de información sectoriales existentes o previstos, ni su evolución, siempre que se tengan en cuenta las necesidades de interoperabilidad que permitan el intercambio de información con otros sistemas pertinentes.

Según un enfoque iterativo, los principios rectores pueden revisarse, sobre todo a la luz de los resultados de los tres proyectos siguientes, que se realizarán con objeto de evaluar la capacidad de los usuarios de los diferentes Estados miembros y comunidades de usuarios para intercambiar información:

- (1) Proyecto piloto sobre la integración de la vigilancia marítima en el Mar Mediterráneo y en la zona adyacente del Atlántico¹⁵. El propósito de este proyecto de dos años de duración es evaluar la capacidad de seis Estados miembros de esta región para intercambiar información sobre vigilancia en lo que respecta al control de las fronteras, la lucha contra el narcotráfico, el terrorismo y el contrabando de bienes ilegales, y la prevención de la contaminación marina. El inicio del proyecto está previsto para finales de 2009.
- (2) Proyecto piloto sobre la integración de la vigilancia marítima en las cuencas marítimas del Norte de Europa¹⁶, con objetivos y duración similares a los del proyecto piloto del Mar Mediterráneo.
- (3) Con motivo del programa de trabajo de 2010 del 7º Programa Marco de Investigación y Desarrollo (tema de la seguridad), se publicó una convocatoria de propuestas para un programa de demostración sobre la integración, la validación y la demostración a gran escala de una solución de «sistemas de sistemas» para la vigilancia de las fronteras marítimas. Las principales cuestiones tratadas son la detección de pequeñas embarcaciones, la fusión de datos para detectar anomalías, la interoperabilidad y la asequibilidad. La solución se probará en una zona seleccionada de la frontera marítima exterior para mostrar, desde un punto de vista técnico, el camino a seguir para el desarrollo del entorno común de intercambio de información en el ámbito marítimo de la UE. Además, dentro del tema «Espacio» del 7º PM, se publicó una convocatoria de propuestas para desarrollar la capacidad de los servicios preoperativos del GMES destinados a la vigilancia marítima.

En el documento de trabajo de los servicios de la Comisión, adjunto a la presente Comunicación, figura una lista de otras iniciativas comunitarias relativas a la integración de la vigilancia marítima.

¹⁵ Convocatoria de propuestas MARE/2008/13.

¹⁶ Convocatoria de propuestas MARE/2009/41.

6. CONCLUSIONES

La utilización de un enfoque integrado de la vigilancia marítima permitirá a las autoridades responsables de las actividades marítimas mejorar su eficacia al poner a su disposición más instrumentos y más información para la realización de sus funciones. Contribuirá también al aumento de la eficacia de las operaciones y a la reducción de gastos de funcionamiento. El ahorro que ello supondría a escala europea es considerable, habida cuenta de la creciente necesidad de detectar, identificar, seguir e interceptar distintas actividades, como la inmigración ilegal o la pesca clandestina, así como prevenir accidentes marítimos, proteger el medio ambiente y facilitar el comercio. Los beneficios que se derivarán de este proceso tendrán repercusiones positivas en la seguridad nacional, la protección y seguridad marítima, la protección del entorno marino, el control de las fronteras y, en general, el cumplimiento de la normativa.

Por consiguiente, la Comisión invita al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones a:

- apoyar los objetivos presentados en la presente Comunicación;
- sostener el enfoque propuesto en sus sectores de responsabilidad respectivos.