COMISIÓN
EUROPEA

Bruselas, 27.11.2013
COM(2013) 842 final

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO

sobre un sistema europeo de seguimiento de la financiación del terrorismo (TFTS de la UE)

{SWD(2013) 488 final}
{SWD(2013) 489 final}

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO

sobre un sistema europeo de seguimiento de la financiación del terrorismo (TFTS de la UE)

Con carácter complementario a la Comunicación de 13 de julio de 2011 (COM (2011) 429), el objeto de la presente Comunicación es informar al Parlamento Europeo y al Consejo de los resultados del análisis de viabilidad de la implantación de un sistema europeo de seguimiento de la financiación del terrorismo (TFTS de la UE).

1. CONTEXTO

1.1. Origen de la petición y definición

Durante las negociaciones que precedieron a la celebración del Acuerdo TFTP UE - EE.UU.[1], se celebró un debate sobre las mejores condiciones para proteger los datos personales y respetar los derechos fundamentales en el contexto de ese Acuerdo. Algunas de las partes arguyeron que la extracción de datos en territorio europeo limitaría el volumen de datos transferidos a los EE.UU, lo que reforzaría consiguientemente las garantías de protección de datos. Algunos Estados miembros apreciaron la existencia de valor añadido en el desarrollo de un sistema independiente europeo para el seguimiento de la financiación del terrorismo a más largo plazo. El Parlamento Europeo solicitó al Consejo y a la Comisión que adoptasen cuantas medidas fueran necesarias para hallar una solución duradera y segura desde el punto de vista jurídico a la extracción de los datos solicitados en territorio europeo. Al aceptar el TFTP UE-EE.UU., el Consejo y el Parlamento Europeo solicitaron a la Comisión que presentase, en el plazo de un año desde la entrada en vigor del Acuerdo, un marco legal y técnico para la extracción de datos en el territorio de la UE y, en el plazo de tres meses desde la entrada en vigor del Acuerdo, un informe de situación sobre la creación de un sistema equivalente en la UE[2]. Además, el artículo 11 del Acuerdo TFTP UE-EE.UU. establece que, durante el periodo de vigencia del Acuerdo, la Comisión estudie la posibilidad de introducir un sistema equivalente de la UE que facilite una transferencia más selectiva de los datos.

---

[1] DO L 195 de 27.7.2010, p.5.

[2] Decisión del Consejo de 13 de julio de 2010 (DO L 195 de 27.7.2010).

A los efectos de la presente Comunicación, es preciso establecer una distinción entre el sistema equivalente de la UE y el marco de extracción de los datos en el territorio de la UE. Por *marco de extracción de los datos* en el territorio de la UE se entiende un sistema que permita la realización en el territorio de la UE de búsquedas en los datos actualmente facilitados por la UE a los EE.UU. En cambio, por *sistema equivalente de la UE* se entendería un sistema europeo independiente de seguimiento de la financiación del terrorismo mediante mecanismos de acceso, búsqueda y análisis de los datos del proveedor o los proveedores designados. El establecimiento de cualquier sistema de la UE requeriría una modificación del Acuerdo TFTP UE-EE.UU.

1.2. Medidas adoptadas

En diciembre de 2010, la Comisión contrató la realización de un *estudio* que se amplió en julio de 2011 para abarcar una opción adicional consistente en un régimen de conservación y extracción. Mientras se realizaba ese estudio, la Comisión organizó cuatro reuniones de expertos en las que participaron Europol, el Supervisor Europeo de Protección de Datos, el proveedor designado del TFTP[3] y numerosos expertos de los Estados miembros en representación de los ministerios interesados, organismos con funciones coercitivas y servicios de inteligencia y autoridades de protección de datos.

El 13 de julio de 2011, en su *Comunicación al Parlamento Europeo y al Consejo («Comunicación de 2011»)*, la Comisión presentó cinco opciones posibles para un sistema europeo de seguimiento de la financiación del terrorismo (TFTS de la UE). Tres de estas opciones se consideraron viables. El objetivo de la Comunicación de 2011 era abrir un debate sobre las posibilidades de actuación futura y aportar material de referencia para la evaluación de impacto preceptiva.

El asunto se presentó ante el Consejo de JAI de octubre de 2011 y la comisión de libertades del Parlamento Europeo.

Dado que ni los Estados miembros ni el Parlamento Europeo expresaron una preferencia clara por ninguna de las opciones, se resolvió estudiarlas todas en la evaluación de impacto de la

[3] Sociedad de telecomunicaciones financieras interbancarias mundiales (SWIFT)

Comisión y desarrollarlas en distintas subopciones. La presente Comunicación se basa en la evaluación de impacto[4].

2. PRINCIPIOS BÁSICOS DE LA COMISIÓN Y OPCIONES DETERMINADAS

2.1. Principios de la Estrategia de gestión de la información adoptada bajo la Presidencia sueca

En su análisis de las propuestas de actuación futura, la Comisión tiene en cuenta los principios esenciales recogidos en la Estrategia de gestión de la información de 2009[5], posteriormente incorporadas y desarrolladas en las Comunicaciones de la Comisión sobre el panorama general de la gestión de la información en el espacio europeo de libertad, seguridad y justicia, de 2010[6], y sobre el Modelo Europeo para el Intercambio de Información, de 2012[7].

Esenciales a este respecto son los principios de protección de los derechos fundamentales y de necesidad, proporcionalidad y rentabilidad.

La garantía de los *derechos fundamentales* consagrados en la Carta de los Derechos Fundamentales de la Unión Europea, particularmente el derecho a la privacidad y a la protección de los datos personales, es una preocupación primordial al elaborar nuevas propuestas que impliquen el tratamiento de datos personales en el ámbito de la seguridad interior. Los artículos 7 y 8 de la Carta proclaman el derecho de toda persona al «respeto de su vida privada y familiar» y a «la protección de los datos de carácter personal que la conciernan». El artículo 16 del Tratado de Funcionamiento de la Unión Europea, que es vinculante para los Estados miembros y para las instituciones, agencias y organismos de la Unión, reafirma el derecho de toda persona a «la protección de los datos de carácter personal que la conciernan». Conforme al artículo 52 de la Carta y con arreglo al principio de proporcionalidad, solo pueden introducirse limitaciones del ejercicio de los derechos reconocidos en la Carta cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás.

---

4 SWD 2013 (xx) de

5 COM(2012) 735 de 7 de diciembre de 2012.

6 Conclusiones del Consejo de 30 de noviembre de 2009 sobre la Estrategia de gestión de la información para la seguridad interior 16637/09

7 COM(2010) 385 de 20 de julio de 2010.

La interferencia con el derecho a la privacidad se considera *necesaria* si responde a una necesidad social acuciante, si guarda proporción con el objetivo perseguido y si las razones expuestas por la autoridad pública para justificarla son pertinentes y suficientes.

Si bien es difícil evaluar todos los costes del terrorismo en términos económicos, sigue siendo válido el principio de *rentabilidad.* Un planteamiento *de rentabilidad* tiene en cuenta las soluciones existentes para minimizar todo solapamiento y maximizar toda sinergia posible. Es preciso llevar a cabo una evaluación que determine la posibilidad de cumplir los objetivos de la propuesta utilizando con mayor eficacia los instrumentos existentes.

2.2. Enfoque

Teniendo presentes los principios recién expuestos, la Comisión ha examinado la necesidad y proporcionalidad de un TFTS de la UE en relación con sus costes, beneficios e impacto en los derechos fundamentales, en comparación con la situación actual.

Por lo que respecta a los *beneficios*, un sistema de la UE podría aumentar la capacidad de la UE y de sus Estados miembros para acceder a los datos pertinentes y reforzar sus capacidades analíticas de rastreo e identificación de terroristas a través de sus transacciones financieras. Dado que las transacciones financieras pueden revelar información valiosa y no disponible a través de otras fuentes, este instrumento encerraría un valor especial para la detección de actividades terroristas y la identificación de los agentes implicados. Por consiguiente, un TFTS de la UE podría constituir una herramienta adicional de información e investigación en la lucha contra el terrorismo y el refuerzo de la seguridad en la UE, especialmente si ese sistema cubriese las actividades de numerosos proveedores de datos y tipos de transacciones financieros. Las ventajas que puede reportar un TFTS de la UE deben sopesarse frente a los costes de implantación y mantenimiento de ese sistema, incluida la carga que puede representar para la UE, los Estados miembros y los proveedores designados de los datos en cuestión.

2.3. Presentación de las distintas opciones

Tanto para el *marco de extracción de* datos en el territorio de la UE como para el *sistema equivalente de la UE* se han analizado distintas opciones.

2.3.1. Marco de extracción de datos en el territorio de la UE

El marco de extracción de datos en el territorio de la UE podría consistir en un sistema de conservación y extracción de los datos que guarda el proveedor designado previa autorización de acceso directo a los datos, facultad de la que actualmente disfrutan los EE.UU. con arreglo al TFTP. Ese acceso directo se conferiría a los analistas u expertos de los EE.UU. habilitados a tal efecto.

Una de las posibilidades de esta opción sería conservar los datos en el servidor del proveedor designado durante un periodo determinado y llevar a cabo las búsquedas directamente en su servidor. No obstante, el proveedor actualmente designado con arreglo al Acuerdo TFTP UE-EE.UU. ha implantado estrictas medidas de protección de datos y de seguridad que impiden la identificación de las personas mencionadas en el contenido de los datos del mensaje, por lo que su base de datos actual no permite realizar búsquedas a partir de datos personales. Sería preciso, por lo tanto, crear otra base de datos separada.

De forma alternativa, los datos podrían extraerse y mantenerse en otro emplazamiento seguro en la UE. Los analistas o expertos de los EE.UU. autorizados para efectuar las búsquedas podrían estar físicamente presentes en los locales del proveedor designado o disponer de acceso remoto a los datos. En todos los casos y, con independencia de la ubicación de los datos, sería preciso establecer dispositivos completos y sólidos de salvaguardia adaptados a la configuración particular del sistema.

2.3.2. Sistema equivalente de la UE

Para un sistema equivalente de la UE (como se anunciaba en la Comunicación de 2011), se han estudiado distintas opciones que incluyen un sistema plenamente centralizado al nivel de la UE, un sistema descentralizado al nivel de los Estados miembros y tres sistemas híbridos en los que tanto la UE como los Estados miembros desempeñarían algún papel.

Cada una de las opciones presenta diversas posibilidades en lo que respecta al alcance del sistema de la UE. Es preciso tomar ciertas decisiones en lo que respecta a los tipos de mensajes y proveedores designados que se incluirían. El sistema equivalente de la UE podría ajustarse al tipo de mensajes sobre transacciones financieras y al proveedor designado que actualmente recoge el Acuerdo TFTP UE-EE.UU. u ofrecer soluciones más amplias.

- La opción de un sistema plenamente centralizado a nivel de la UE implicaría que un único organismo de la UE ejecutaría todas las funciones esenciales del sistema: solicitar la extracción de datos, almacenar datos, efectuar búsquedas, llevar a cabo análisis de inteligencia, proteger y supervisar el sistema y divulgar pistas de inteligencia a los Estados miembros. Esta opción es poco sostenible desde el punto de vista jurídico, pues supondría un incumplimiento del artículo 72 del TFUE, que confirma que la responsabilidad principal de mantener el orden público y la salvaguardia de la seguridad interior incumbe a los Estados miembros. Semejante sistema no sería viable ni resultaría aceptable para los Estados miembros, pues requeriría la creación de alguna forma de capacidad de inteligencia centralizada al nivel de la UE.
- Un sistema plenamente descentralizado a nivel de los Estados miembros implicaría la gestión del sistema por parte de las autoridades competentes de los Estados miembros, sin que a nivel de la UE se desempeñara función alguna. Esto significaría que los datos podrían transferirse hacia los 28 Estados miembros e interrogarse en todos ellos en paralelo, lo que multiplicaría los flujos de datos y tendría importantes repercusiones en los costes. Además, aumentaría el riesgo de tratamiento incoherente de los datos y desembocaría en la creación de mecanismos desiguales de protección de datos. Por lo tanto, esta opción tampoco se considera viable.

Se ha descartado por lo tanto la evaluación más detallada de ambas opciones.

Las tres opciones restantes para un sistema equivalente de la UE implican una distribución de las distintas funciones entre las distintas organizaciones a los niveles de la UE y nacionales («sistemas híbridos»).

En todos estos sistemas híbridos, los datos deberían solicitarse de forma constante y reiterada al proveedor o los proveedores de datos, extraerse y almacenarse en un emplazamiento seguro en la UE. Las búsquedas se efectuarían a continuación en esta base de datos central. En cualquiera de las opciones sería también preciso implantar las garantías de protección de datos adecuadas.

- A) En el primer sistema híbrido o Servicio de coordinación y análisis del TFTS de la UE sería preciso crear una unidad central de la UE a la que corresponderían las tareas

de solicitar datos al proveedor o los proveedores designados, efectuar las búsquedas, llevar a cabo los análisis de inteligencia y distribuir los resultados. La diferencia con un sistema plenamente centralizado sería que los Estados miembros disfrutarían de acceso directo al sistema y podrían solicitar la realización de búsquedas en su nombre por la unidad central o por sus propios analistas.

- B) El segundo sistema híbrido o Servicio de extracción del TFTS de la UE implicaría también la creación de una unidad central de la UE. No obstante, en esta opción el organismo de la UE efectuaría las búsquedas a petición de los Estados miembros y divulgaría los resultados a los Estados miembros sin proceder a un análisis de inteligencia. No obstante, el organismo de la UE podría efectuar sus propias búsquedas y analizar los resultados que estas arrojen.

- C) Con el último sistema híbrido o Servicio de coordinación de la Unidad de inteligencia financiera[8] (UIF), se crearía una plataforma especial de la UE. No sería un órgano permanente sino más bien de la reunión periódica de un grupo de expertos en inteligencia financiera. Lo que se podría hacer con ese fin sería ampliar la plataforma UIF. Cada Estado miembro designaría a un representante que actuaría en su nombre. Esta autoridad especial reuniría las solicitudes presentadas a la UIF por cada Estado miembro y emitiría las solicitudes de datos al proveedor o los proveedores designados con arreglo a lo requerido por esos Estados miembros. El representante de cada Estado miembro sería responsable de efectuar las búsquedas, llevar a cabo los análisis y gestionar los resultados en nombre de su propio Estado miembro. Correspondería después a las autoridades competentes de los Estados miembros utilizar las pistas de inteligencia y proceder a su mayor divulgación a escala nacional.

2.3.3. Statu quo: Acuerdo TFTP UE-EE.UU.

Actualmente, la UE y los Estados miembros pueden solicitar a los EE.UU. que efectúen búsquedas al amparo del Acuerdo TFTP UE-EE.UU. relativo al tratamiento y la transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos a efectos del Programa de seguimiento de la financiación del terrorismo (TFTP).

[8] Decisión 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.

El TFTP es una herramienta de lucha contra el terrorismo desarrollada por los EE.UU. en el periodo que siguió a los atentados terroristas del 9/11. Se basa en la búsqueda de los datos facilitados por el proveedor de datos, incluidos los transferidos por la UE.

El Acuerdo TFTP UE-EE.UU regula pormenorizadamente el proceso de solicitud de los datos por las autoridades de los EE.UU. Europol comprueba que las solicitudes de datos recibidas de los EE.UU se ajustan al Acuerdo y, en particular, que están especificadas con el mayor detalle posible para minimizar el volumen de datos transferidos. Numerosas disposiciones se dedican a regular el manejo, el almacenamiento y la supresión de los datos. Los datos facilitados se conservan en un entorno físico seguro y se almacenan aparte de otros datos. El Acuerdo impone un periodo de conservación de cinco años, además de la obligación de revisar regularmente la necesidad de conservar los datos. Entre los supervisores independientes ubicados en los EE.UU se incluyen dos seleccionados por la UE. Estos ejercen un control continuo sobre el método de operación del sistema y tienen la posibilidad de comprobar todas las búsquedas efectuadas por el Departamento del Tesoro de los EE.UU. a fin de asegurarse de que la búsqueda presenta algún nexo con el terrorismo o su financiación.

El Acuerdo incluye además disposiciones sobre el derecho de acceso a los datos personales y a su rectificación y sobre los procedimientos de recurso. El Acuerdo establece que cualquier persona que estime que sus datos personales se han tratado contraviniendo lo dispuesto en el Acuerdo podrá pedir reparación efectiva por la vía administrativa o judicial al amparo de la legislación de la Unión Europea, sus Estados miembros y los Estados Unidos, respectivamente. El Acuerdo establece además que todas las personas, con independencia de su nacionalidad o su país de residencia, disponen de una vía de recurso judicial al amparo de la legislación de los EE.UU. contra todo acto de la Administración que les perjudique.

Las normas pertinentes para la obtención de reparación respecto de un acto administrativo perjudicial del Departamento del Tesoro en relación con los datos recibidos en aplicación del Acuerdo incluyen la Ley de Procedimiento Administrativo (*Administrative Procedure Act*) y la Ley de Libertad de Información (*Freedom of Information Act*). La Ley de Procedimiento Administrativo brinda a las personas que hayan sufrido daños y perjuicios como resultado de un acto de la Administración de los EE.UU. la posibilidad de recurrir ese acto por vía judicial. La Ley de Libertad de Información permite a las personas utilizar las vías de recurso administrativa y judicial para acceder a los registros públicos. Los procedimientos uniformes

vigentes de acceso, rectificación, supresión o bloqueo de los datos personales, acordados por la Comisión, los EE.UU y el Grupo de trabajo del artículo 29 pretenden facilitar a los ciudadanos de la UE el ejercicio de esos derechos. La aplicación del Acuerdo y sus salvaguardias y controles es objeto de revisiones periódicas conforme al artículo 13 del Acuerdo. En 2011[9] y 2012[10] se llevaron sendas revisiones de ese tipo, que permitieron concluir que el Acuerdo se había ejecutado correctamente. Está prevista una tercera revisión para la primavera de 2014. El informe conjunto sobre el valor de los datos facilitados, elaborado con arreglo al artículo 6 del Acuerdo, pone de manifiesto la utilidad del TFTP para prevenir el terrorismo y luchar contra él, así como el uso del TFTP por parte de varios Estados miembros. La información del TFTP y su exactitud permiten la identificación y el rastreo de los terroristas y sus redes de apoyo en todo el mundo. Revela datos sobre las estructuras financieras de las organizaciones terroristas y permite la identificación de nuevas fuentes de ayuda financiera y de los individuos involucrados.

3. EVALUACIÓN

Al evaluar la conveniencia de proponer el establecimiento de un TFTS de la UE, la Comisión ha de conciliar las distintas opiniones y expectativas acerca del grado de ambición de un sistema propio de la UE. Los distintos interesados y responsables tienen diferentes conceptos de los objetivos del TFTS de la UE. La Comisión ha examinado las posibilidades e implicaciones de ambas hipótesis, confrontándolas a los principios de elaboración y aplicación de nuevas iniciativas políticas antes expuestos. Concretamente, cada opción se ha sopesado con arreglo a los criterios de necesidad, proporcionalidad y rentabilidad.

3.1. Marco de extracción de datos en el territorio de la UE

Conforme a lo descrito en la sección 2.3.1., la opción consistente en un régimen de conservación y extracción permitiría la recogida, el almacenamiento y la búsqueda de datos (que actualmente se transfieren a los EE.UU con arreglo al TFTP UE-EE.UU,) en el territorio de la UE. Por consiguiente, en comparación con la situación actual, no generaría beneficios adicionales para la UE ni para los Estados miembros. Por el contrario, debido al almacenamiento de los datos TFTP en los EE.UU. y en la UE, la fragmentación de las búsquedas, que actualmente se efectúan dentro de un único conjunto de datos TFTP, podría

[9] SEC(2011) 438 de 30 de marzo de 2011.
[10] SWD(2012) 454 de 14 de diciembre de 2012.

repercutir de forma negativa en la calidad y el número de pistas de inteligencia y menoscabar la eficiencia general del TFTP. Además, podría ralentizar significativamente el proceso de análisis, puesto que un seguimiento más pormenorizado de una pista de inteligencia podría exigir diferentes búsquedas consecutivas en los datos TFTP almacenados en dos emplazamientos, y a menudo la rapidez es un factor esencial en las investigaciones sobre terrorismo.

La extracción de los datos en territorio europeo, en lugar de en el territorio de los EE.UU., no garantizaría por sí misma una mejor protección de los datos personales. La protección del acceso a los datos es clave para asegurar su adecuado manejo, con independencia de su ubicación. Con tal fin, se precisaría un conjunto de sólidas garantías que garantizase el cumplimiento de los requisitos necesarios en toda operación de tratamiento y manejo de los datos. El sistema habría de estar equipado con una función de control para verificar las solicitudes de búsquedas y sus justificaciones. El papel de los supervisores independientes sería crucial para asegurar que los datos se usen con los fines restringidos definidos en cualquier acuerdo constitutivo. Deberían adoptarse medidas que impidieran todo acceso no autorizado o toda revelación indebida de los datos, como el mantenimiento de estos en un entorno físico seguro. Deberían incorporarse procedimientos de acceso a los datos personales y de rectificación de los mismos, así como las vías de recurso oportunas. Debería encargarse una auditoría externa para asegurar el correcto funcionamiento del sistema.

Con arreglo al Acuerdo TFTP UE-EE.UU., los Estados Unidos no tienen acceso a todos los datos del proveedor designado, sino solamente a los juegos de datos solicitados por dicho país y aprobados por Europol conforme a los análisis de riesgo de terrorismo vigentes en el pasado y en la actualidad. A no ser que se implante un mecanismo similar de restricción inicial de datos, la autorización de búsquedas directas en la totalidad de los datos del proveedor designado aumentaría aun más la exposición de los datos, con las consiguientes repercusiones en los derechos de protección de los mismos. Ello exigiría una importante reformulación de los métodos de trabajo y almacenamiento de datos del proveedor designado. Actualmente, los mensajes financieros regulados por el Acuerdo se conservan en un formato que impide la identificación de las personas mencionadas en el contenido de datos del mensaje. Cada mensaje sobre transacciones financieras es cifrado y solo puede ser objeto de búsqueda a través de metadatos, es decir, la fecha de envío del mensaje, el tipo de mensaje y los bancos

emisores y receptores. El proveedor designado ha implantado estrictas medidas de seguridad y protección de datos a fin de proteger los datos de sus clientes en todo el mundo. Por lo tanto, para permitir la realización de búsquedas directas en el servidor del actual proveedor designado, todos esos mensajes deberían ser primero descifrados. Esa operación resultaría tan excesiva como desproporcionada, habida cuenta de que el servidor del proveedor designado contiene más mensajes de los que se requieren para la lucha contra el terrorismo. Además, el acceso directo con fines de búsqueda sería prohibitivamente invasivo en las operaciones cotidianas del proveedor designado y generaría considerables riesgos operativos, sistémicos y para la seguridad. Por lo tanto, requeriría la creación de una base de datos separada en el territorio de la UE que albergase los datos necesarios del proveedor designado.

Para poner en marcha el sistema y garantizar la plena observancia de las garantías de seguridad se requerirían cuantiosas inversiones. Sería preciso adaptar los locales del proveedor designado -u otras instalaciones de seguridad- a los requisitos específicos, desarrollar soluciones de TI y técnicas y contratar y formar personal debidamente cualificado para administrar y supervisar el sistema.

En esta opción, la UE y los Estados miembros cargarían con todos los inconvenientes y costes de un mecanismo creado exclusivamente al servicio del TFTP, instrumento propiedad de un tercer país. Actualmente, esta opción no se considera necesaria, proporcional ni rentable pues no aportaría beneficios adicionales en el ámbito de la inteligencia, sería costosa y podría poner en riesgo la protección de los datos personales.

3.2. Sistema equivalente de la UE

Se ha descartado una evaluación más pormenorizada de un TFTS de la UE plenamente centralizado debido a la inexistencia de base jurídica y a la escasa posibilidad de que los Estados miembros acepten otorgar a la UE un papel centralizado en un área de competencia de los primeros. El sistema plenamente descentralizado se ha excluido debido a sus posibles y graves implicaciones económicas y a su múltiple impacto en los derechos de protección de datos. Los tres sistemas híbridos evaluados permitirían a los Estados miembros ejercer niveles de control variables sobre las búsquedas que lleven a cabo tanto ellos mismos como el órgano centralizado de la UE.

La ampliación del ámbito de aplicación de un sistema equivalente de la UE a fin de cubrir las cámaras de compensación automatizadas, el dinero electrónico y otros datos no financieros aportaría beneficios en términos de inteligencia, pues aumentaría la capacidad de la UE para rastrear los pagos interiores de la UE y podría crear un sistema más previsor que el exclusivamente dedicado a los mensajes sobre transacciones financieras. No obstante, cada proveedor designado adicional aumentaría el riesgo de infracción de los derechos de protección de datos y requería por tanto un conjunto rígido de condiciones, garantías y medidas de control. También agravaría la carga administrativa de los proveedores designados. La introducción de diversos proveedores de datos y mensajes para crear un sistema tan complejo y exigente desde los puntos de vista organizativo y técnico dispararía además los costes.

Este análisis indica que, para ser viable, un TFTS de la UE debería utilizar únicamente datos de mensajes financieros, pues la Comisión considera que los beneficios suplementarios de utilizar múltiples tipos de datos y proveedores no compensan sus importantes costes para las empresas privadas ni el menoscabo de la privacidad y los derechos de protección de los datos que semejante sistema entrañaría. Por consiguiente, habida cuenta de que el sistema de la UE cubriría únicamente el mismo proveedor designado y tipo de mensaje que el TFTP, la calidad y la cantidad de pistas de inteligencia y el nivel de exposición de los datos serían comparables a los del TFTP UE-EE.UU.

Como ya se ha indicado anteriormente, hay tres opciones para este sistema equivalente de la UE: A) el Servicio de coordinación y análisis TFTS de la UE, B) el Servicio de extracción TFTS de la UE y C) El Servicio de coordinación de la UIF.

La Opción A tendría probablemente repercusiones positivas para la prevención del terrorismo y el aumento de la seguridad en la UE. La realización de búsquedas y el análisis de los resultados por equipos tanto de la UE como de los Estados miembros contribuiría en cierta medida a asegurar que se tienen plenamente en cuenta los requisitos específicos de inteligencia de la UE y los Estados miembros y que el sistema enfoca la amenaza específica para la UE. No obstante, esta mejora está supeditada a la creciente disposición y capacidad de los Estados miembros para compartir la información y los análisis en un plazo entre medio y largo. No es seguro que puede confiarse en que se produzca este aumento del flujo de información. Además, habida cuenta de que los Estados miembros conservarían la capacidad

de solicitar búsquedas a los EE.UU. con arreglo al TFTP, este sistema requeriría un importante grado de asimilación y cooperación por parte de los Estados miembros para reflejar un panorama de la UE más coherente.

La opción B podría tener efectos positivos en la prevención del terrorismo y el aumento de la seguridad en la UE. El sistema respondería con mayor eficacia a los análisis de amenazas de la UE, dado que las búsquedas se llevarían a cabo conforme a los requisitos específicos de inteligencia de los Estados miembros. No obstante, el papel del órgano centralizado de la UE se limitaría a la realización de búsquedas y a la transferencia de los datos de respuesta al Estado miembro solicitante; su papel se ceñiría casi exclusivamente al de control del acceso. En consecuencia, no se realizarían análisis al nivel de la UE y, para obtener un panorama coherente de la situación de la inteligencia en la UE, el sistema debería apoyarse en la puesta en común de los análisis de los Estados miembros, al margen del sistema. La incapacidad del sistema para garantizar un planteamiento uniforme de las definiciones de las búsquedas aumentaría el riesgo de falsos resultados positivos, con la consiguiente vulneración de los derechos de protección de datos y privacidad.

La opción C respondería a las necesidades específicas de inteligencia de los Estados miembros y, por lo tanto, tendría cierto impacto positivo para la prevención del terrorismo y el aumento de la seguridad. No obstante, dado que las UIF serían responsables de las búsquedas y análisis de sus Estados miembros, esta opción adolece de los mismos inconvenientes que la opción B: sólo podría obtenerse un panorama claro mediante el refuerzo de la cooperación entre Estados miembros al margen del sistema. Además, las UIF se centran exclusivamente en la inteligencia financiera, y la brecha entre esta información y el panorama de inteligencia en sentido más amplio podría dificultar la percepción de los nexos entre distintos elementos y la detección de la financiación del terrorismo. Esta opción supone además una escasa participación de la UE y un aumento de la capacidad que se limita por lo esencial al nivel nacional.

Todas estas opciones entrañarían importantes costes para la UE, los Estados miembros y el proveedor designado, incluidos los derivados, entre otros conceptos, del desarrollo de la infraestructura de TI, la seguridad de las instalaciones y las decenas, por no decir centenas, de empleados responsables de la administración del sistema y de la aplicación de las garantías y los controles. No obstante, cada uno de estos sistemas posibles encierra cierto potencial de

contribuir a la mejora de la situación de la seguridad en Europa al partir de análisis de las amenazas específicos para las necesidades europeas.

Una herramienta independiente de inteligencia e investigación en el territorio europeo eliminaría la necesidad de transferir datos a los EE.UU. Pero cualquier TFTS de la UE seguiría requiriendo amplias garantías de protección de datos y controles similares a los ya vigentes con arreglo al Acuerdo TFTP UE-EE.UU. y, en cualquier caso, conformes con el acervo en materia de protección de datos de la UE y de los Estados miembros. Toda solicitud de búsqueda en los datos almacenados en sistemas de la UE debería ser objeto de un control de conformidad con el objetivo estricto y limitado de luchar contra el terrorismo y su financiación, incluida la justificación de la transferencia de datos. Concretamente, se necesitarían supervisores independientes cualificados que comprobasen que cada búsqueda de la UE y cada búsqueda de cada Estado miembro ha sido debidamente autorizada y es necesaria para la lucha contra el terrorismo y su financiación. Debería asegurarse el manejo y almacenamiento seguro de los datos e impedirse todo acceso no autorizado a los mismos. Será además necesaria una auditoría externa del adecuado funcionamiento del sistema y todas sus garantías. Deberían integrarse en el sistema todos los procedimientos necesarios para el acceso a los datos y la rectificación de los mismos, así como los procedimientos de recurso pertinentes.

En conclusión, en cumplimiento de la solicitud del Parlamento Europeo y el Consejo, la Comisión ha evaluado las posibles opciones de TFTS de la UE, incluido un régimen de extracción y retención.

Esa evaluación tiene en cuenta los principios recogidos en la Estrategia de gestión de la información adoptada bajo la Presidencia sueca. Todo sistema que se implante debe ser necesario, proporcional y rentable, además de respetar los derechos fundamentales. El análisis llevado a cabo por la Comisión, que se detalla en el presente documento y en la evaluación de impacto, muestra que cada una de las opciones viables presenta ventajas e inconvenientes. Como también se ha explicado, la Comisión ha descartado las opciones que no son viables.

A la luz de la información recogida, la conveniencia de presentar, en la fase actual, una propuesta de TFTS de la UE no ha quedado claramente demostrada.

La Comisión agradecería recibir las ideas del Parlamento Europeo y del Consejo sobre la presente Comunicación.