COMISIÓN EUROPEA

Bruselas, 13.7.2011
COM(2011) 429 final

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

Sistema europeo de seguimiento de la financiación del terrorismo: posibles opciones

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

Sistema europeo de seguimiento de la financiación del terrorismo: posibles opciones

1. INTRODUCCIÓN

Cuando el Consejo aprobó la celebración del Acuerdo entre la Unión Europea y los Estados Unidos de América 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 (Acuerdo TFTP UE-EE.UU.)[1], invitó asimismo a la Comisión a presentar al Parlamento Europeo y al Consejo, a más tardar un año después de la fecha de entrada en vigor del Acuerdo (1 de agosto de 2010), «un marco jurídico y técnico para la extracción de los datos sobre el territorio de la UE»[2]. El Parlamento Europeo ha venido insistiendo también en que se contemple una solución permanente y jurídicamente sólida al problema de la extracción de los datos solicitados en el territorio europeo[3]. La Comunicación *La Estrategia de Seguridad Interior de la UE en acción: cinco medidas para una Europa más segura* también establece que a partir de 2011 la Comisión desarrollará una política de extracción y análisis por parte de la UE de datos de mensajería que se encuentren en su propio territorio[4]. Dada la probada efectividad del TFTP estadounidense, un sistema europeo debería contribuir significativamente a los esfuerzos para evitar el acceso de los terroristas a financiación y a materiales, así como seguir las transacciones que realicen. Cabe referirse igualmente al artículo 11 del Acuerdo TFTP UE-EE.UU., el cual establece que durante su vigencia la Comisión Europea realizará un estudio sobre la posible introducción de un sistema equivalente de la UE que permita una transferencia más selectiva de los datos. La presente Comunicación representa la primera fase de la respuesta de la Comisión al mencionado artículo y a la invitación del Consejo. En ella se describen las diferentes medidas adoptadas por la Comisión para avanzar hacia la creación del citado «marco jurídico y técnico» y se presentan las distintas opciones planteadas para alcanzar esta meta. Aunque en esta fase no se señala una opción preferida, sí se indican los aspectos relevantes que deberán tenerse en cuenta en relación con las opciones consideradas. Dada la importancia política del asunto y su complejidad jurídica y técnica, la Comisión desea informar al Consejo y al Parlamento Europeo sobre el estado actual de la cuestión y poner en marcha un debate. La Comisión considera que sería conveniente este debate antes de presentar propuestas concretas basadas en una evaluación de impacto.

En este contexto, es preciso insistir en que la presente Comunicación no prejuzga la propuesta que la Comisión pueda presentar. Cualquier propuesta futura deberá tener presente el debate antes mencionado y la evaluación de impacto, que se basará en un estudio que la Comisión encargó en el segundo semestre de 2010. A la vista de los efectos sobre los derechos fundamentales, y en particular sobre la protección de datos, que podrían derivarse de esta propuesta legislativa, la evaluación de impacto deberá prestar una atención especial a la necesidad y proporcionalidad de cualquier medida

---

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, p. 3.

3 Véase, por ejemplo, la Resolución P7_TA(2010)0143 y la exposición de motivos de la Recomendación A7-0224/2010.

4 COM(2010) 673 final de 22.11.2010. Véase, acción 2 del objetivo 2, p. 8.

que la Comisión pudiera proponer. A tal efecto, la Comisión seguirá las directrices recogidas en su Comunicación sobre la Estrategia para la aplicación efectiva de la Carta de los Derechos Fundamentales por la Unión Europea[5].

Por otro lado, la evaluación de impacto permitirá obtener los conocimientos técnicos de referencia precisos, así como una valoración detallada de todas las opciones disponibles. Estos temas han sido ya objeto de diálogo con muchos interlocutores en este ámbito, entre ellos las instituciones de los Estados miembros, las autoridades de protección de datos, Europol y el proveedor designado. Las conclusiones finales del estudio no estarán disponibles antes de finales del presente año. Para contribuir a la preparación de la evaluación de impacto, la Comisión Europea ha organizado tres reuniones de expertos con los interlocutores mencionados, así como con los organismos de los Estados Unidos que tienen a su cargo la administración del TFTP. Las opciones examinadas en la presente Comunicación se basan en los resultados preliminares del estudio y en los debates mantenidos en estas reuniones de expertos.

2. OBJETIVOS DE LA INTRODUCCIÓN DE UN SISTEMA EUROPEO DE SEGUIMIENTO DE LA FINANCIACIÓN DEL TERRORISMO

Son dos los objetivos principales que justifican la introducción de un sistema europeo de seguimiento de la financiación del terrorismo (TFTS):

- El sistema debe representar una contribución eficaz a la lucha contra el terrorismo y su financiación dentro de la Unión Europea.

- Debe contribuir a reducir el volumen de datos personales transferidos a terceros países. Ha de permitir el tratamiento de los datos necesarios para su funcionamiento en el territorio europeo con arreglo a los principios y normas de la UE en materia de protección de datos.

En los Estados Unidos, el Programa de Seguimiento de la Financiación del Terrorismo (TFTP) ha demostrado que aporta un significativo valor añadido a la lucha contra el terrorismo y su financiación, beneficiando no solo a las autoridades de este país, sino también a las de los Estados miembros de la Unión Europea y a las de terceros países. Con ocasión de la reciente revisión del Acuerdo TFTP UE-EE.UU.[6] se confirmó que desde la introducción del TFTP en Estados Unidos se habían compartido con las autoridades de terceros países más de 2 500 informes, la inmensa mayoría de ellos (1 700) con la Unión Europea. La eficacia del programa estadounidense y su utilidad para luchar contra el terrorismo y su financiación ha sido confirmada igualmente por los dos informes presentados por el juez Bruguière, designado en 2008 por la Comisión Europea para examinar el programa. La información obtenida a través del TFTP que se comunicó a las autoridades de la UE incluía pistas importantes en relación con una serie de atentados (o intentos de atentados) terroristas de gran relieve, como los de Madrid y Londres, el complot de 2006 para derribar vuelos transatlánticos mediante explosivos líquidos, o el intento de atentado de 2007 contra intereses estadounidenses en Alemania. El equipo de examen de la UE concluyó que había recibido «indicaciones convincentes del valor añadido del TFTP para la lucha contra el terrorismo y su financiación». A la luz de estas experiencias, existen

[5] COM(2010) 573 final de 19.10.2010.
[6] SEC(2011) 438 final de 30.3.2011.

fuertes razones para creer que un TFTS europeo aportaría igualmente un importante valor añadido a los esfuerzos realizados por la UE y los Estados miembros para combatir el terrorismo y su financiación.

Mientras que está fuera de discusión la eficacia del TFTP estadounidense en la lucha contra el terrorismo y su financiación, se han planteado fuertes dudas en relación con sus efectos sobre los derechos fundamentales de los ciudadanos. Tales dudas giran principalmente en torno al hecho de que la ejecución del Acuerdo TFTP UE-EE.UU. conlleva la transmisión de grandes volúmenes de datos de carácter personal («datos masivos») a las autoridades estadounidenses, a pesar de que la inmensa mayoría de estos datos se refieren a ciudadanos que no tienen nada que ver con el terrorismo ni con su financiación. Esos datos se transmiten de forma masiva (en función de categorías de datos pertinentes) y no de forma individualizada (en respuesta a una petición relacionada con una o varias personas), debido a que el proveedor de los datos no tiene competencia técnica para segregarlos. Por otro lado, para que el proveedor pudiera proporcionar los datos de forma individualizada, tendría que establecer una función específica de búsqueda y análisis que sus procesos empresariales no exigen y que tendría consecuencias significativas en materia de recursos. Además, una solicitud individualizada de datos pondría en conocimiento del proveedor el nombre de las personas objeto de investigaciones relacionadas con el terrorismo y con sus ramificaciones financieras y podría afectar a la eficacia de tales investigaciones.

Para contrarrestar el suministro de datos masivos, se han establecido importantes medidas de protección destinadas a impedir su utilización indebida, entre ellas que los datos suministrados solo puedan ser analizados y utilizados para la lucha contra el terrorismo y su financiación. La reciente revisión del Acuerdo TFTP UE-EE.UU. ha permitido confirmar que estas medidas de protección se están aplicando efectivamente de conformidad con las disposiciones del Acuerdo.

No obstante, se ha objetado que la entrega a un tercer país de estos grandes volúmenes de datos personales constituye una vulneración injustificada de los derechos fundamentales de los ciudadanos afectados, teniendo en cuenta los principios de necesidad y proporcionalidad. Este es el motivo por el que el Consejo invitó a la Comisión a presentar propuestas para la creación de un sistema «para la extracción de los datos sobre el territorio de la UE», con la finalidad principal de garantizar que su tratamiento se realice de acuerdo con la legislación y los principios europeos de protección de datos y respetando la Carta de los Derechos Fundamentales de la UE. En este contexto conviene señalar que la recogida y tratamiento de datos financieros por las autoridades públicas afecta al derecho a la protección de los datos de carácter personal, consagrado en el artículo 16 del TFUE y en el artículo 8 de la Carta.

En virtud del artículo 52, apartado 1, de ésta, solo se podrán introducir limitaciones a estos derechos fundamentales si así se establece por la ley, con la necesaria precisión y calidad que permitan una previsibilidad y respetando el contenido esencial de dichos derechos. Solo se podrán introducir limitaciones, respetando el principio de proporcionalidad, cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión. Por lo tanto, deben tenerse en cuenta estos principios no solo al decidir si se debe adoptar o no un TFTS europeo, sino también en relación con las diversas alternativas disponibles de aplicación de dicho sistema. En consecuencia, estos principios afectan por igual a cualquier decisión que sea preciso adoptar sobre cuestiones tales como el alcance del sistema, los plazos de conservación de los datos, los derechos de las personas en relación con el acceso y eliminación, etc. Se trata de cuestiones que aunque no se tratan detalladamente en la presente Comunicación, serán objeto de un análisis exhaustivo en la evaluación de impacto.

Como es lógico, la posible introducción de un sistema para la extracción de los datos sobre el territorio de la UE tendrá consecuencias para el Acuerdo UE-EE.UU. existente, como se reconoce en su artículo 11, apartado 3, que especifica que, dado que el establecimiento de un sistema europeo podría modificar sustancialmente el contexto del Acuerdo, en el caso de que la Unión Europea decida establecer dicho sistema las partes deberán consultarse para determinar si es necesario adaptarlo en consecuencia. Por lo tanto, cualquiera de las opciones afectará también a la futura aplicación y posible adaptación del actual Acuerdo TFTP UE-EE.UU.

3. FUNCIONES PRINCIPALES DE UN SISTEMA EUROPEO DE SEGUIMIENTO DE LA FINANCIACIÓN DEL TERRORISMO

Una de los primeros elementos planteados en las conversaciones con los interlocutores antes mencionados es que todos ellos opinan mayoritariamente que, si se introduce un sistema europeo de seguimiento de la financiación del terrorismo (TFTS europeo), su finalidad debería consistir en ofrecer seguridad a los ciudadanos de la UE. El sistema no debería utilizarse exclusivamente para facilitar la información correspondiente a las autoridades estadounidenses, porque también los Estados miembros están verdaderamente interesados en sus resultados. Este planteamiento implica asimismo que, aun cuando el TFTP estadounidense podría servir de inspiración para la organización del sistema, su equivalente europeo no tiene por qué reproducir necesariamente todos sus aspectos. Asimismo, al establecer un sistema europeo es preciso tener presente las peculiaridades del marco legislativo y administrativo de la UE, al igual que el respeto de los derechos fundamentales aplicables a los que se ha aludido antes.

En todo caso, cualquier sistema destinado a rastrear la financiación del terrorismo que se ajuste a los objetivos antes descritos deberá contemplar la inclusión de las siguientes funciones principales:

- elaborar y emitir solicitudes (jurídicamente válidas) dirigidas al(a los) proveedor(es) de servicios de mensajería financiera designado(s), para la entrega de datos primarios al destinatario o destinatarios autorizados. Esto implica definir las categorías de mensajes que se solicitan y la frecuencia con que se deben enviar, y mantener contactos con los proveedores sobre estos temas;

- controlar y autorizar las solicitudes de datos primarios al(a los) proveedor(es) designado(s). Esto implica comprobar si tales solicitudes han sido elaboradas respetando las restricciones aplicables;

- recibir y almacenar (tratar) los datos primarios entregados por el(los) proveedor(es) designado(s). Esto implica establecer un sistema apropiado de seguridad física y electrónica de los datos;

- tramitar las búsquedas reales de los datos facilitados, en consonancia con el marco jurídico aplicable, basadas en las solicitudes de búsqueda de las autoridades de los Estados miembros, de los Estados Unidos o de terceros países sobre la base de condiciones y salvaguardias claramente establecidas, o por propia iniciativa del organismo (u organismos) responsables del tratamiento de los datos;

- vigilar y autorizar la realización de búsquedas de los datos suministrados;

- analizar los resultados de las búsquedas, combinando tales resultados con otras informaciones o datos de inteligencia disponibles;

- distribuir los resultados de las búsquedas (sin análisis ulterior) o los resultados de los análisis a los destinatarios autorizados;

- implantar un régimen adecuado de protección de datos que incluya los plazos de conservación aplicables, las obligaciones de registro, la gestión de las solicitudes de acceso, rectificación y eliminación, etc.

Estas funciones principales deberán reflejarse en los instrumentos jurídicos apropiados y tener validez a nivel de la UE, a nivel nacional o a ambos niveles, dependiendo de la opción elegida.

4. PRINCIPIOS CLAVE PARA EL EXAMEN DE LAS OPCIONES DISPONIBLES

Además de las anteriores consideraciones relativas a las funciones principales, la elección entre las alternativas disponibles dependerá en gran medida de una serie de aspectos fundamentales, que se analizarán en la evaluación de impacto y que se comentan a continuación.

4.1. Eficacia

Uno de los factores clave de las diferentes opciones es su eficacia para el cumplimiento del objetivo esencial de combatir el terrorismo y su financiación. Desde esta perspectiva, las opciones que permitan mejorar la comunicación y análisis de los datos a nivel internacional deberán ser las preferidas, ya que con ello se mejora su eficacia y se obtiene un mayor valor añadido. En particular, la elección de la organización u organizaciones que se encargarán del análisis de los datos y de facilitar los resultados del análisis a las autoridades apropiadas, tendrá un impacto significativo en la eficacia general del sistema, así como en el volumen de datos que serán transferidos. En cualquier caso, tal como se viene practicando actualmente, los Estados miembros seguirán teniendo pleno control sobre si deben o no comunicar la información o datos de inteligencia en su poder a otras autoridades.

4.2. Protección de datos

La comunicación y análisis a nivel internacional de la información y datos de inteligencia solo puede llevarse a cabo en un marco de protección de datos sólido y bien organizado. La eficacia de este marco no dependerá solamente de las disposiciones legislativas en vigor, que permiten a los afectados ejercer derechos tales como el de presentar recursos judiciales, sino también de la disponibilidad de personal experimentando, como por ejemplo responsables de protección de datos independientes, y de una autoridad de control en materia de protección de datos competente. Algunas de las organizaciones que podrían participar en la eventual introducción de un TFTS europeo ya han implantado este tipo de estructura, mientras que otras deberán hacerlo aún. Por lo tanto, habrá que examinar cuidadosamente las implicaciones de cada una de las distintas opciones a la luz de los principios generales relativos al respeto de los derechos fundamentales, a los que se hace referencia en la sección 2 de la presente Comunicación.

4.3. Seguridad de los datos

Las medidas estrictas en el ámbito de la protección de datos deberán combinarse con unas infraestructuras y tecnologías de vanguardia en lo relativo a su seguridad. Las consideraciones de seguridad de los datos abogan por limitar el número de lugares en los que se realiza el tratamiento de los datos suministrados y por restringir el acceso a ellos desde el exterior. La opción más segura consistiría en almacenarlos en un único lugar sin ningún tipo de acceso exterior. La mayor parte de las

organizaciones que podrían participar en la gestión del TFTS ya disponen de tecnologías seguras para el tratamiento de los datos, pero no todas tienen actualmente la capacidad necesaria para manejar los datos clasificados en un nivel superior al de «Restringido UE».

4.4. Almacenamiento de datos

El almacenamiento de datos puede efectuarse a nivel nacional o de la UE. En este último nivel, el almacenamiento de los datos recibidos del(de los) proveedor(es) designado(s) podría confiarse a Europol o a otro organismo de la UE, como por ejemplo la Agencia para la Gestión Operativa de los Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (Agencia TI)[7], que se encuentra en proceso de constitución. Dado que el almacenamiento de datos está ligado inextricablemente a los problemas relativos a su protección y seguridad, la elección de la organización responsable del mismo guarda una estrecha relación con el régimen adoptado por dicha organización en lo relativo a la protección y seguridad de los datos.

4.5. Utilización de las estructuras y medios existentes

Todas las opciones deberán hacer uso en la mayor medida posible de las estructuras ya existentes. De este modo se reducirán los costes y se podrán aprovechar las experiencias adquiridas y las infraestructuras ya establecidas. Esta utilización de los medios existentes exige que las nuevas tareas asignadas a una organización preexistente sean compatibles con las funciones que tiene atribuidas esta última. Por ejemplo, Europol, Eurojust o las autoridades judiciales nacionales pueden considerar desempeñar la función de verificación y autorización de las solicitudes de suministro de datos a(a los) proveedor(es) designado(s).

4.6. Cooperación entre las autoridades responsables

Las opciones que se describen a continuación presentan diferentes grados de cooperación y de intercambio de información y de datos de inteligencia entre las autoridades nacionales, y entre éstas y las autoridades europeas. Cada Estado miembro ha establecido diferentes modalidades de colaboración de sus autoridades nacionales en la lucha contra el terrorismo, y cualquier medida adoptada a nivel europeo deberá respetar las limitaciones impuestas por el artículo 72 del TFUE en relación con las responsabilidades de los Estados miembros en cuanto al mantenimiento del orden público y la salvaguardia de la seguridad interior. Por consiguiente, cualquier variante del TFTS europeo deberá permitir un nivel de control importante por parte de los Estados miembros sobre la información y datos de inteligencia que están dispuestos a compartir en el marco de un sistema de este tipo. Esta cuestión ha sido abordada con diversos enfoques por una serie de organizaciones a las que se hace referencia más adelante, algunos de los cuales podrían ser de aplicación directa al sistema que se deberá establecer.

4.7. Primer examen general del posible impacto financiero de las distintas opciones

El coste total de la introducción de un TFTS europeo y su distribución entre la UE y los niveles nacionales dependerá, en gran medida, de la opción política elegida. En todo caso, incluirá los conceptos siguientes:

- costes relacionados con la transmisión y almacenamiento seguro de los datos recibidos del(de los) proveedor(es) designado(s);

---

[7] COM(2010) 93 final de 19.3.2010.

- costes relacionados con el desarrollo y mantenimiento de las aplicaciones informáticas necesarias para ejecutar las búsquedas y facilitar sus resultados;

- costes relacionados con la distribución de los resultados de las búsquedas a los destinatarios autorizados;

- costes correspondientes al personal que realiza las búsquedas y analiza y distribuye los resultados;

- costes correspondientes al personal responsable de las funciones de control y auditoría;

- costes correspondientes al personal responsable de la protección de datos y de los derechos de los ciudadanos.

Aunque en la presente fase no se dispone aún de previsiones de costes, los cálculos iniciales indican que los costes asociados a un planteamiento meramente europeo, con las distintas opciones híbridas que se describen posteriormente, se situarían en torno a los 33-47 millones de euros para la primera instalación, a los que habría que añadir 7-11 millones de euros anuales correspondientes a los gastos de funcionamiento. Las distintas opciones son las descritas más adelante, en la parte 6 de la presente Comunicación. La opción 3 sería la más costosa, ya que supone 43 millones de euros de coste de la primera instalación para la UE y 3,7 millones para los Estados miembros (en su conjunto), más 4,2 millones anuales de gastos de funcionamiento para la UE y 6,8 millones para los Estados miembros (en su conjunto). La opción 2 sería la más económica, con 33 millones de euros de coste de la primera instalación y 3,5 millones de gastos de funcionamiento a nivel de la UE, a los que habría que añadir 3,3 millones de gastos de funcionamiento para el conjunto de los Estados miembros. La opción 1 requeriría 40,5 millones de euros para la primera instalación y 4 millones anuales de gastos de funcionamiento a nivel de la UE, además de 5 millones de gastos de funcionamiento para el conjunto de los Estados miembros. Evidentemente, es posible reducir estos costes empleando al personal de las organizaciones actuales, y haciendo uso de las infraestructuras, equipos y aplicaciones informáticas ya existentes. Los costes de establecimiento y funcionamiento de un sistema exclusivamente nacional serían considerablemente mayores (390 millones de euros para la primera instalación y 37 millones anuales de gastos de funcionamiento), ya que todos los Estados miembros estarían obligados a instalar sistemas de tratamiento de datos de alta seguridad, y contratar al personal necesario para el manejo del sistema.

Estos importes son preliminares y tendrán que ser analizados y detallados más en profundidad a la luz de los resultados de la evaluación de impacto.

5. CUESTIONES A TENER EN CUENTA

Con independencia de la opción elegida para el establecimiento y funcionamiento de un TFTS europeo, es preciso tener en cuenta una serie de cuestiones relevantes relacionadas con el alcance de un posible sistema de esta índole, que se analizan a continuación.

5.1. ¿Únicamente el terrorismo y su financiación, o también otros temas?

El acceso a los datos de mensajería financiera no sirve exclusivamente para combatir el terrorismo y su financiación. Apenas cabe duda de que este acceso constituiría asimismo una valiosa herramienta para combatir otras modalidades de delincuencia grave, en particular la delincuencia organizada y el blanqueo de capitales. Sin embargo, en el contexto del Acuerdo UE-EE.UU., las consideraciones

relativas a la proporcionalidad han llevado a limitar escrupulosamente el uso de los datos a los fines de la lucha contra el terrorismo y su financiación. De las conversaciones preliminares que han tenido lugar hasta ahora se desprende que existe un amplio consenso en que tales consideraciones de proporcionalidad apuntan en la dirección de aplicar las mismas limitaciones al alcance de un sistema europeo equivalente, en consonancia con los principios de carácter general relativos al respeto de los derechos fundamentales que se abordan en la sección 2 de la presente Comunicación.

5.2. ¿Más de un proveedor?

El Acuerdo TFTP UE-EE.UU. está limitado actualmente a la solicitud de datos a un único proveedor de servicios de mensajería financiera internacional. Aunque se trata claramente del proveedor más importante a escala mundial de este tipo de servicios, hay otros proveedores que actúan en el mercado. Las consideraciones de eficiencia y de competencia equitativa para todos los actores del mercado aconsejan la creación de un sistema aplicable a todos los proveedores de servicios de mensajería financiera. En cualquier caso, al elegir entre las opciones disponibles se deberá tener en cuenta la carga de trabajo administrativo para las empresas que ofrecen servicios de mensajería financiera.

5.3. ¿Exclusivamente los servicios internacionales de mensajería, o también los nacionales?

El Acuerdo TFTP UE-EE.UU. actual se limita exclusivamente a solicitar datos de proveedores de servicios de mensajería financiera internacionales, es decir, de los servicios utilizados para llevar a cabo transacciones transfronterizas, incluidas las realizadas entre los Estados miembros, pero excluyendo los datos de mensajería financiera relativos a la zona única de pagos en euros (ZUPE). Un TFTS europeo debería contemplar asimismo si se deben incluir o no a los servicios de mensajería financiera que transmiten datos entre los Estados miembros o si debe ceñirse a los intercambios internacionales realizados por los servicios de mensajería financiera. Actualmente, los servicios de mensajería financiera de carácter meramente nacional (utilizados en el contexto de transacciones financieras nacionales) quedan fuera del alcance del Acuerdo TFTP UE-EE.UU. El acceso a estos servicios nacionales sería de interés a efectos de combatir el terrorismo y otras formas de delincuencia. Sin embargo, dejando a un lado la cuestión de si el acceso a estas transacciones meramente nacionales debe ser objeto de regulación a nivel europeo, las discusiones preliminares confirman la impresión de que un acceso de este tipo se considera desproporcionado, debiendo por tanto quedar excluido del alcance del sistema europeo.

5.4. ¿Qué tipos de datos de mensajería financiera deberían tratarse?

El sistema bancario internacional utiliza múltiples tipos de datos de mensajería financiera. En la actualidad, el Acuerdo TFTP UE-EE.UU. está limitado a datos de un tipo concreto. Sería interesante poder acceder a otros tipos de datos con el fin de luchar contra el terrorismo y su financiación, y posiblemente también contra otras formas de delincuencia. Sin embargo, también en este punto las consideraciones de proporcionalidad y respeto de los derechos fundamentales de los ciudadanos pesan a la hora de limitar el alcance de los tipos de mensajes controlados por el sistema. En la evaluación del impacto se incluirán nuevos detalles relacionados con este aspecto técnico.

6. OPCIONES PARA UN TFTS EUROPEO

Las opciones descritas a continuación están siendo objeto de examen por parte de la Comisión, en el marco de la evaluación de impacto actualmente en curso. No son necesariamente limitativas, y en

ningún caso prejuzgan la evaluación de impacto definitiva ni la decisión que la Comisión adoptará basándose en ella.

Una de las opciones que siempre se tienen en cuenta durante el proceso de elaboración de nuevas iniciativas y sus correspondientes evaluaciones de impacto es la del mantenimiento del *statu quo*, lo que en este caso significaría seguir aplicando el Acuerdo TFTP UE-EE.UU. y no presentar ninguna propuesta relativa a un TFTS europeo. Esta opción no sería congruente con la invitación formulada por el Consejo y el Parlamento a la Comisión para presentar «un marco jurídico y técnico para la extracción de los datos sobre el territorio de la UE», mencionada en la sección 1 de la presente Comunicación. Por otro lado, dicha opción tampoco contribuiría a reducir el volumen de datos personales transferidos a terceros países y no permitiría un tratamiento de los datos en el territorio europeo sujeto a los principios y leyes sobre protección de datos aplicados en la UE. Todas las demás opciones, analizadas a continuación con mayor detalle, presentan posibles vías alternativas para el establecimiento de un TFTS europeo.

En teoría, todas las funciones principales de este sistema, identificadas en la sección 3 de la presente Comunicación, podrían llevarse a cabo tanto a nivel europeo como nacional. Tales funciones podrían asignarse asimismo a una o a varias organizaciones en función de sus cometidos actuales, o bien podrían crearse nuevas organizaciones encargadas de su realización que, a su vez, podrían tener carácter europeo o nacional. Esto implica, también en teoría, que es posible un planteamiento exclusivamente europeo, en el que todas las funciones principales se asignarían a organizaciones a escala de la UE, y que es igualmente posible un planteamiento exclusivamente nacional, en el cual todas las funciones se llevarían a cabo dentro de cada Estado miembro. En general, conviene tener presente también que, en este caso concreto, las alternativas correspondientes al sistema centralizado, descentralizado o híbrido no coinciden necesariamente con las de otras iniciativas que incluyen algún tratamiento de los datos y que tienen como objeto perseguir el terrorismo y la delincuencia organizada, por lo que cada iniciativa en este ámbito deberá ser juzgada en función de sus propios méritos.

Tanto el planteamiento exclusivamente centralizado como el exclusivamente nacional presentan graves inconvenientes. Por ejemplo, el exclusivamente europeo adolecería ciertamente de su desvinculación con las organizaciones y operaciones policiales y de inteligencia de los Estados miembros, con la consiguiente merma de eficacia. Sin las contribuciones de los organismos nacionales responsables de estos temas, sería casi imposible definir con precisión las categorías de datos que se deben solicitar al(a los) proveedor(es) designado(s). La utilidad del sistema quedaría igualmente menoscabada si las consultas a la base de datos se efectuasen en función de los informes de inteligencia disponibles a nivel de la UE, porque en la fase actual de la integración europea solo se dispone de tales informes al nivel nacional. Asimismo, los Estados miembros probablemente no aceptarían un enfoque meramente europeo ya que no añadiría valor alguno a sus propios esfuerzos para combatir el terrorismo y su financiación. Durante el proceso de consulta, los Estados miembros señalaron también que esta opción sería difícil de encajar políticamente, por motivos de orden jurídico y operativo.

En el extremo opuesto, un planteamiento exclusivamente nacional traería consigo el riesgo de una implantación divergente en los distintos Estados miembros, y el probable incremento de las violaciones de la seguridad de los datos, como resultado de la necesidad de realizar 27 copias de los datos requeridos. Este tipo de planteamiento también supondría dificultades para la introducción de un marco armonizado de protección de datos y de una estrategia armonizada en relación con (el control de) otras restricciones necesarias, como por ejemplo la limitación a la lucha contra el terrorismo y su financiación. Además, en este planteamiento meramente nacional no queda claro cuál de los Estados miembros asumiría la responsabilidad de tramitar las solicitudes de búsqueda procedentes de terceros

países, y desaparecerían las ventajas adicionales derivadas del análisis de los resultados de las búsquedas a nivel europeo. Por otro lado, como se ha indicado antes, los costes correspondientes a esta opción serían notablemente más elevados, dado que todos los Estados miembros tendrían que instalar sistemas de tratamiento de datos de alta seguridad y contratar personal para gestionarlos.

Así pues, durante los trabajos preparatorios realizados junto con los interlocutores enseguida se puso de manifiesto que las alternativas situadas en ambos extremos de la gama de posibles opciones carecían de apoyos, surgiendo un consenso en torno a que una solución híbrida, en la que las diferentes funciones se repartiesen entre varias organizaciones a nivel europeo y nacional, posiblemente ofrecería los mejores resultados en relación con los dos objetivos principales. Si bien este consenso contribuye a identificar la opción más adecuada, dentro de un planteamiento híbrido caben aún numerosas variantes. En los apartados posteriores se describen algo más extensamente las tres opciones híbridas que se han revelado como las más plausibles en los trabajos preparatorios actualmente en curso, y en el Anexo se presentan nuevamente en forma de tabla.

6.1. Un TFTS europeo como servicio de coordinación y análisis (opción 1)

Esta opción implicaría la creación de una unidad central del TFTS europeo, que llevaría a cabo la mayor parte de las tareas y funciones al nivel de la UE. A este nivel europeo se emitirían las solicitudes de datos primarios a(a los) proveedor(es) designado(s), se tramitarían y ejecutarían las solicitudes de búsquedas, se analizarían los resultados y se entregarían a los solicitantes los informes correspondientes. Sin embargo, la preparación de las solicitudes a(a los) proveedor(es) designado(s) se realizaría mediante consultas con las autoridades competentes de los Estados miembros, y éstos podrían optar también por destacar a sus propios analistas a la unidad central, al objeto de colaborar en la tramitación de las búsquedas. A diferencia de la opción exclusivamente centralizada, los Estados miembros podrían solicitar la realización de búsquedas para sus propios fines, de forma similar al procedimiento seguido actualmente con el TFTP estadounidense, o bien realizarlas con sus propios analistas.

Los Estados miembros tendrían que compartir información con la unidad central del TFTS europeo, con el fin de «validar» la solicitud y su nexo con el terrorismo antes de ejecutar la búsqueda, o bien obtener una «autorización previa» de las autoridades nacionales. Estas últimas podrían ser, por ejemplo, los fiscales o jueces de instrucción encargados de perseguir el terrorismo, cuya autorización para realizar una búsqueda determinada entre los datos suministrados permitiría a la unidad central del TFTS llevarla a cabo sin verificaciones ulteriores. En este escenario no sería preciso facilitar nuevos informes de inteligencia a la unidad central del TFTS europeo. Esta unidad central distribuiría los resultados de las búsquedas y sus análisis, pero también podría suministrar información por propia iniciativa. Los Estados Unidos y otros terceros países deberían solicitar igualmente la realización de búsquedas mediante un procedimiento similar.

La vigilancia del cumplimiento a través de medidas de protección y control también estaría centralizada, y posiblemente requeriría la supervisión de las entidades interesadas externas, por ejemplo de representantes del(de los) proveedor(es) designado(s) o de organismos designados como supervisores independientes. La protección, integridad y seguridad de los datos serían asimismo tareas realizadas a nivel central.

Las principales agencias implicadas en el sistema podrían ser Europol y Eurojust. En tal caso, las tareas asignadas a Europol y Eurojust deberían ser compatibles con las funciones encomendadas a estas agencias por el Tratado de Funcionamiento de la Unión Europea (TFUE). También convendría

determinar hasta qué punto sería necesario modificar las normas legales que rigen actualmente su funcionamiento. Si fuera elegida Europol como unidad central del TFTS europeo, debería atender asimismo las solicitudes de los interesados relativas al acceso, rectificación y bloqueo, todo ello de acuerdo con su marco jurídico vigente y con las normas en materia de protección de datos. La unidad central del TFTS europeo llevaría a cabo su cometido observando la legislación en vigor, y las reclamaciones y recursos se tramitarían igualmente de conformidad con las disposiciones legales aplicables. A nivel nacional, los organismos policiales nacionales se encargarían de verificar y autorizar las solicitudes de búsqueda. También cabe contemplar la posibilidad de crear nuevos organismos nacionales, pero esta alternativa debe dejarse al arbitrio de los Estados miembros, con arreglo al principio de subsidiariedad[8].

6.2. Un TFTS europeo como servicio de extracción de datos (opción 2)

Al igual que la primera de las opciones políticas, esta alternativa implicaría la creación de una unidad central del TFTS europeo, cuyas tareas abarcarían la emisión de solicitudes de datos primarios al(a los) proveedor(es) designado(s), su verificación, la realización de las búsquedas y la tramitación de las solicitudes de búsqueda. Sin embargo, en esta opción el TFTS europeo no tendría facultades para analizar los resultados de las búsquedas, comparándolos con otras informaciones o datos de inteligencia disponibles, cuando tales búsquedas se hicieran a petición de las autoridades de los Estados miembros, en cuyo caso su función quedaría limitada a la preparación y distribución de los resultados en la forma más apropiada.

Lo mismo que en la opción 1, las solicitudes de datos primarios dirigidas al(a los) proveedor(es) designado(s) se elaborarían en colaboración con los Estados miembros, los cuales comunicarían sus necesidades específicas a la unidad central del TFTS para que esta procediera a analizarlas y a formular las solicitudes sobre la base de dicho análisis.

Las autoridades de los Estados miembros podrían solicitar la realización de búsquedas para sus propios fines. La comprobación de la justificación de estas solicitudes y de su nexo con el terrorismo tendría lugar en el nivel nacional. La unidad central del TFTS europeo efectuaría la búsqueda y entregaría el conjunto completo de resultados, en un formato apto para su presentación, al Estado miembro. Las autoridades de los Estados miembros serían las únicas facultadas para realizar el análisis de los resultados, pudiendo optar igualmente por facilitar la información de manera espontánea.

La unidad central del TFTS europeo se encargaría de realizar las búsquedas y de analizar los resultados en nombre de las instituciones de la UE, de los Estados Unidos o de otros terceros países. También podría optar por facilitar, por propia iniciativa, información basada en dichos resultados.

Del mismo modo que en la opción precedente, la vigilancia del cumplimiento con medidas de salvaguardia y controles también estaría centralizada, y posiblemente supondría la supervisión por entidades interesadas externas, por ejemplo representantes del(de los) proveedor(es) designado(s) o de organismos designados como supervisores independientes. La protección, integridad y seguridad de los datos serían asimismo tareas realizadas a nivel central.

Al igual que antes, los principales organismos implicados en este sistema podrían ser Europol y Eurojust. En cuanto al nivel nacional, se requeriría la colaboración de los organismos policiales o servicios de

[8] En el estadio actual, las consecuencias para el presupuesto de las agencias de la UE que podrían desempeñar un papel en la puesta en marcha del sistema todavía se desconocen.

inteligencia de cada país. De forma similar, la creación de nuevos organismos nacionales dependería de los Estados miembros, en aplicación del principio de subsidiariedad. Europol o los organismos nacionales tramitarían las solicitudes de acceso, rectificación o eliminación formuladas por los ciudadanos de la UE, con participación de las autoridades competentes en materia de protección de datos y de la Autoridad Común de Control que supervisa las actividades de Europol. Las reclamaciones y recursos se tramitarían de acuerdo con las disposiciones legales aplicables a nivel nacional o de la UE[9].

6.3. Un servicio de coordinación de las Unidades de Inteligencia Financiera (UIF) (opción 3)

Esta opción política implicaría la creación de un organismo específico a nivel de la UE, basado en una plataforma UIF reforzada, formada por las unidades UIF de los Estados miembros. Dicho organismo específico a escala europea emitiría las solicitudes de datos primarios a(a los) proveedor(es) designado(s), condensando las necesidades indicadas por las UIF en una única solicitud, que sería igualmente verificada y autorizada a nivel central.

Cada UIF se responsabilizaría de organizar las búsquedas y de gestionar los resultados obtenidos en representación del Estado miembro correspondiente, y también de efectuar los análisis y de distribuir los informes que considerase relevantes. La comprobación de la justificación de estas solicitudes y de su nexo con el terrorismo tendría lugar en el nivel nacional o europeo. Las UIF podrían asimismo suministrar información por propia iniciativa.

La plataforma UIF reforzada estaría en condiciones de realizar las búsquedas y de analizar sus resultados en nombre de las instituciones europeas y de terceros países con los que la UE hubiera suscrito los acuerdos oportunos, aunque también podría suministrar informaciones de manera espontánea.

La vigilancia del cumplimiento a través de medidas de protección y controles estaría centralizada, requiriéndose probablemente la supervisión de entidades interesadas externas, por ejemplo de representantes del(de los) proveedor(es) designado(s), o de organismos designados como supervisores independientes. La protección, integridad y seguridad de los datos serían asimismo tareas realizadas a nivel central.

La plataforma UIF reforzada debería contar con un estatuto jurídico formal, con funciones y responsabilidades claramente definidas. En cuanto al nivel nacional, se requeriría la colaboración de los organismos policiales o servicios de inteligencia de cada país.

Cualquier organismo europeo podría atender las solicitudes de los ciudadanos de la UE relativas al acceso, rectificación y eliminación, y las reclamaciones y recursos se tramitarían de acuerdo con las disposiciones legales aplicables a nivel nacional o de la UE.

7. CONCLUSIÓN

Basada en los trabajos preparatorios realizados por la Comisión hasta la fecha, y sujeta a los resultados de la evaluación de impacto, la presente Comunicación describe las diversas opciones posibles para el establecimiento de «un marco jurídico y técnico para la extracción de los datos sobre el territorio de la UE», en el contexto de un sistema de seguimiento de la financiación del terrorismo. Las diferentes

[9] Véase la nota 8.

opciones analizadas en la presente Comunicación ponen de relieve la necesidad de elegir entre ellas y de adoptar decisiones relevantes para el respeto de los derechos fundamentales, siendo preciso abordar múltiples cuestiones de tipo jurídico, técnico, organizativo y financiero de forma mucho más pormenorizada durante las tareas preparatorias aún pendientes. Teniendo en cuenta estos importantes retos, la Comisión considera que se requiere un período de tiempo suficiente para llevar a cabo los ulteriores trabajos preparatorios y el debate con el Consejo y el Parlamento.

*** * ***

Anexo: Tabla de opciones híbridas

	TFTS europeo como servicio de coordinación y análisis (opción 1)	TFTS europeo como servicio de extracción de datos (opción 2)	Servicio de coordinación de las Unidades de Inteligencia Financiera (UIF) (opción 3)
Elaboración y emisión de solicitudes de datos primarios	Unidad central del TFTS europeo en coordinación con los Estados miembros	Unidad central del TFTS europeo en coordinación con los Estados miembros	Plataforma UIF reforzada
Control y autorización de las solicitudes de datos primarios	Eurojust u otro organismo existente	Eurojust u otro organismo existente	Eurojust u otro organismo existente
Recepción y almacenamiento de los datos primarios, seguridad de los datos	Europol u otro organismo de la UE, como la Agencia TI	Europol u otro organismo de la UE, como la Agencia TI	Europol u otro organismo de la UE, como la Agencia TI
Realización de búsquedas de datos primarios	Unidad central del TFTS europeo, analistas destacados por los Estados miembros o una combinación de ambos	Unidad central del TFTS europeo	UIF nacionales, plataforma UIF reforzada
Control y autorización de la realización de las búsquedas	Supervisores independientes, posiblemente las autoridades nacionales	Supervisores independientes, autoridades nacionales	Supervisores independientes
Análisis de los resultados de las búsquedas	Unidad central del TFTS europeo, analistas destacados por los Estados miembros o una combinación de ambos	Autoridades nacionales para búsquedas nacionales, analistas de la unidad central del TFTS europeo para búsquedas de la UE y de terceros países	Plataforma UIF reforzada, UIF nacionales

Distribución de los resultados de las búsquedas	Analistas de Europol o destacados por los Estados miembros	Autoridades nacionales para búsquedas nacionales, analistas de la unidad central del TFTS europeo para búsquedas de la UE y de terceros países	Plataforma UIF reforzada, UIF nacionales
Implantación de un régimen apropiado de protección de datos	Europol u otro organismo de la UE, como la Agencia TI	Europol u otro organismo de la UE, como la Agencia TI	Europol u otro organismo de la UE, como la Agencia TI