

# Estudio del tratamiento y transferencia de datos de mensajería financiera entre la Unión Europea y Estados Unidos a los efectos de la lucha contra la financiación del terrorismo

Covadonga Mallada Fernández  
Universidad de Valladolid

---

Fecha de presentación: marzo de 2020

Fecha de aceptación: junio de 2020

Fecha de publicación: marzo de 2021

## Resumen

En este artículo analizaremos el intercambio de información entre la Unión Europea y Estados Unidos para luchar contra la financiación del terrorismo dentro del acuerdo TFTP: «Acuerdo entre la Unión Europea y los Estados Unidos de América relativo al tratamiento y la transferencia de datos de mensajería financiera de la UE a los Estados Unidos a efectos del Programa de seguimiento de la financiación del terrorismo». Así pues, en primer lugar, haremos una pequeña introducción de la situación actual de la lucha contra la financiación del terrorismo en Europa. En segundo lugar, analizaremos los acuerdos de intercambio de información entre Europa y Estados Unidos. En tercer lugar, nos detendremos en el proyecto en ciernes del sistema europeo de seguimiento de la financiación del terrorismo (TFTS), y, ya, por último, en las conclusiones, intentaremos efectuar un análisis crítico de la situación actual y cómo creemos que se desarrollará este intercambio de información dentro del marco del TFTP y del TFTS en un futuro próximo.

## Palabras clave

financiación del terrorismo, intercambio de información, sistema europeo de seguimiento de la financiación del terrorismo, SWIFT

## *Study on the processing and transfer of financial messaging data between the European Union and the United States for the purposes of the fight against the financing of terrorism*

### **Abstract**

*In this article there will be an analysis of the exchange of information between the European Union and the United States in order to fight against the financing of terrorism within the TFTP agreement: "Agreement between the European Union and the United States of America relating to the processing and transfer of financial messaging data from the European Union to the United States for the purposes of the Terrorist Financing Tracking Programme." As such, firstly, there will be a short introduction on the current situation in the fight against the funding of terrorism in Europe. Secondly, we will analyse the agreements on the exchange of information between Europe and the United States. Thirdly, we will study the incipient project that is the European Terrorist Finance Tracking System (TFTS), and lastly, in the conclusion we will attempt to carry out a critical analysis of the current situation and how we believe this exchange of information will be developed within the framework of the TFTP and the TFTS in the near future.*

### **Keywords**

*financing of terrorism, exchange of information, European Terrorist Financing Tracking System, SWIFT*

## 1. Introducción

Antes de comenzar con el estudio del tratamiento y transferencia de datos de mensajería entre la Unión Europea y Estados Unidos a los efectos de la lucha contra la financiación del terrorismo (TFTP), vamos a analizar la situación actual de la lucha contra el terrorismo y su financiación en Europa. Así pues, la vigente Estrategia de la Unión Europea de lucha contra el terrorismo se centra en cuatro pilares: «prevenir, proteger, perseguir y responder». Además, estos cuatro pilares siempre se apoyan en el intercambio de información con terceros países y organismos internacionales.

### a) Primer pilar: prevenir

En este primer pilar, la UE se ha centrado en la legislación preventiva para evitar la radicalización. Desde este pilar, se ha elaborado la Estrategia de la Unión Europea para luchar contra la radicalización y la captación de terroristas en 2008, que fue revisada en junio de 2014 con objeto de incluir medidas de lucha contra los lobos solitarios, los combatientes extranjeros terroristas y el uso de redes sociales por parte de los terroristas.

### b) Segundo pilar: proteger

Dentro de este bloque se refuerza la seguridad en las fronteras exteriores, se mejora la seguridad de los transportes, se protegen los objetivos estratégicos y, por último, se reduce la vulnerabilidad de las infraestructuras críticas. Todo ello en aras de proteger a la ciudadanía y las infraestructuras y reducir la vulnerabilidad ante los atentados. Así pues, para dar respuesta a este segundo bloque, se dictó en abril de 2016 la Directiva (UE) 2016/681, que reglamenta la utilización de los datos del registro de nombres de los pasajeros (PNR).

### c) Tercer pilar: perseguir

Este pilar se centra en la persecución de las organizaciones terroristas a fin de desmantelarlas y enjuiciarlas. Al respecto, la UE ha centrado sus esfuerzos en las siguientes líneas de actuación:

- reforzar las capacidades nacionales;
- mejorar la cooperación y el intercambio de información entre las autoridades policiales y judiciales;
- combatir la financiación del terrorismo; y
- privar a los terroristas de sus medios de apoyo y comunicación.

En este marco se ha desarrollado, por un lado, la normativa preventiva de lucha contra la financiación del terrorismo, es decir, la Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo de 30 de mayo de 2018 por la que se modifica la Directiva (UE) 2015/849, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y las Directivas 2009/138/CE y 2013/36/UE, y, por otro, la normativa punitiva con la tipificación penal de los delitos de terrorismo a través de la Directiva relativa a la lucha contra el terrorismo. Esta directiva introduce la tipificación penal del adiestramiento o el viaje con fines terroristas; la organización o facilitación de este tipo de movimientos; la aportación o recaudación de fondos en relación con grupos o actividades terroristas; y, por último, la financiación del terrorismo.

### d) Cuarto pilar: responder

En este pilar, la estrategia se centra en desarrollar y gestionar planes para poder reducir las posibles consecuencias de un ataque terrorista. Estos planes incluirían los siguientes puntos<sup>1</sup>:

- la elaboración de dispositivos de coordinación de la UE en caso de crisis;
- la revisión del mecanismo de protección civil;
- la elaboración de instrumentos de evaluación de riesgos; y
- la puesta en común de buenas prácticas en la asistencia a las víctimas del terrorismo.

1. Así pues, podemos destacar entre las prioridades de los últimos años de la Estrategia de lucha contra el terrorismo las siguientes: «definir los mecanismos de aplicación de la cláusula de solidaridad por la UE, mediante una Decisión del Consejo adoptada en junio de 2014; revisar los dispositivos de coordinación de la UE en caso de emergencias y crisis, sustituidos en junio de 2013 por el Dispositivo Integrado de Respuesta Política de la UE a las Crisis (DIRPC); y revisar la legislación de la UE en materia de protección civil a finales de 2013».

Por otro lado, dentro de esta estrategia se encuentra el Reglamento para reforzar los controles en las fronteras exteriores, adoptado por el Consejo el 7 de marzo de 2017, mediante el cual se modifica el Código de fronteras Schengen. Con este reglamento se obliga a los Estados miembros a llevar a cabo comprobaciones sistemáticas de todas las personas que crucen las fronteras exteriores mediante la consulta de las correspondientes bases de datos<sup>2</sup>.

Por último, también en relación con esta estrategia se ha creado en enero de 2016 el Centro Europeo de Lucha contra el Terrorismo (ECTC/CELT). Enmarcado dentro de la Europol, en dicho organismo se desarrollan varios proyectos, entre ellos el que nos ocupa en este trabajo: el proyecto TFTP. Además, el ECTC trabaja en estrecha colaboración con otros centros operativos de Europol, como el Centro Europeo de Delitos Cibernéticos (EC3) o el Centro Europeo de Tráfico Ilícito de Migrantes (EMSC).

A través del CELT, los Estados miembros pueden intercambiar información y cooperar en asuntos relacionados con los combatientes terroristas extranjeros, el tráfico de armas de fuego ilegales y la financiación del terrorismo.

## 2. El intercambio de información entre los Estados para luchar contra la financiación del terrorismo

La lucha preventiva contra la financiación del terrorismo se lleva a cabo en la mayor parte de los Estados en legislaciones compartidas con la lucha contra el blanqueo de capitales<sup>3</sup>.

Algunos autores<sup>4</sup> críticos con las normativas de lucha contra la financiación del terrorismo consideran que un terrorista -con un presupuesto limitado y una mochila llena de explosivos- puede cometer un ataque terrorista y el rastreo de la fuente de financiación para cometerlo es casi imposible. No obstante, a pesar de que la mayoría de los últimos ataques terroristas han sido cometidos por lobos solitarios<sup>5</sup>, todavía nos encontramos con grupos terroristas organizados cuyas redes, aunque tengan células independientes entre sí, van más allá del país de origen del terrorista y tienen una gran fuente de financiación<sup>6</sup>. Por ende, aquí es donde cobra lógica la lucha conjunta contra la financiación del terrorismo y la cooperación de los Gobiernos para erradicar este tipo de delincuencia. A través de la cooperación internacional, los países pueden poner en práctica una de las herramientas más eficaces para luchar contra el terrorismo: eliminar y confiscar los fondos de los que disponen estos grupos criminales, ya que las organizaciones terroristas necesitan financiación para poder seguir reclutando y formando en su escuela del terror a nuevos miembros. Tal y como expone Richard<sup>7</sup>, dado que el terrorismo es una amenaza actual global, la respuesta al mismo debe ser también global; no cabe una respuesta individual de Europa, de Estados Unidos, o de los países afectados por el azote del terrorismo en particular: a este peligro que a todos nos concierne debe responderse mediante una lucha en *networking* de los países implicados y las organizaciones internacionales tales como GAFI, IMF u OSCE, entre otras.

Por ello, creemos que uno de los instrumentos más efectivos a la hora de luchar contra la financiación del terrorismo es la firma de acuerdos de intercambio de información entre países y actores internacionales<sup>8</sup>. Pero no solo es necesario que se firmen estos acuerdos; también lo es que el intercambio de información sea efectivo y eficaz, ya que mediante este intercambio se podrá rastrear los movimientos del dinero del

2. Véase también la Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza.
3. Para profundizar en la relación entre blanqueo de capitales y financiación del terrorismo véase Mallada Fernández (2015).
4. Véase Buesa Blanco (2016) y Mallada Fernández (2018, págs. 239-263).
5. Recordemos los ataques en Barcelona o en Londres en 2017, por ejemplo.
6. Si echamos la vista atrás, podemos observar que algunos ataques terroristas apenas necesitaron presupuesto para perpetrarse (París 1995: 680 francos; Bali 2002: 20.000 dólares), si bien hubo otros -como el 11S- que costaron entre 400.000 y 500.000 dólares llevarse a cabo. Véase: [http://www.9-11commi-ssion.gov/staff\\_statements/911\\_Terrfin\\_Monograph.pdf](http://www.9-11commi-ssion.gov/staff_statements/911_Terrfin_Monograph.pdf) [Fecha de consulta: 2 de septiembre de 2020].
7. Richard (2006, págs. 9-10).
8. Palicio (2010, págs. 5 y sigs.).

grupo terrorista, y, una vez cortada su fuente de financiación, debilitar a la organización terrorista, ya que sin presupuesto económico no pueden llevar a cabo los ataques.

Es cierto que, al no existir un concepto universal de terrorismo y financiación del terrorismo, es necesario intentar crear unos mínimos estándares internacionales de obligado cumplimiento para los Estados con objeto de homogeneizar la lucha contra el terrorismo y su financiación y que, de este modo, el intercambio de información entre los Estados y los organismos internacionales sea eficaz. De este modo, tanto la UE como Naciones Unidas han trabajado en las últimas décadas sin descanso para crear unos estándares internacionales mínimos que sean de obligado cumplimiento para los Estados. Entre estos estándares, destacaremos los siguientes<sup>9</sup>:

- Convenio Internacional para la Represión de la Financiación del Terrorismo (1999).
- Resolución 1373 (2001) del Consejo de Seguridad. De acuerdo con esta resolución se crea el Comité contra el Terrorismo de las Naciones Unidas, y, además, los Estados deben sancionar la financiación del terrorismo y la ayuda en actividades terroristas en unos listados.
- Convenio Europeo para la Represión del Terrorismo de 1977 (modificado en 2003).
- Convenio del Consejo de Europa sobre la Prevención del Terrorismo (2005).
- Convenio relativo al blanqueo, seguimiento, embargo y comiso de los productos del delito y a la financiación del terrorismo, firmado en Varsovia el 16 de mayo de 2005.
- Decisión marco del Consejo, de 13 de junio de 2002, sobre la lucha contra el terrorismo.

- Directiva 2005/60/CE del Parlamento Europeo y del Consejo, de 26 de octubre de 2005, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo.
- Las nueve recomendaciones especiales del GAFI (Grupo de Acción Financiera Internacional) sobre la financiación del terrorismo.

En general, podemos destacar que, para homogeneizar la lucha contra el terrorismo internacional y su financiación, casi todos los instrumentos internacionales actuales establecen la necesidad de una regulación autónoma del delito de financiación del terrorismo del delito de terrorismo<sup>10</sup>. Además, las medidas preventivas para luchar contra la financiación del terrorismo son prácticamente las mismas que las medidas establecidas para luchar contra el blanqueo de capitales: conozca a su cliente, conservación de los documentos de cinco a diez años (dependiendo de la legislación del país), etc.<sup>11</sup>, ya que los cauces de movimiento del dinero son prácticamente los mismos<sup>12</sup>.

### 3. La lucha transnacional contra la financiación del terrorismo: relación entre Estados Unidos y Europa

Hacer frente a las organizaciones terroristas globales necesita estrategias y respuestas globales que van más allá de un Estado. Por ello, las redes transnacionales de lucha contra el terrorismo y su financiación no deben estar formadas solo por los países; también la sociedad civil y las instituciones financieras y el sector privado deben estar comprometidos en esta lucha, involucrarse y colaborar ac-

9. Ertl, B. (2004). «Der Kampf gegen Geldwäscherei und Terrorismusfinanzierung». *Working Paper 4/2004*. Viena: Bundesministerium für Finanzen [en línea] <https://www.yumpu.com/de/document/view/5535509/der-kampf-gegen-geldwascherei-und-terrorismusfinanzierung> [Fecha de consulta: 3 de septiembre de 2020].

10. Cuestión que se ha trasladado a los ordenamientos jurídicos nacionales: como el español, donde se ha tipificado el delito de financiación del terrorismo como delito autónomo del delito de terrorismo.

11. Para profundizar sobre este tema véase Mallada Fernández (2015).

12. De todos modos, los mecanismos de investigación para la lucha contra la financiación del terrorismo son muy diferentes de los mecanismos de lucha contra la prevención del blanqueo de capitales. Al respecto, véase Mallada Fernández (2018).

tivamente proporcionando información a las autoridades y facilitando la posible congelación de los activos.

La solución a la lucha contra la financiación del terrorismo no está en una organización, legislación o Estado sino en la cooperación de todos ellos, es decir, en una lucha conjunta de Estados, organizaciones internacionales como GAFI, Naciones Unidas, Europol o Interpol y organizaciones no gubernamentales como el Comité de Supervisión Bancaria de Basilea<sup>13</sup>.

No obstante, esta lucha conjunta se puede tornar complicada por las distintas políticas de lucha contra la financiación del terrorismo de los distintos países. Así, por ejemplo, Estados Unidos trata siempre de luchar contra el terrorismo de manera *bilateral*, es decir, aunque participe en organizaciones como la OTAN, sus esfuerzos de cooperación transatlántica siempre se centran en establecer convenios bilaterales con otros países. En cambio, Europa intenta luchar contra el terrorismo y su financiación con mecanismos multilaterales, a través de las directivas que se transponen en los distintos ordenamientos jurídicos de los Estados miembros. Así pues, para superar este escollo de las distintas maneras de enfrentarse al terrorismo por parte de Estados Unidos y de Europa, debemos llamar la atención acerca de que Estados Unidos intenta aumentar su cooperación con Europa a través del cumplimiento de la Recomendación 3 de GAFI de financiación del terrorismo sobre congelación de activos o la Resolución 1373 de Naciones Unidas<sup>14</sup>. Sin embargo, hay problemas en esta cooperación entre Europa y Estados Unidos que aún están pendientes de resolver: entre otros, la congelación de activos y los fondos económicos de las organizaciones benéficas. Así pues, por ejemplo, en cuanto a la congelación de activos, esta cooperación se torna complicada, ya que las listas de terroristas que manejan Estados Unidos y Europa no coinciden, lo cual dificulta el intercambio de información y la congelación de activos de esos terroristas.

### 3.1. El caso de Estados Unidos: Acuerdo entre la Unión Europea y los Estados Unidos de América relativo al tratamiento y 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

Dentro de los acuerdos de intercambio de información para luchar contra el terrorismo y su financiación podemos destacar el Acuerdo entre la Unión Europea y los Estados Unidos de América relativo al tratamiento y transferencia de datos de mensajería financiera de la UE a los Estados Unidos, a efectos del Programa de Seguimiento de la Financiación del Terrorismo<sup>15</sup>. Este programa es conocido como el Acuerdo SWIFT, PSFT o, por sus siglas en inglés, TFTP, gracias al cual Estados Unidos y la UE pueden intercambiar los datos obtenidos en la plataforma SWIFT a efectos de la lucha contra la financiación del terrorismo. Esto permite a las autoridades acceder a información sobre envío de datos de mensajería financiera entre instituciones bancarias a través de la red SWIFT.

SWIFT es una plataforma de intercambio de información privada y segura entre entidades financieras para efectuar intercambios de información financiera entre ellas. La Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT, Society for Worldwide Interbank Financial Telecommunication) es una cooperativa propiedad de sus miembros a través de la cual el sector financiero lleva a cabo buena parte de sus operaciones comerciales. SWIFT nació en Bélgica en 1973 y tiene oficinas en los principales centros financieros del mundo.

Cada banco que forma parte de esta plataforma tiene un código internacional ISO 9632 que le identifica en el sistema. El código SWIFT de un banco está formado por el código del país, el código del banco y una serie de datos adicionales, como la localización o el tipo

13. Morris (2002).

14. Resolución 1373 de Naciones Unidas: «Internationally, we are focusing our efforts on achieving greater European cooperation and support for our terrorist financing designations. We are capitalizing on our progress in improving and clarifying international standards for freezing terrorist-related assets under FATF Special Recommendation III by: (i) pursuing bilateral and multilateral efforts to reform the EU Clearinghouse process, and (ii) encouraging national implementation of UN member state obligations under United Nations' Security Council Resolution 1373».

15. [https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:22010A0113\(01\)&from=EN](https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:22010A0113(01)&from=EN). [Fecha de consulta: 2 de septiembre de 2020].

de sucursal<sup>16</sup>. El sistema SWIFT solo transmite información, que incluye datos personales del remitente y del destinatario de la transferencia, pero nunca se mueve dinero ni se almacena la información de manera permanente ya que los mensajes permanecen en los centros operativos durante 124 días<sup>17</sup>. Durante este período, los mensajes son guardados en los dos centros de computación de SWIFT y después son borrados de todas sus bases de datos. La plataforma es usada por más de once mil organizaciones bancarias y de valores y está presente en más de doscientos países.

Hasta finales de 2009, SWIFT disponía de dos plataformas: una en Europa (Bélgica) y otra en Estados Unidos. Por motivos de seguridad, todos los mensajes procesados por SWIFT se almacenaban en ambos centros mediante un sistema de almacenaje «en espejo»<sup>18</sup>: Estados Unidos podía acceder a la información de operaciones realizadas en Europa y viceversa. Pero, después de toda la controversia internacional que causó el hecho de que Estados Unidos tuviera acceso a esa información sin implementar ningún requerimiento a la UE<sup>19</sup>, para evitar dicha polémica, a partir del 1 de enero de 2010 SWIFT cambió todo su sistema de procedimiento y creó una nueva plataforma en Estados Unidos para que los datos de las transacciones realizadas en Europa y en Estados Unidos estuvieran separadas<sup>20</sup>. De este modo, por un lado, se encuentra una plataforma situada en Estados Unidos para las operaciones efectuadas en Estados Unidos y, por otro lado, otra plataforma situada en Europa para las operaciones llevadas a cabo en Europa. Además, se sigue conservando la plataforma original situada en Bélgica, donde se guardan las operaciones realizadas en ambos continentes como respaldo o *back-up* para posibles fallos de los sistemas de las otras dos plataformas. Así pues, a partir del 1 de enero de 2010 Estados Unidos dejó de tener acceso a toda la información almacenada en las plataformas SWIFT y planteó la posibilidad de firmar un acuerdo con la UE para garantizar el intercambio

de información de todas las plataformas SWIFT siempre y cuando esa información solo se usara para la lucha contra la financiación del terrorismo.

Como se puede observar, todos los movimientos financieros quedan grabados en estas plataformas; por ello, tener acceso a las mismas, es un gran avance para la lucha contra la financiación del terrorismo ya que, de este modo, los Gobiernos pueden seguir, detectar y, en su caso, congelar los movimientos relacionados con la financiación de los grupos terroristas, siempre que la congelación de esos activos no ponga en alerta a los terroristas. Debemos recalcar en este punto que si bien la congelación de activos se puede realizar preventivamente en el caso de que las autoridades tengan pruebas fehacientes de que se va a cometer de manera inminente un ataque terrorista, lo más normal es que la congelación se efectúe a *posteriori*, con una orden judicial, ya que cualquier movimiento extraño por parte de la entidad financiera podría levantar sospechas por parte de los terroristas.

Pero ¿cómo es posible que Estados Unidos tuviera acceso a información sensible sobre operaciones realizadas en Europa? Pues bien, como ya hemos mencionado varias veces en este trabajo, los ataques del 11S supusieron un antes y un después en el desarrollo de la legislación para luchar contra la financiación del terrorismo. Así pues, luego de estos ataques, Estados Unidos aprobó el Programa de Seguimiento de la Financiación del Terrorismo (Terrorism Finance Tracking Program, TFTP). Dentro de este programa, el Departamento del Tesoro de Estados Unidos (US Treasury, UST) cursó requerimiento administrativo al centro operativo de SWIFT en Estados Unidos solicitando datos de transferencias bancarias dentro y fuera de Estados Unidos que pudieran estar relacionados con el terrorismo. Como SWIFT tenía información sobre operaciones efectuadas en Estados Unidos y en la UE, el Departamento del Tesoro de Estados Unidos tuvo acceso también a información de operaciones financieras llevadas

16. Palicio (2010); Cremona (2011); De Goede (2012); Santos Vara (2012, págs. 355-380).

17. Véase: <https://www.swift.com> [Fecha de consulta: 2 de septiembre de 2020].

18. Bosch Moliné (2014, pág. 160 y sigs).

19. Sobre la controversia suscitada por el acceso de Estados Unidos a los datos de transacciones realizadas dentro de Europa del sistema SWIFT, véase Monar (2010, págs. 143-151) y Pfisterer (2009, págs. 1173-1189).

20. Véase: «SWIFT: el Parlamento Europeo rechaza el acuerdo con Estados Unidos» [en línea] <http://www.europarl.europa.eu/sides/getDoc.do?language=es&type=IM-PRESS&reference=20100209IPR68674> [Fecha de consulta: 2 de septiembre de 2020].

a cabo dentro de Europa sin la autorización de las agencias nacionales de protección de datos europeas<sup>21</sup>. Esto derivó en varias investigaciones por parte de la agencia belga de protección de datos concluyendo en septiembre de 2006 que se había «sometido a vigilancia durante años a una cantidad masiva de datos personales de forma secreta y sistemática, sin justificación suficiente y clara y sin control independiente conforme al derecho belga y europeo»<sup>22</sup>. Como consecuencia de todo ello, y para evitar posteriores problemas con las autoridades europeas, SWIFT cambió su estructura, como ya hemos mencionado, a partir del 1 de enero de 2010, con lo cual Estados Unidos ya no tendría acceso a las operaciones realizadas en Europa. Por ello, el Gobierno estadounidense decidió intentar alcanzar un acuerdo con las autoridades europeas para poder hacer requerimientos sobre estos datos<sup>23</sup>, firmando así el Acuerdo entre la Unión Europea y los Estados Unidos de América relativo al tratamiento y la transferencia de datos de mensajería financiera de la UE a los Estados Unidos a efectos del Programa de seguimiento de la financiación del terrorismo<sup>24</sup>. El acuerdo entró en vigor el 1 de agosto de 2010 (publicado en el DOUE L 195, de 27 de julio de 2010, pág. 1)<sup>25</sup>. En este nuevo acuerdo se respetaban las exigencias del Parlamento Europeo, en concreto «la limi-

tación estricta del objetivo de las transferencias a la lucha contra el terrorismo, la exclusión de los datos del sistema europeo de pagos (SEPA), la prohibición de las transferencias en bloque, la limitación a cinco años del período de conservación de los datos, la posibilidad de denunciar el acuerdo en caso de incumplimiento de las normas de protección de datos y el derecho a la reparación administrativa y judicial»<sup>26</sup>.

Sin embargo, tras sendas comunicaciones en 2011 y 2013, la Comisión concluyó que la necesidad de establecer este sistema no está claramente demostrada y suspendió cautelarmente dicho acuerdo<sup>27</sup> debido al escándalo Snowden<sup>28</sup>. El Parlamento consideraba que debía hacerse una suspensión cautelar del acuerdo para investigar si la Agencia Nacional de Seguridad de Estados Unidos (NSA, National Security Agency) había tenido acceso directo a los datos proporcionados por SWIFT para usarlos en casos no relacionados directamente con la financiación del terrorismo, lo que supondría una violación de los términos del Programa de seguimiento de financiación del terrorismo.

A principios de 2014, el Informe Moraes sobre los diversos programas de vigilancia de la NSA, realizado por el euro-

21. Es decir, sin la autorización de los Estados miembros.

22. Dictamen 37/2006 del 27 de septiembre de 2006 de la Comisión Belga para la Protección de la Intimidad relativa a la transferencia de datos personales por parte de SWIFT por los requerimientos del UST (OFAC), pág. 27 [en línea] (en francés y en holandés). El nuevo acuerdo se firmó el 28 de junio de 2010 para un período de cinco años renovable.

23. No debemos olvidar que el Tratado de Lisboa entró en vigor el 1 de diciembre de 2009, y que una de las novedades que incluía era el requisito del consentimiento del Parlamento Europeo para la conclusión de acuerdos internacionales, por lo que el acceso del Departamento del Tesoro a los datos del SWIFT europeo debía pasar por la aprobación del Parlamento Europeo.

24. También conocido como Acuerdo SWIFT.

25. La premura en alcanzar un acuerdo fue debido a que, como ya hemos señalado, SWIFT almacena los datos durante 124 días, con lo cual, si Estados Unidos dejaba de tener acceso al sistema durante un período más largo, hubiera perdido la posibilidad de analizar los datos de ese período.

26. Este intercambio de información funciona en ambas direcciones, por lo que, del mismo modo, tanto Europa podrá proporcionar información a Estados Unidos como al contrario (artículo 1.1 del acuerdo). El procedimiento de dicho acuerdo funciona del siguiente modo. En primer lugar, el Departamento del Tesoro de Estados Unidos solicitará al proveedor designado que se encuentre en el territorio de Estados Unidos la puesta a disposición de los datos necesarios para «la prevención, investigación, detección o persecución del terrorismo o de la financiación del terrorismo que estén almacenados en el territorio de la Unión Europea» (artículo 4 del acuerdo). En la solicitud se ha de detallar claramente los motivos y los datos que se requieren quedando siempre al margen del acuerdo los datos sobre el espacio único de pagos en euros. De todos modos, aunque el acuerdo establezca limitaciones, no se van a evitar la transferencia masiva de datos personales a las autoridades estadounidenses ya que las transferencias no son individualizadas sino por categorías. En segundo lugar, el Departamento del Tesoro debe enviar a Europol una copia de la solicitud. Europol comprueba que la solicitud cumple los requisitos del acuerdo y acto seguido «el proveedor designado queda autorizado para facilitar y debe facilitar los datos al Departamento del Tesoro de Estados Unidos».

27. Communication from the Commission to the European Parliament and the Council on a European Terrorist Finance Tracking System (TFTP) (COM (2013) 842 final).

28. Véase: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0449+0+DOC+XML+VO//ES> [Fecha de consulta: 2 de agosto de 2020].



diputado Claude Moraes, reiteró la recomendación de la suspensión del acuerdo con Estados Unidos<sup>29</sup>. Sin embargo, una investigación efectuada por las autoridades belgas y holandesas de protección de datos no encontró ninguna prueba que apoyara las afirmaciones de que un tercero había adquirido ilegalmente el acceso a la base de datos de SWIFT<sup>30</sup>.

En 2015, Estados Unidos se negó a permitir el acceso del Parlamento Europeo a un documento sobre la implementación del programa SWIFT (TFTP) escrito por el propio comité interno de protección de datos de Europol, la Autoridad Común de Control. Las modalidades técnicas del acuerdo entre Estados Unidos y Europa requieren que Europol obtenga un permiso de las autoridades de Estados Unidos antes de divulgar cualquier registro relacionado con el programa. Las autoridades estadounidenses han rechazado el acceso público, argumentando que el documento contiene información clasificada de Estados Unidos y que el requisito de «need to know» (necesidad de saber) no se había cumplido. La Defensora del Pueblo de la UE, Emily O'Reilly, se opuso a esta decisión arguyendo que esta negativa le impedía realizar una supervisión democrática sólida del TFTP<sup>31</sup>.

El último informe de la Comisión, publicado el 19 de enero de 2017<sup>32</sup>, demuestra los beneficios importantes del TFTP para los esfuerzos internacionales de lucha contra el terrorismo.

De todos modos, a pesar de las críticas, el programa ha seguido en vigor hasta la actualidad, ya que, como es sabido, el Parlamento Europeo no tiene poder para suspender la aplicación de ningún acuerdo, lo cual compete al Consejo de la UE<sup>33</sup>.

El acuerdo salvaguarda los derechos de protección de datos relacionados con la transparencia, los derechos de acceso, la rectificación y el borrado de datos inexactos.

Además, garantiza que cualquier persona cuyos datos se procesen en virtud del acuerdo tendrá derecho a solicitar una reparación judicial en Estados Unidos por cualquier acción administrativa adversa.

Una parte importante del acuerdo se encuentra en que los datos del programa puedan ser transferidos a terceros. Sin embargo, esta transferencia queda supeditada a la autorización por parte de ambos Estados salvo causa de fuerza mayor relacionada con la financiación del terrorismo.

Europol evalúa si los datos solicitados en un caso determinado son necesarios para la lucha contra el terrorismo y su financiación verificando que cada solicitud use la menor cantidad de datos posibles solicitados. Además, todas las búsquedas realizadas dentro del marco del programa son supervisadas por supervisores independientes y en el caso de que haya dudas sobre el nexo terrorista pueden bloquear todas las búsquedas relacionadas con ese nexo en virtud del artículo 5 del acuerdo.

En resumen, creemos que este programa de seguimiento de la financiación del terrorismo entre Estados Unidos y Europa es uno de los instrumentos más importantes para luchar contra la financiación del terrorismo no solo porque propone una cooperación recíproca entre Estados Unidos y Europa para intercambiar información en ambos sentidos, sino también por permitir observar los movimientos del dinero de los grupos terroristas para que los cuerpos y fuerzas de seguridad puedan adelantarse a sus movimientos, cortando sus fuentes de financiación.

29. European Parliament (2014).

30. Belgian Privacy Commission (2014).

31. 31 European Ombudsman (2015): <https://www.ombudsman.europa.eu/en/speech/en/58851> [Fecha de consulta: 2 de septiembre de 2020]; y NIELSEN, N. (2015): <https://euobserver.com/justice/127142> [Fecha de consulta: 2 de septiembre de 2020].

32. Informe de la Comisión al Parlamento Europeo y al Consejo (2017): <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017DC0031&from=EN> [Fecha de consulta: 2 de septiembre de 2020].

33. El acuerdo debía estar en vigor durante cinco años, pero, aunque ya se ha pasado ese plazo, sigue vigente a la espera de la aprobación del nuevo pilar de protección de datos de la UE.

## 4. Sistema europeo de seguimiento de la financiación del terrorismo (TFTS)

En el ámbito europeo se está perfeccionando desde hace algunos años la posible creación de un sistema europeo de seguimiento de la financiación del terrorismo (TFTS) capaz de seguir las transacciones de los presuntos terroristas en la zona del euro paralelo al programa que actualmente existe con Estados Unidos según el cual se intentarían detectar las redes terroristas a través del rastreo de la cadena de financiación en Europa. Este programa aún no ha visto la luz, pero en este apartado haremos un pequeño resumen de cómo están actualmente las negociaciones al respecto.

En una comunicación del 27 de noviembre de 2013, la Comisión Europea concluyó que una propuesta para un TFTS propio de la UE no está claramente demostrada. Así pues, sorprendentemente, el resultado de esta evaluación de impacto fue el abandono de un TFTS de la UE. En su informe, la Comisión presentaba dudas sobre los impactos potenciales en términos de derechos fundamentales y sobre el coste del nuevo y más amplio<sup>34</sup> sistema propuesto<sup>35</sup>.

Sin embargo, este programa sería beneficioso para cubrir todas las transacciones que se realicen dentro de la zona SEPA pero que estén excluidas del acuerdo con Estados Unidos, por ejemplo los pagos dentro de la UE en euros. Además, el acuerdo con Estados Unidos no proporciona una herramienta para rastrear actividades de financiación del terrorismo dentro de los países SEPA<sup>36</sup>, ni entre ellos, en el caso de transacciones SEPA. Como consecuencia, resulta imposible detectar y obtener información relativa a los combatientes terroristas extranjeros y a sus socios dentro de los países SEPA; y,

a pesar de la integración de la Red de Unidades de Inteligencia Financiera (UIF) en Europol, esta laguna no se subsana, ya que el TFTP no forma parte de los métodos de trabajo de las UIF<sup>37</sup>.

Después de los recientes ataques acaecidos en Europa (París, Niza, Barcelona) la idea del TFTS europeo volvió a ponerse sobre la mesa<sup>38</sup> en aras de mejorar la lucha contra la financiación del terrorismo en territorio europeo. Así pues, la eurodiputada conservadora francesa Rachida Dati, durante una sesión de preguntas parlamentarias con la Comisión Europea el 28 de enero 2015<sup>39</sup>, expuso que había que retomar el programa de seguimiento de financiación de terrorismo europeo dado que las amenazas terroristas en Europa y en Estados Unidos a día de hoy son complemente opuestas. La mayor preocupación actual europea es la amenaza de los ciudadanos europeos retornados de Siria o Irak o de aquellos lobos solitarios inspirados por la ideología del Dáesh y dispuestos a perpetrar un ataque terrorista en territorio europeo. Así pues, el Plan de Acción de la UE establece que la Comisión Europea acuerda que se retomará la iniciativa para complementar el actual programa firmado con Estados Unidos adicionando las transacciones excluidas en dicho acuerdo<sup>40</sup>.

Por tanto, abogamos por la creación de un sistema europeo de seguimiento de la financiación del terrorismo (TFTS) capaz de seguir las transacciones de los presuntos terroristas en la zona del euro, además del Programa de Seguimiento de la Financiación del Terrorismo (TFTP) existente entre Estados Unidos y la UE.

Por último, dentro de Europol se encuentra el Centro Europeo de Lucha contra el Terrorismo (ECTC)<sup>41</sup>. Entre sus objetivos principales se encuentran, por un lado, aumentar el intercambio de información entre los Estados

34. European Commission (2013, pág. 37).

35. Así pues, la Comisaria de Asuntos de Interior, Cecilia Malmström, confirmó que la Comisión no tenía la intención de presentar una propuesta específica para un TFTS de la UE, ya que «no aportaría ninguna inteligencia adicional».

36. Aquellos que excluyen los datos de transacciones financieras relativos a la zona única de pagos en euros.

37. Maricaa (2017). La UIF española es el Servicio ejecutivo de prevención de blanqueo de capitales (SEPBLAC). Todas las UIF europeas comparten información a través de FIU.net.

38. De Goede y Wesseling (2017).

39. Dati (2015): [https://www.europarl.europa.eu/doceo/document/P-8-2015-001000\\_EN.pdf](https://www.europarl.europa.eu/doceo/document/P-8-2015-001000_EN.pdf) [Fecha de consulta: 2 de septiembre de 2020].

40. European Commission (2016, pág. 12).

41. Los proyectos que se llevan a cabo son AP Hydra, Travellers, Dolphin, TFTP y Check the Web.

miembros y Europol, y, por otro intensificar los rastreos de las actividades de financiación del terrorismo<sup>42</sup>.

## 5. Conclusiones

En primer lugar, podemos afirmar que los instrumentos para luchar contra la financiación del terrorismo más eficaces son aquellos que, en primer lugar, son preventivos, y que, en segundo lugar, abogan por el intercambio efectivo de información entre los Estados y las organizaciones internacionales, ya que el *modus operandi* del terrorismo ha cambiado en las últimas décadas para pasar a ser un terrorismo internacional. Por ello, la herramienta por excelencia para la prevención de la financiación del terrorismo es facilitar el intercambio de información entre Estados y organizaciones internacionales.

El terrorismo actual no es un problema nacional, sino internacional, que cruza las fronteras nacionales del país en cuestión. De ahí la necesidad de compartir información con otros países para una lucha exitosa en contra de la financiación del terrorismo.

Aunque en la actualidad ya existan bases de datos de terrorismo<sup>43</sup>, algunos autores apuntan la posibilidad de desarrollar bases de datos más específicas que puedan compartir Estados Unidos y Europa a fin de poder llevar a cabo esta medida preventiva<sup>44</sup>, lo cual creemos que es harto complicado ya que el principal problema que existe con el intercambio de información entre países es el relativo a aquella información que está considerada como inteligencia clasificada (*classified intelligence*)<sup>45</sup>. Así, por ejemplo, si Estados Unidos tiene evidencias de actividades terroristas será más fácil lograr la cooperación con países europeos; el problema es cuando no pueden compartir la información de origen de esas pruebas de terrorismo porque está considerada como clasificada. Sin esa información de origen, los países europeos serán más reacios a colaborar con Estados Unidos. De todos modos, la línea actual que se está llevando a cabo en Europa y en Naciones Unidas prevé una homogeneización cada vez más mayor de la normativa de lucha contra el terrorismo y su financiación con un concepto universal de terrorismo y de su financiación, lo cual ayudará a disminuir estas barreras entre países a fin de lograr un intercambio de información más rápido y eficaz.

42. Además de efectuar investigaciones más específicas contra el tráfico ilícito de armas de fuego con fines de actividades terroristas, así como investigaciones con objeto de detectar el material de propaganda extremista violenta en internet, funciones ideadas para tener un mayor impacto operativo contra las redes terroristas y los llamados combatientes extranjeros.

43. En cambio, Europol sí que tiene una amplia base de datos de terroristas. Así pues, los distintos Estados miembros de la UE pueden proporcionar información a la Europol según los distintos códigos de manejo. El primer código es el «H0» o «no-código», ya que si se selecciona significa que la información puede distribuirse a todos los Estados miembros sin ningún tipo de restricción. En segundo lugar, el código «H1» prohíbe compartir la información antes de que se termine el procedimiento judicial a no ser que exista una autorización previa por el Estado miembro que incorporó los datos. En tercer lugar, el código «H3» permite incorporar las restricciones que el Estado miembro crea convenientes, y por ello se puede añadir texto en una casilla en blanco (por ejemplo, que solo se pueda compartir la información con un determinado centro focal). Véase Blasi Casagran (2016, pág. 20).

44. Richard (2006, pág. 25 y ss.).

45. Los países pueden contribuir a proporcionar información a Europol, siendo los propios dueños de la misma a través de los códigos de manejo. Estos códigos de tratamiento constituyen un medio para proteger una fuente de información. Garantizan su seguridad, así como su tratamiento protegido y adecuado, de conformidad con los deseos del propietario de la información y con plena observancia de las normas jurídicas nacionales de los Estados miembros. Los códigos de tratamiento indican qué puede hacerse con una información determinada y quién dispone de acceso a ella en el futuro.

## Referencias bibliográficas

- BELGIAN PRIVACY COMMISSION (2014). Only available in Dutch or French at <https://www.privacycommission.be/fr/news/les-instances-chargees-de-controler-le-respect-de-la-vie-privee-ne-constatent-aucune-infraction> (en línea). [Fecha de consulta: 18 de marzo de 2020].
- BLASI CASAGRAN, C. (2016). «El Reglamento europeo de Europol: un nuevo marco jurídico para el intercambio de datos policiales en la UE». *Revista General de Derecho Europeo*, núm. 40.
- BOSCH MOLINÉ A. (2014). La dimensión exterior de EUROPOL desde el punto de vista de la protección de datos. En: PI LLORENS, M., ZAPATER DUQUE, E. (coord.). *El caso del acuerdo TFTP en La dimensión exterior de las agencias del espacio de libertad, seguridad y justicia* Barcelona: Marcial Pons.
- BUESA BLANCO, M. (2016). «Financiación del terrorismo». *Economía*, núm. 893.
- CREMONA, M. (2011). «Justice and home affairs in a globalised world: ambitions and reality in the tale of the EU-US SWIFT Agreement». *Institute for European integration Research (Working Paper No. 4/2011)*.
- DATI, R. (2015). «Parliamentary Questions» [en línea] [https://www.europarl.europa.eu/doceo/document/P-8-2015-001000\\_EN.pdf](https://www.europarl.europa.eu/doceo/document/P-8-2015-001000_EN.pdf) [Fecha de consulta: 2 de septiembre de 2020].
- DE GOEDE, M. (2012). «The SWIFT affair and the Global Politics of European Security». *Journal of Common Market Studies*, vol. 50, pág. 214.
- DE GOEDE, M.; WESSELING, M. (2017). «Secrecy and security intransatlantic terrorism finance tracking». *Journal of European Integration*, núm. 39, vol. 3, págs. 253-269.
- ERTL, B. (2004). «Der Kampf gegen Geldwäscherei und Terrorismusfinanzierung». *Working Paper 4/2004*. Viena: Bundesministerium für Finanzen [en línea] <https://www.yumpu.com/de/document/view/5535509/der-kampf-gegen-geldwascherei-und-terrorismusfinanzierung> [Fecha de consulta: 2 de septiembre de 2020].
- EUROPEAN COMMISSION (2013). *Commission Staff Working Document*.
- EUROPEAN COMMISSION (2016). «Communication from the Commission to the European Parliament and the Council on an Action Plan for Strengthening the Fight against Terrorist Financing», COM/2016/050 final.
- EUROPEAN PARLIAMENT (2014). «Report on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and their Impact on EU Citizens, Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs» en *Committee on Civil Liberties, Justice and Home Affairs*, 2013/2188(INI).
- EUROPEAN OMBUDSMAN (2015). «Presentation by the European Ombudsman, Emily O'Reilly- Decision of the European Ombudsman Closing the Inquiry into Complaint 1148/2013/TN as Regards Europol», 8 de enero de 2015 [en línea] <https://www.ombudsman.europa.eu/en/speech/en/58851> [Fecha de consulta: 2 de septiembre de 2020].
- INFORME DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO (2017). Sobre la revisión conjunta de la aplicación 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 [en línea] <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017DC0031&from=EN> [Fecha de consulta: 2 de septiembre de 2020].
- MALLADA FERNÁNDEZ, C. (coord.) (2015). *Guía práctica de prevención del blanqueo de capitales*. Madrid: Lex Nova.

- MALLADA FERNÁNDEZ, C. (2018). «La financiación del terrorismo desde la perspectiva de las nuevas tecnologías: a propósito de la quinta Directiva de la UE de prevención del blanqueo de capitales y la financiación del terrorismo». *Anuario de derecho penal y ciencias penales*, tomo 71, fasc. 1, págs. 239-263.
- MARICAA, A. (2017). «Medidas y cambios normativos en la UE para intensificar la lucha contra el terrorismo global». *Revista del IEEE*, núm. 10 [en línea] <http://revista.ieee.es/article/view/190/310> [Fecha de consulta: 2 de septiembre de 2020].
- MONAR, J. (2010). «The rejection of the EU-US SWIFT interim agreement by the European parliament: a historic vote and its implications». *European foreign affairs review*, vol. 15, núm. 2, págs. 143-151.
- MORRIS, S. (2002). «Following the money trail: where corruption meets terrorism». *TIQ: Transparency International's Quartely Newsletter*.
- NIELSEN, N. «US Gag Order on EU Police Agency Stirs Controversy», *EU Observer* [en línea] <https://euobserver.com/justice/127142> [Fecha de consulta: 2 de septiembre de 2020].
- PALICIO, I. (2010). «El intercambio internacional de información financiera y la lucha contra la financiación del terrorismo: el acuerdo UE-EEUU sobre SWIFT». *ARI 49/2010*.
- PFISTERER, V. (2009). «The second SWIFT Agreement between the European Union and the United States of America: an overview». *German Law Journal*, vol. 11, núm. 10, págs. 1.173-1.189 [en línea] <https://doi.org/10.1017/S2071832200020174> [Fecha de consulta: 2 de septiembre de 2020].
- RICHARD, A. (2006). *Fighting terrorism financing: transatlantic cooperation and international institutions*. Center for Transatlantic Relations.
- SANTOS VARA, J. (2012). «El Acuerdo SWIFT con Estados Unidos: génesis, alcance y consecuencias». En: MARTÍN Y PÉREZ DE NANCLARES, J. (coord.). *La dimensión exterior del espacio de libertad, seguridad y justicia de la Unión Europea*. Madrid: IUSTEL, págs. 355-380.

### Cita recomendada

MALLADA FERNÁNDEZ, Covadonga (2021). «Estudio del tratamiento y transferencia de datos de mensajería financiera entre la Unión Europea y Estados Unidos a los efectos de la lucha contra la financiación del terrorismo». *IDP. Revista de Derecho, Internet y Política*, núm. 32, págs. xx-xx. UOC [Fecha de consulta: dd/mm/aa] <https://dx.doi.org/10.7238/idp.v0i32.373741>



Los textos publicados en esta revista están –si no se indica lo contrario– bajo una licencia Reconocimiento-Sin obras derivadas 3.0 España de Creative Commons. Puede copiarlos, distribuirlos y comunicarlos públicamente siempre que cite su autor y la revista y la institución que los publica (*IDP. Revista de Internet, Derecho y Política*; UOC); no haga con ellos obras derivadas. La licencia completa se puede consultar en: <http://creativecommons.org/licenses/by-nd/3.0/es/deed.es>.

### Sobre la autora

Covadonga Mallada Fernández  
 covadonga.mallada@gmail.com  
 Universidad de Valladolid

Licenciada en Derecho (2006). Máster en Asesoría Fiscal por la Universidad Pontificia de Salamanca (premio al mejor expediente de la promoción 2008). Doctora por la Universidad de Oviedo (2012) y premio extraordinario de doctorado (2013). Premio jóvenes investigadores menores de treinta y cinco años del Max Planck Institute (2015) e investigadora en varios proyectos nacionales, entre ellos investigadora principal del proyecto DER2014-58257-R Ciberlaundry (2014-2017). Asimismo, fue investigadora posdoctoral en la Universidad Humboldt de Berlín bajo la dirección del profesor Heinrich durante el curso 2012-2013, profesora adjunta de la UDIMA entre 2013 y 2017 y profesora de tributación del CEF entre 2013 y 2017. Actualmente es profesora ayudante doctor de la Universidad de Valladolid.