

Riesgo de financiación del terrorismo: Vulnerabilidades de los canales de pago

Terrorist financing risk: Vulnerabilities in the payment systems

María Julia Martínez Martínez¹

¹ Analista de riesgos, España

mjulia.martinezmartinez@gmail.com

RESUMEN. Este artículo evalúa el riesgo de financiación del terrorismo en los canales de pago tradicionales. Combatir la financiación del terrorismo es uno de los principales frentes en la lucha contra la actual amenaza yihadista y una prioridad global. Las recomendaciones del ente intergubernamental independiente Grupo de Acción Financiera Internacional (GAFI) son reconocidas universalmente como el estándar en la lucha contra la financiación del terrorismo. La recomendación número 1 establece que los países deben identificar, evaluar y entender sus riesgos en materia de financiación de terrorismo, aplicando un Enfoque Basado en el Riesgo (EBR) que depende de tres factores: amenaza, vulnerabilidad y consecuencia. En este contexto, se estudia el funcionamiento de los canales de pago tradicionales, así como sus vulnerabilidades. Finalmente, se destaca la importancia de disponer de un sistema de pagos eficiente, para evitar la proliferación de las actividades informales y prevenir usos indebidos, como la financiación del terrorismo.

ABSTRACT. The aim of this article is to assess the terrorist financing risk through the traditional payment systems channels. Combating terrorist financing is on the front line against the current threat posed by the jihadi terrorism and a global priority. The inter-governmental body Financial Action Task Force (FATF) recommendations are recognized as the global counter-terrorist financing standard. Recommendation number 1 calls countries to identify, assess, and understand their terrorist financing risks, applying a Risk Based Approach (RBA) which depends on three factors: threat, vulnerability and consequence. Within this context, the way traditional payment systems channels operate is studied, so as their vulnerabilities. Finally, the importance of an efficient payment system is highlighted in order to avoid the proliferation of informal activities and to prevent misuses such as terrorist financing.

PALABRAS CLAVE: Financiación del terrorismo, GAFI, Riesgo, Vulnerabilidad, Sector bancario, Entidades de pago, Sistemas de transferencia informal de fondos, Hawala.

KEYWORDS: Terrorist financing, FATF, Risk, Vulnerability, Banking sector, Money value transfer systems, Alternative remittance systems, Hawala.

1. Introducción

Uno de los fenómenos que más preocupa a la comunidad internacional es la creciente amenaza de algunos grupos terroristas yihadistas. Las grandes organizaciones terroristas requieren un volumen considerable de fondos, dado que además de la propia subsistencia y seguridad de sus integrantes, precisan financiación para la adquisición de armas, entrenamiento de combatientes, captación de nuevos integrantes y difusión de su propaganda. Sin embargo, los pequeños grupos terroristas precisan una menor cantidad de fondos, y los que actúan en solitario aún menos. Combatir la financiación del terrorismo es uno de los principales frentes en la lucha contra la actual amenaza yihadista, e impedir su acceso a fuentes de financiación es una prioridad global.

En la lucha contra la financiación del terrorismo, el Grupo de Acción Financiera Internacional (GAFI¹) es el organismo de referencia mundial. Sus recomendaciones son reconocidas universalmente como el estándar en la lucha contra la financiación del terrorismo. En su Recomendación número 5 establece que se debe tipificar la financiación del terrorismo como delito y en la Recomendación número 1 que los países deben identificar, evaluar y entender sus riesgos en materia de financiación de terrorismo, aplicando un enfoque basado en el riesgo (EBR), a partir de la metodología de evaluación nacional del riesgo desarrollada por el Fondo Monetario Internacional (FMI). El modelo EBR consiste en evaluar el riesgo en función de tres factores: amenaza, vulnerabilidad y consecuencia. El objetivo es que cada país tome las medidas necesarias en proporción a sus riesgos nacionales.

En este contexto, las organizaciones que integran el sistema financiero, principalmente entidades, supervisores y mercados, deben cuantificar el riesgo específico de financiación del terrorismo, en función de sus circunstancias particulares, y así destinar los recursos necesarios a aquellos ámbitos cuyo nivel de riesgo se considere superior.

En la siguiente sección se conceptualizan los términos relacionados con el terrorismo, en el ámbito de las recomendaciones de GAFI. A continuación, se analiza la recomendación número 1, para identificar, evaluar y entender los riesgos en materia de financiación de terrorismo, aplicando el modelo EBR. Posteriormente, se describe el funcionamiento de los canales de pago tradicionales, y se valora el riesgo de financiación de terrorismo a través de los mismos.

2. Terrorismo y financiación del terrorismo

El terrorismo es un fenómeno de naturaleza peculiar y los sucesivos intentos de conceptualizar dicho término han sido objeto de gran controversia (Tofangsaz, 2015). Lo que para algunos es un atentado terrorista, para otros es un acto de insurgencia o una lucha por una reclamación territorial. Las principales dificultades para establecer una definición consensuada internacionalmente surgen cuando se intentan determinar los factores que caracterizan al terrorismo, tales como los tipos de conductas, las circunstancias y las motivaciones. Por otra parte, tampoco hay consenso en la delimitación de las víctimas del terrorismo, en concreto, si se debe limitar a las personas directamente afectadas por las acciones violentas, o si debería extenderse a las afectadas indirectamente, además de a instituciones, a estados o, incluso, a la humanidad en su conjunto.

En el glosario de términos de las recomendaciones de GAFI (Financial Action Task Force, 2012), se conceptualizan los siguientes términos relacionados con el terrorismo y su financiación:

- **Acto terrorista:** Es un acto que constituye un delito según lo establecido en los tratados internacionales² o que persigue causar muerte o daños graves a civiles o personas que no son parte activa en conflictos armados, cuando el propósito de dichos actos es intimidar a la población o interferir en la toma de decisiones de un gobierno u otra organización internacional.
- **Terrorista:** Persona natural que comete o intenta cometer actos terroristas, participa como cómplice, organiza o dirige a otros terroristas, o contribuye a la comisión de actos terroristas.
- **Organización terrorista:** Grupo de terroristas que cometen o intentan cometer actos terroristas,

¹ Financial Action Task Force (FATF). www.fatf-gafi.org

Martínez, M. J. (2016). Riesgo de financiación del terrorismo: Vulnerabilidades de los canales de pago. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 1(1), 66-78.

participan como cómplices, organizan o dirigen a otros terroristas, o contribuyen a la comisión de actos terroristas.

- Financiación del terrorismo: Financiación de terroristas, organizaciones terroristas o actos terroristas.

GAFI es un ente intergubernamental, nacido en 1989, que tiene el mandato de fijar estándares y promover la implementación de medidas para combatir el blanqueo de capitales, la financiación del terrorismo y la relativa a la proliferación de armas de destrucción masiva y otras amenazas. Ello conlleva, asimismo, la identificación de vulnerabilidades, con el fin de proteger al sistema financiero internacional de usos indebidos. En 1990 elaboró un esquema de medidas, denominado las Cuarenta Recomendaciones, que los países debían implementar para combatir el uso indebido del sistema financiero por parte de quienes pretendían blanquear las ganancias procedentes del tráfico ilícito de drogas. Posteriormente, en 1996, y dado el alcance de las nuevas y complejas técnicas de ingeniería financiera en el blanqueo de capitales, se revisaron dichas recomendaciones, ampliándose su ámbito de aplicación a otras actividades delictivas. Tras los atentados del 11S, en octubre de 2001, GAFI incorporó Ocho (posteriormente ampliadas a Nueve) Recomendaciones Especiales sobre Financiación de Terrorismo. Las Cuarenta Recomendaciones y las Nueve Especiales se refundieron en Cuarenta en el año 2012. Las revisiones y actualizaciones de las recomendaciones son el resultado de la cooperación de GAFI con diversos organismos regionales, además de la participación de otros organismos supranacionales observadores, tales como Naciones Unidas, Banco Mundial y Fondo Monetario Internacional. Actualmente las recomendaciones de GAFI son reconocidas universalmente como el estándar internacional de la lucha contra el blanqueo de capitales, la financiación del terrorismo y la proliferación de armas. Las recomendaciones han sido respaldadas por más de 180 países, que se han comprometido a implementarlas en sus correspondientes jurisdicciones nacionales, si bien adaptadas a sus propias peculiaridades.

GAFI establece en su Recomendación 5 que los países³ deben tipificar la financiación del terrorismo como delito tomando como referencia el artículo dos de la Convención Internacional para la Supresión de la Financiación del Terrorismo. El delito de financiación del terrorismo debe:

- comprender tanto la financiación de acciones terroristas, como la aportación de fondos a organizaciones o grupos terroristas y a terroristas individuales, aunque no haya una vinculación directa con actos terroristas específicos;
- extenderse a toda persona que suministre o recaude fondos deliberadamente, por medios directos o indirectos, tanto con la intención de financiar directamente actos terroristas, como para ser destinados a otros fines por parte de personas, organizaciones o grupos vinculados con el terrorismo;
- considerar que los fondos pueden provenir de fuentes legítimas o ilegítimas;
- ser calificado tanto el intento de cometer un delito de financiación del terrorismo, como la organización para que otros lo cometan y la participación como cómplice, además de cualquier acción que contribuya a la comisión del delito.

La lucha contra el terrorismo es ineficaz si se plantea individualizada y aisladamente en el marco de las distintas jurisdicciones nacionales. Es incompleta si se reduce a que las Fuerzas y Cuerpos de Seguridad, junto con los Servicios de Inteligencia, se ciñan a la mera detección de personas que ya están preparadas para pasar

² Los tratados internacionales son: Convenio para la Represión del Apoderamiento Ilícito de Aeronaves (1970), Convenio para la Represión de Actos Ilícitos contra la Seguridad de la Aviación Civil (1971), Convención sobre la Prevención y el Castigo de Delitos contra Personas Internacionalmente Protegidas, inclusive los Agentes Diplomáticos (1973), Convención Internacional contra la Toma de Rehenes (1979), Convenio sobre la Protección Física del Material Nuclear (1980), Protocolo sobre la Supresión de Actos de Violencia Ilegales en Aeropuertos que Sirven a la Aviación Civil Internacional, suplementario al Convenio para la Represión de Actos Ilícitos contra la Seguridad de la Aviación Civil (1988), Convenio para la Represión de Actos Ilícitos contra la Seguridad de la Navegación Marítima (2005), Protocolo para la Represión de Actos Ilícitos contra la Seguridad de las Plataformas Fijas ubicadas en la Plataforma Continental (2005), Convención Internacional para la Supresión de Ataques Terroristas (1997) Convenio Internacional para la Represión de la Financiación del Terrorismo (1999).

³ En España, el delito de financiación del terrorismo está tipificado en el artículo 576 del Código Penal.

a la acción de manera inminente. La amenaza del terrorismo constituye un desafío que afecta a la sociedad en su conjunto: instituciones públicas, sector privado y sociedad civil. En el ámbito de la seguridad y la defensa se ha evolucionado hacia un concepto de seguridad integral, como objetivo compartido por todos, que constituye la base⁴ para que la sociedad pueda desarrollarse, preservar su libertad y prosperidad, garantizando la estabilidad y buen funcionamiento de las instituciones. La lucha contra el terrorismo es un esfuerzo compartido por todos, es decir, un proceso incardinado en las estrategias nacionales, que consideran la seguridad como un bien público de interés prioritario.

Combatir el terrorismo precisa de la cooperación entre países. Es más efectiva cuando adquiere dimensión internacional. También precisa la implicación del sistema financiero, que incluye tanto a los supervisores como a las instituciones financieras y las Actividades y Profesiones No Financieras Designadas⁵ (APNFD), que establecen los mecanismos para detectar flujos monetarios vinculados con personas o actividades terroristas. Por consiguiente, la lucha contra el terrorismo es más eficaz cuando uno de los objetivos estratégicos es combatir su financiación, y el sistema financiero participa a nivel táctico, implementando medidas de prevención, y a nivel operativo, evitando que se canalicen flujos monetarios puntuales, que puedan llegar a financiar actos terroristas, o que sean utilizados por organizaciones o grupos terroristas, o terroristas individuales.

3. Modelo EBR para la evaluación del riesgo de financiación del terrorismo

El enfoque EBR (Financial Action Task Force, 2007) plantea un sistema de valoración del riesgo (Financial Action Task Force, 2013b) para los países, las instituciones financieras y las APNFD en función de unos elementos clave o riesgos genéricos identificados. Según dicho enfoque, el riesgo de financiación de terrorismo se determina en función de tres factores: amenaza, vulnerabilidad y consecuencias.

La amenaza es un objeto, actividad, persona o grupo con el potencial de causar daño. Según el Informe anual de Seguridad Nacional de 2014, la amenaza terrorista es un fenómeno internacional y polimorfo capaz de innovar creando nuevas formas y modos, y adaptarse a las medidas preventivas que toman los estados. En las nuevas organizaciones terroristas se han generalizado las acciones de martirio, que reducen el número de efectivos que precisan ser repuestos. Destinan muchos recursos a la propaganda, a la difusión de información, llegando en algunos casos a tener sus medios de comunicación propios. Utilizan, por otro lado, narrativas que consiguen aglutinar a decenas de miles de simpatizantes. Comenzaron difundiendo mensajes explícitos de llamada con base religiosa, que principalmente calaban en los segmentos más marginados de la sociedad. Pero están mutando, adaptándose rápidamente a una nueva realidad, en un estricto sentido darwiniano. Ya no se apela al ideal religioso, sino al héroe. El nuevo objetivo es el segmento de la población adolescente, aprovechando la situación de inestabilidad propia de la edad. La amenaza es un concepto que en las últimas décadas se ha reformulado en términos geopolíticos. Para determinar la amenaza hay que tener en cuenta una diversidad de actores que interaccionan conjuntamente: determinados estados, agentes no estatales, entre los que se encuentran grupos terroristas, organizaciones de delincuencia organizada, empresas privadas y la población civil. El ámbito de las amenazas actuales es transnacional, mientras que anteriormente se circunscribían a ubicaciones geográficas concretas. Si bien es difícil determinar la amenaza futura, lo que sí es cierto es que el terrorismo es un fenómeno que requiere un continuo seguimiento. Cuanto más se comprenda la amenaza terrorista, mejor se determinará su aportación al riesgo de financiación del terrorismo.

La vulnerabilidad comprende el conjunto de objetos, actividades, personas o grupos cuyas debilidades pueden ser explotadas por la amenaza para apoyar o facilitar sus actividades.

La consecuencia es el impacto o daño que puede causar una actividad terrorista sobre la población civil, el tejido empresarial, los intereses nacionales e internacionales, además de sobre el sistema financiero, su

⁴ Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

⁵ Las Actividades y Profesiones No Financieras Designadas son casinos, agentes inmobiliarios, comerciantes de metales y piedras preciosas, abogados, notarios, otros profesionales jurídicos independientes, proveedores de servicios societarios y fideicomisos.

reputación y la de sus instituciones. Las consecuencias de los actos terroristas se evalúan en términos compensatorios. La gravedad de los efectos destructivos en infraestructuras siniestradas se estima en función de sus costes de reconstrucción. En cuanto a los daños personales, se aplican criterios indemnizatorios, en función de los coeficientes de las tablas actuariales de mortalidad. Para determinar el impacto sobre el sistema financiero y las estructuras mercantiles, se estiman las eventuales pérdidas económicas. Sin embargo, aunque se pueda llegar a determinar un importe en términos monetarios, como suma de pérdidas de diversa índole, incluido el coste en términos de víctimas, la consecuencia de un acto terrorista nunca se puede llegar a medir, puesto que el valor de la vida humana es inconmensurable.

El terrorismo actual supone un desafío global, por lo que integrar la amenaza, la vulnerabilidad y la consecuencia en un modelo de evaluación del riesgo de financiación del terrorismo como el EBR beneficia a los tres grandes actores implicados. En primer lugar, a las instituciones públicas, como actores estatales, puesto que toman sus decisiones políticas en el ámbito de la seguridad y la defensa. En segundo lugar, a las empresas privadas, como actores no estatales, que toman sus decisiones mercantiles en un contexto de inteligencia económica. Y finalmente, a la población civil, preocupada por su propia seguridad, que en los últimos años ha experimentado una creciente percepción de la amenaza del terrorismo, y sobre todo del yihadista.

4. Canales de pago tradicionales

El sistema financiero canaliza un gran volumen de transacciones comerciales, entre las que se esconden los flujos procedentes de actividades ilícitas, y también se disimulan transacciones, tanto lícitas como ilícitas, vinculadas con la financiación del terrorismo.

Para efectuar los pagos que requieren las actividades económicas, así como para el movimiento de fondos, se utilizan instituciones financieras u otros agentes intermedios, sobre todo cuando los volúmenes transaccionales alcanzan cifras considerables, o cuando la distancia entre emisor y receptor hace inviable una transacción directa. Los intermediarios, que en el marco normativo español se denominan sujetos obligados, deben establecer procedimientos de prevención y control para evitar ser utilizados en los procesos de blanqueo de capitales, y sobre todo en la canalización de fondos vinculados con la financiación del terrorismo. El grado de exposición al riesgo de financiación de terrorismo es muy diferente en cada tipo de sujeto obligado, ya que depende de factores cualitativos y cuantitativos, relacionados con el tipo de actividad realizada por el propio sujeto obligado.

En la actualidad, para transferir fondos y gestionar la gran variedad de instrumentos financieros disponibles, existen distintos canales o sistemas de pago en los que intervienen, por una parte, las instituciones que ordenan el trasvase de activos financieros por cuenta propia o de sus clientes (ordenantes), y por otra parte, las instituciones que reciben dichos activos por cuenta propia o de sus clientes (beneficiarios). A través de los canales fluyen tanto las operaciones directas de institución a institución, como las que requieren un paso intermedio, es decir, los servicios de corresponsalía de una tercera institución, que liquida las transacciones mediante cuentas de compensación. Los procedimientos de prevención y control en los sistemas de pago son complejos, dado el ingente volumen de transacciones que tramitan. Precisan de herramientas informáticas especializadas, tanto para detectar flujos relacionados con el blanqueo de capitales, como para identificar aquellos que pueden estar vinculados con la financiación del terrorismo.

Por otra parte, excepto en algunas zonas delimitadas que permanecen aisladas, la mayor parte de la población mundial desarrolla actividades económicas, que requieren la participación, en mayor o menor medida, del sistema financiero. La implementación de medidas que involucren conjuntamente a instituciones financieras, sistemas de pago y supervisores es la forma más eficaz de detectar transacciones inusuales en las que participen personas relacionadas con el terrorismo, cuyo perfil puede ser muy variado: terroristas integrados en un grupo establecido, terroristas que forman parte de pequeñas células, reclutadores que intentan captar nuevos adeptos, combatientes retornados, captadores de fondos, distribuidores de fondos, simpatizantes,... Sin embargo, las medidas de control deberían ser capaces de discriminar entre las personas

que hacen un uso indebido intencionado de aquellas que intervienen involuntariamente, ya que su propósito es la mera aportación de fondos con fines benéficos, por ejemplo la limosna obligatoria zakat, o los actos voluntarios de caridad, como waqf o sadaqah.

Los grupos terroristas se organizan en función de sus necesidades, que son muy diversas. Desde un punto de vista funcional, las organizaciones o grupos terroristas tienen distintos requisitos en función de su estructura: organización compuesta de un número considerable de integrantes agrupados geográficamente (como el caso de Boko Haram), estructura dispersa compuesta de franquicias semi-independientes (Al Qaeda), organización que domina un territorio en el que pretende instaurar un pseudo-estado (Daula Al Islami, más conocida como Daesh), pequeña célula integrada por un número reducido de personas, lobo solitario, reclutador... Sus necesidades financieras dependen de sus estructuras.

Las grandes organizaciones terroristas requieren un volumen considerable de fondos para su propia subsistencia y la seguridad de sus integrantes. Precisan financiación para la adquisición de armas, entrenamiento de combatientes, captación de nuevos integrantes y la difusión de propaganda. En la mayor parte del mundo desarrollado, tanto las instituciones financieras como los canales de pago tradicionales han establecido procedimientos de control para detectar flujos financieros vinculados con el terrorismo, dentro de lo que se denominan medidas de prevención AML/CFT, es decir, las medidas contra el blanqueo de capitales (AML: Anti Money Laundering) y la financiación del terrorismo (CFT: Countering the financing of terrorism). Estas grandes organizaciones terroristas han tenido que evolucionar, adaptándose y aprovechando las vulnerabilidades de los nuevos canales de pago, que surgen gracias a las innovaciones tecnológicas, al convertirse en servicios accesibles de uso generalizado. Tienen recursos suficientes para conseguir servicios profesionales especializados, que les ofrecen la oportunidad de seguir transfiriendo fondos sin ser detectados por los procesos de control del sistema financiero. Las herramientas de control no siempre tienen el dinamismo suficiente para adaptarse a las últimas novedades, e impedir la financiación de estas organizaciones.

Sin embargo, tanto los pequeños grupos terroristas, como los que actúan en solitario, suelen carecer de los recursos, el conocimiento o la oportunidad para acceder a estos nuevos servicios. En consecuencia, tienden a seguir usando los canales tradicionales de pago.

Según un informe de GAFI (Financial Action Task Force, 2015), en el pasado se han detectado transacciones cuyos beneficiarios son grupos extremistas locales, que reciben financiación mediante transferencias ordenadas por organizaciones terroristas internacionales. Sin embargo, Daesh parece ser una excepción, debido a su capacidad para generar tal volumen de fondos en su territorio, que no ha precisado financiación ajena. No obstante, ha recibido una cantidad relativamente pequeña de fondos procedentes de fuentes externas. Por su parte, y según el mismo informe, además del efectivo, los combatientes terroristas extranjeros o foreign terrorist fighters⁶ (FTFs), han estado usando fundamentalmente los canales tradicionales de pago, es decir, los saldos que presentan sus cuentas bancarias (principalmente se dispone de dichos fondos a través de cajeros automáticos) y giros a través de entidades de pago.

En los próximos apartados se analiza el riesgo de financiación del terrorismo en los canales financieros tradicionales, que son los sistemas de transferencias de fondos formales (transferencias bancarias y envíos a través de entidades de pago) y los sistemas informales (los más comúnmente conocidos son los Hawala).

4.1. Transferencias bancarias

Las entidades bancarias canalizan sus operaciones a través de sistemas multilaterales integrados e interrelacionados en infraestructuras financieras, que aseguran el procesamiento, la compensación y la liquidación de transacciones. Las principales infraestructuras de los mercados financieros en los que

⁶ Según la Resolución 2178 (2014) del Consejo de Seguridad de Naciones Unidas, foreign terrorist fighters (FTFs) o combatientes terroristas extranjeros son "las personas que viajan a un Estado distinto de su Estado de residencia o nacionalidad con el propósito de cometer, planificar o preparar actos terroristas o participar en ellos, o de proporcionar o recibir adiestramiento con fines de terrorismo".

intervienen entidades bancarias son sistemas de pago y sistemas de poscontratación de valores.

En Europa, el Eurosistema es el propietario de principal sistema de pagos, TARGET2 (sistema europeo de grandes pagos), legalmente estructurado como un conjunto de sistemas nacionales, que funciona de manera centralizada. Participan 1.007 instituciones de manera directa y 837 de manera indirecta (Banco de España, 2015). La conexión de TARGET2 con la Securities-T2S, plataforma para liquidación de valores, en junio de 2015, ha supuesto la integración en Europa de los sistemas de pago y los sistemas de poscontratación de valores. La operativa de los sistemas de pago europeos debe ser acorde con los principios CPMI (señalados por el Comité de Pagos e Infraestructuras de Mercado del Banco Internacional de Pagos) e IOSCO⁷ (establecidos por la Organización Internacional de Comisiones de Valores), en especial los Sistemas de Importancia Sistémica (SIPS), que son aquellos que cumplen al menos dos de los siguientes cuatro requisitos: impacto financiero (canalizan más de 10.000 millones de euros diarios), peso en los mercados (su cuota de mercado debe ser, al menos, el 15% en volumen transaccional, el 5% de los pagos transfronterizos o el 75% del total de pagos de un estado miembro), dimensión transfronteriza (actividad transfronteriza con al menos cinco países distintos al operador, que supongan un mínimo del 33% de lo procesado por el sistema) e interdependencia directa (liquidación de sistemas vinculados).

TARGET2-BE es el componente español del sistema europeo de grandes pagos. Ocupa la quinta posición en el ranking de los componentes que más número de operaciones canalizan y la cuarta por volumen transaccional, tras Alemania, Francia y Holanda. Tiene la relevancia y peso suficiente para ser considerado sistema SIPS. En el año 2014 ha canalizado 7,2 millones de operaciones cuyo importe total ascendió a 62 billones de euros. El sistema de pagos español clave para pagos minoristas es el Sistema Nacional de Compensación Electrónica (SNCE), que durante 2014 canalizó 1,5 billones de euros en 1.688 millones de operaciones procesadas.

El sector bancario puede transferir fondos internacionales del modo más fiable y eficiente, a la vez que es vulnerable a usos indebidos. Por tanto, cada entidad debe establecer sus propios procedimientos de control, en el ámbito de las medidas de prevención AML/CFT, que permitan detectar operativas sospechosas, dentro de los millones de transacciones tramitadas a través de sus sistemas informáticos.

Las entidades bancarias que operan en España tienen que establecer un Órgano de Control Interno⁸ (OCI), que es el responsable de la aplicación de las políticas y procedimientos en materia de diligencia debida⁹, con objeto de prevenir e impedir operaciones relacionadas con el blanqueo de capitales o la financiación del terrorismo. Las medidas de diligencia debida conllevan la identificación del titular formal y real, así como el conocimiento de la actividad del mismo, lo que incluye conocer el origen de los fondos que canaliza el cliente en la propia entidad. Las medidas de control interno se establecen en función del grado de exposición al riesgo inherente a la naturaleza de la actividad que lleva a cabo cada entidad. La valoración del riesgo depende de elementos objetivos tales como “sector de actividad, volumen de negocio, número de empleados, zonas en las que se opera, medios de pago empleados y procedencia de los mismos, nacionalidades o países que intervengan en las transacciones, realización del negocio mediante agentes,...” (Sepblac, 2013). Dicha valoración servirá para establecer las políticas, procedimientos y manuales adecuados.

Los OCI también deben participar activamente en la toma de decisiones durante los desarrollos informáticos que establecen los sistemas de detección, gestión y resolución de operativas inusuales, así como las alertas adecuadas por tipología, intervinientes y cuantía de las operaciones, en función del riesgo específico

⁷ La Organización Internacional de Comisiones de Valores establece los estándares de los mercados de valores. La Secretaría tiene su sede en Madrid. Regula el 90% de los mercados de valores del mundo.

⁸ Capítulo IV – Del control interno, Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

⁹ Capítulo II – De la Diligencia debida, Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

de la entidad. Dichos desarrollos deben servir para evitar que la entidad canalice operativas que puedan estar relacionadas con actividades no lícitas, en general, y con la financiación del terrorismo, en particular. Además, deben cumplir con la obligación de verificar que ni los clientes ni las personas que realizan operaciones estén incluidos en la lista de sanciones publicadas. Los sistemas deben ser capaces de bloquear de forma automática la ejecución de operaciones con intervinientes cuya identidad coincida inequívocamente con algún registro que figura en las listas. Y en el caso de que las operaciones hayan sido ya ejecutadas, los sistemas deben ser capaces de cancelarlas o retrotraerlas. Deben contar con una unidad técnica con personal especializado, en dedicación exclusiva, y con formación adecuada en materia de análisis, acorde con lo establecido en el artículo 35 del Real Decreto 304/2014 de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

Los clientes del sistema bancario pueden mover fondos globalmente de manera fácil y rápida, a través del sistema financiero internacional, lo que proporciona una oportunidad a los grupos criminales de realizar actividades financieras, que pasan desapercibidas entre las operativas normales y habituales. Las operaciones de financiación del terrorismo a través del sector bancario, si son de pequeña magnitud, son difíciles de distinguir entre el gran número de transacciones financieras legítimas que se realizan cada día. Pero las medidas de prevención AML/CFT implementadas en el sector bancario han logrado que sea más difícil que se utilice el sector financiero para canalizar fondos procedentes de actividades ilícitas, en general, y vinculados al terrorismo, en particular. No obstante, algunos riesgos persisten. Es posible el uso indebido de los productos financieros tradicionales, por ejemplo, cuando los simpatizantes de grupos terroristas abren cuentas de ahorro y entregan la tarjeta asociada a un miembro de la organización terrorista, que le permite acceder a efectivo mediante reintegros en cajeros automáticos, tanto en bancos nacionales como en bancos extranjeros (Financial Action Task Force, 2015). Otro ejemplo y motivo de preocupación de GAFI, es que Daesh busque aprovecharse de las sucursales de los bancos sirios o iraquíes o de otras instituciones financieras para financiar sus actividades, además de mandar fondos al extranjero para obtener armas y otros bienes para su funcionamiento (Financial Action Task Force, 2015).

4.2. Entidades de pago

Las Remesas de Emigrantes son los ahorros transferidos a los correspondientes países de origen, a partir de los recursos generados por el desarrollo de sus actividades económicas en los países donde residen. La población emigrante procedente de países bancarizados (por ejemplo europeos, estadounidenses, canadienses,...) tramitará sus envíos a través de canales bancarios, mientras que los emigrantes cuyas áreas de origen tienen un nivel de bancarización limitado (sudamericanos, asiáticos y africanos) tenderán a utilizar otro tipo de intermediarios.

Los principales intermediarios de transferencias no bancarias son las entidades de pago (entidades remesadoras, anteriormente denominadas gestoras de transferencias) o MVTS (Money Value Transfer Services). Según la normativa española, los MVTS son sujetos obligados, y por tanto deben establecer procedimientos de control, en el ámbito de las medidas de prevención AML/CFT, para evitar tramitar operaciones relacionadas con el blanqueo de capitales o la financiación del terrorismo. Deben tener un Órgano de Control Interno (OCI) responsable de la aplicación de las políticas y procedimientos adecuados a las circunstancias particulares de este tipo de sujeto obligado.

Según el informe de tipologías del Servicio Ejecutivo de la Comisión de Prevención de Blanqueo de Capitales e Infracciones Monetarias (Sepblac, 2008b), los MVTS se caracterizan por: (1) una amplia red de agentes con establecimientos en los que se pueden desarrollar simultáneamente otras actividades económicas no financieras, como los conocidos locutorios; (2) suele coincidir la nacionalidad de los gerentes o propietarios de los establecimientos con la de los clientes; (3) los fondos se canalizan a través de grandes cuentas bancarias compensadoras que agrupan las remesas, de manera que estas pierden el detalle del importe individualizado; (4) la propia dinámica facilita que grupos criminales intenten captar a determinados agentes para que se integren en sus organizaciones y así puedan llegar a adquirir el control de remitentes y beneficiarios en transacciones puntuales. Como los agentes operan con un elevado nivel de autonomía, tienen la capacidad de



adulterar información sobre determinadas transacciones, dificultando que el OCI las detecte. Por consiguiente, es un canal especialmente sensible al blanqueo de capitales. Los establecimientos de cambio de moneda y gestión de transferencias han sido utilizados por los delincuentes para blanquear fondos de distintas formas (Sepblac, 2008a). Sin embargo, en España se han tomado una serie de medidas durante los últimos años, entre las que destaca el incremento de las inspecciones en estas entidades de pago, que han tenido como resultado un proceso de purga en el sector (Financial Action Task Force, 2016). Las principales consecuencias de dicho proceso han sido: (1) la desaparición de varias entidades, (2) la mejora generalizada en los procedimientos de control de las entidades que continúan operando, (3) la creación de una base de datos de agentes cuyas operativas hayan sido consideradas sospechosas, y (4) una considerable reducción en la canalización de flujos de fondos ilícitos por este sistema.

En general, las entidades de pago son muy vulnerables a la financiación del terrorismo, especialmente, porque puede utilizar como contraparte a agentes ubicados en zonas próximas a las áreas de conflicto, en las que el acceso a los servicios bancarios es muy limitado. Algunos de esos agentes no están regulados, ni están sujetos a una supervisión AML/CFT apropiada, operan sin licencia (por lo que carecen de medidas de control AML/CFT) o se relacionan con agentes de sistemas de TIF (Sistemas de Transferencia Informal de Fondos), todo ello sin conocimiento del OCI.

No obstante, el mayor riesgo de las MVTS consiste en que alguno de sus agentes (o algún empleado de un establecimiento) transfiera fondos en nombre de un grupo terrorista, falsificando la documentación requerida para tramitar la operación. Se cree que los talibán usaban el sistema bancario para blanquear las ganancias derivadas de la venta de drogas, pero volvieron a utilizar los canales de las MVTS cuando la autoridad monetaria afgana implementó una normativa bancaria más restrictiva (Financial Action Task Force, 2013a). También hay informes sobre el uso de MVTS para proveer de fondos para reclutar FTFs y ayudarles a costear sus viajes a las zonas de conflicto (Financial Action Task Force, 2013b).

4.3. Envíos por sistemas informales

Los sistemas de Sistemas de Transferencia Informal de Fondos (TIF), más conocidos como Alternative Remittance Systems (ARS), nacieron por la necesidad de disponer de un instrumento financiero en las antiguas rutas comerciales, debido a los peligros que conllevaba portar oro u otros medios de pago. Para evitar perder todas las ganancias del viaje, los comerciantes utilizaban los servicios prestados, de manera un tanto rudimentaria, por aquellos primeros intermediarios financieros. Se utilizaban mucho en Asia oriental, y todavía siguen operando, aunque con distintos nombres (El-Qorchi, 2002): Fei-Ch'ien en China, Padala en Filipinas, Hundi en India, Hui Kuan en Hong Kong y Phei Kwan en Tailandia. Con el nacimiento de la banca moderna los sistemas de TIF perdieron relevancia internacional. Sin embargo, los movimientos migratorios desde Asia oriental y África hacia Europa, Estados Unidos, Canadá y región del Golfo Pérsico han dado un nuevo impulso a estos sistemas. El sistema de TIF de uso más extendido en la actualidad es el Hundi, más conocido como Hawala, en el que las transacciones se transfieren entre hawaladars (proveedores de servicios o agentes), con independencia de la naturaleza de la transacción y del país de origen o destino.

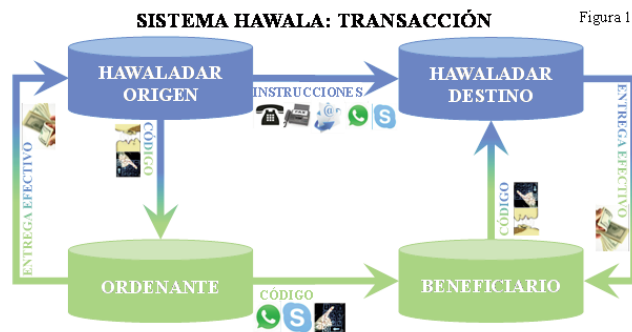


Figura 1. Sistema Hawala: Transacción. Fuente: Elaboración propia.

En el sistema Hawala, el ordenante entrega los fondos al hawaladar origen, quien le indica un código transaccional. El hawaladar origen envía las instrucciones de pago (como importe y código transaccional) al hawaladar destino por teléfono, fax, correo electrónico o cualquier otro medio de comunicación. Por su parte, el ordenante le indica dicho código transaccional al beneficiario, a través del medio por el que habitualmente se comunican. El hawaladar destino entregará los fondos a la persona que disponga del citado código transaccional.

Los hawaladars operan al margen de los canales financieros oficialmente regulados. Utilizan procedimientos manuales de anotaciones en cuenta para el registro de sus transacciones. Las operaciones no suponen movimiento físico de fondos, sino que se liquidan por compensación de saldos, por lo que los flujos financieros canalizados entre hawaladars suponen una pequeña fracción de su volumen de negocio.

Los usuarios de los servicios Hawala los prefieren a la banca o a otros sistemas formales de transferencia de fondos porque les ofrecen las siguientes ventajas:

- **Más económicos:** Las comisiones son más bajas, dado que no tienen que cumplir con todos los requisitos burocráticos que los sistemas financieros regulados exigen para tramitar transacciones. Además, si los agentes operan sin licencia, las autoridades fiscales no les pueden exigir la carga tributaria que les corresponde, que sí tienen que pagar los intermediarios financieros legalmente establecidos.

- **Mayor rapidez:** Dado que el mecanismo es muy sencillo, el dinero se transfiere en menos de 24 horas, incluso si el origen o el destino están en una zona remota a cientos de kilómetros del operador financiero convencional más próximo. La disponibilidad de los usuarios de este sistema no siempre coincide con los horarios de la banca convencional, ni con los de otros sistemas formales de transferencia de fondos. Sin embargo, los hawaladars no tienen las limitaciones de horario de la banca convencional, puesto que sus jornadas de trabajo son flexibles y adaptadas a las circunstancias de su clientela.

- **Ventajas sociales:** Los usuarios confían menos en los empleados de banca o los agentes de los servicios de transferencia formal de fondos que en sus hawaladars, con los que suelen tener un vínculo étnico, de parentesco o una relación personal. Si hay confianza, es posible anticipar los pagos, es decir, que el hawaladar que actúa de contraparte entregue los fondos al beneficiario antes de que el ordenante efectúe su pago al hawaladar de origen.

- **Ventajas culturales:** Los hawaladars comparten los mismos lazos culturales que los usuarios y respetan los códigos sociales. Así, por ejemplo, en el caso de que la persona que recibe los fondos fuera una mujer ubicada en un lugar en el que la tradición o religión le impide el contacto fuera del ámbito familiar, el hawaladar le haría llegar los fondos a través de un intermediario considerado socialmente aceptable, lo que evitaría que ella tuviera relación con el mundo exterior, especialmente con empleados de banca, que además le obligarían a identificarse, mostrando su rostro.

- **Menores restricciones:** Los sistemas de prevención AML/CFT han incrementado los controles, reducido el umbral transaccional (importe unitario preestablecido como límite para determinadas operaciones de riesgo) y aumentado los requisitos para enviar fondos a determinados países. Por tanto, es bastante complejo el uso de los canales convencionales, incluso para aquellos emigrantes que pretenden remitir parte de sus salarios obtenidos lícitamente a sus familias, las cuales permanecen en países que las entidades consideran de riesgo, especialmente si la ubicación de destino está cerca de las zonas de conflicto. Por otra parte, las entidades convencionales son inaccesibles para aquellos que quieren ocultar su condición de inmigrantes ilegales. Además, algunas entidades pueden llegar a establecer políticas restrictivas, impidiendo expresamente que se transfieran fondos a determinadas zonas o, incluso, que se tramiten transacciones en las que ordenantes o beneficiarios sean de determinadas nacionalidades. El hawaladar evita al usuario todos estos inconvenientes de los sistemas convencionales.

Los costes, la lentitud, las restricciones y la ineficacia de las instituciones convencionales han contribuido al desarrollo y propagación de los sistemas de TIF, que conectan financieramente una amplia zona del mundo en la que no existe regulación ni control.



Regular el funcionamiento de los sistemas de TIF es bastante complejo, ya que implicaría una normativa jurídica uniforme, lo que no es viable, dada la cantidad y diversidad de jurisdicciones existentes. En algunos países los sistemas de TIF están prohibidos, por lo que regularlos conllevaría legitimarlos. Sin embargo, en los países donde son jurídicamente aceptados, una regulación restrictiva podría ocasionar eventualmente una mayor opacidad de las transacciones. Tanto el sistema Hawala como otros sistemas de TIF han sido utilizados por terroristas para sus transacciones financieras (Financial Action Task Force, 2013c). Por consiguiente, las autoridades monetarias y los supervisores financieros deben centrar sus esfuerzos en evitar que los sistemas de TIF sean utilizados para el blanqueo de capitales o la financiación del terrorismo.

Actualmente los sistemas de TIF siguen siendo vulnerables a ser utilizados como canal de transmisión de fondos vinculados a la financiación del terrorismo por:

- **Falta de supervisión:** Coexiste la insuficiencia de recursos destinados a la supervisión con la ausencia de voluntad supervisora de algunas jurisdicciones.
- **Sistema de liquidación:** Las transacciones se compensan y se liquidan por canales financieros no regulados establecidos entre diferentes jurisdicciones, por lo que es difícil que las autoridades financieras admitan asumir íntegramente su responsabilidad.
- **Agentes financieros:** Los agentes suelen compatibilizar su labor de hawaladar con la de gestor de otro tipo de negocio, de manera que no se puede llegar a delimitar exactamente la parte imputable a cada actividad.
- **Naturaleza de la transacción:** Se producen compensaciones entre pagos de diversa índole: (1) origen lícito, (2) origen ilícito, relacionados con actividades delictivas, y (3) de origen lícito o ilícito, pero cuyos destinatarios son personas vinculadas con el terrorismo.

Algunos de los casos conocidos de uso del sistema Hawala para la financiación del terrorismo en Estados Unidos son (Financial Action Task Force, 2013c): Hamza Case, Time Square Bomber Case y Carnival Ice Cream Case.

En España también hay casos conocidos de utilización del sistema Hawala para la financiación del terrorismo (Financial Action Task Force, 2013c; Lombardero Expósito, 2015):

- Sentencia Audiencia Nacional, Sala de lo Penal, número 6284/2006: “Se declara acreditado que el acusado ejercía funciones de Hawala. El acusado afirma que es el responsable del sistema Hawala en España y que forma parte de una estructura superior fiscalizada por otros individuos”.
- Sentencia Tribunal Supremo, Sala II, número 4947/2007: “El acusado regentaba un locutorio desde el que se realizaban importantes movimientos de dinero, tanto ingresos como transferencias, que era el responsable de una red Hawala en España y que al menos había acreditados dos pagos para financiar actividades terroristas”.
- Sentencia Tribunal Supremo, Sala II, número 2754/2008: “Se analiza un supuesto envío de fondos por el sistema Hawala efectuado por pakistaníes desde locutorios ubicados en el barrio de El Raval”.
- Sentencia Audiencia Nacional, número 2591/2010: “El acusado moviliza fondos a través de un hawaladar a Argelia por cuenta de grupos terroristas y a través de gestoras de transferencias”.
- Sentencia Audiencia Nacional, número 1943/2011: “Los acusados financian la fuga de algunos terroristas que habían participado en los atentados de 2004 en Madrid, facilitándoles alojamiento y financiando sus gastos de viaje”.

5. Conclusión

El terrorismo yihadista es uno de los fenómenos que más preocupa a la comunidad internacional. Hacer frente a la amenaza terrorista supone un desafío en el ámbito de la seguridad y la defensa. Durante los últimos años se ha evolucionado hacia un concepto de seguridad integral, como objetivo y esfuerzo compartido por todos, instituciones públicas, sector privado y sociedad civil. Además, se ha reforzado la cooperación entre países en esta materia.

Conscientes de que una de las claves de la expansión de los grupos terroristas es la capacidad que tienen de disponer de una considerable cantidad de recursos económicos, las estrategias para combatir la amenaza terrorista incluyen la lucha contra sus fuentes de financiación. Para ello es necesaria la implicación del sistema financiero, cuyas instituciones pueden establecer los mecanismos para detectar flujos monetarios vinculados con actividades terroristas. El objetivo es evitar que se canalicen flujos monetarios puntuales que puedan llegar a financiar actos terroristas, o que sean utilizados por organizaciones, grupos terroristas o terroristas individuales.

Una gran cantidad de países han aceptado adoptar los estándares internacionales planteados por GAFI, que consisten en que, dependiendo de las circunstancias de cada jurisdicción, se evalúen los riesgos nacionales en función de la amenaza terrorista, las vulnerabilidades de sus sistemas y las consecuencias del terrorismo. El estudio y análisis de la amenaza terrorista, así como de sus consecuencias está suficientemente tratado, tanto en el ámbito de los profesionales de la seguridad y la defensa como en el científico y académico. Es por tanto en el ámbito de las vulnerabilidades donde es más necesario profundizar en su estudio. Por este motivo, todas las organizaciones que integran los sistemas financieros (entidades, supervisores y mercados) tienen que realizar un análisis interno pormenorizado, con objeto de detectar sus propias vulnerabilidades, como requisito necesario para cuantificar el riesgo de financiación del terrorismo, cuyo propósito es la toma de decisiones sobre la asignación de recursos, que son necesarios para mitigar dicho riesgo.

Los flujos financieros circulan por los canales de pago. Se ha analizado el funcionamiento de los canales de pago tradicionales, como las transferencias bancarias, las entidades de pago y los de transferencia informal de fondos, como el sistema Hawala. Tanto en el sector bancario, como en las entidades de pago, se han implementado unos órganos de control interno responsables de la aplicación de las políticas y procedimientos para prevenir e impedir operaciones relacionadas con la financiación del terrorismo. Desde la implementación de dichos órganos de control, se ha reducido considerablemente el riesgo de que dichos canales de pago sean utilizados para la financiación del terrorismo, aunque todavía es posible tomar medidas adicionales que mitiguen dicho riesgo mucho más.

Sin embargo, algunos canales de pago tradicionales continúan siendo vulnerables, en concreto los sistemas de transferencia informal de fondos, como el Hawala, que pueden ser utilizados por los terroristas para sus transacciones financieras. La regulación del funcionamiento de los sistemas informales sería bastante compleja, además de que podría tener como consecuencia una mayor opacidad de las transacciones.

Por tanto, es imprescindible que se centren los esfuerzos en fomentar la utilización de los canales formales de pago, en detrimento de los sistemas de transferencia informal. Disponer de un sistema de pagos eficiente, con menores costes y poco vulnerable evitará la proliferación de actividades informales, y contribuirá a la prevención de usos indebidos, como la financiación del terrorismo. Simultáneamente, también es preciso evitar que una eventual disminución en el flujo canalizado por los canales de pago tradicionales, tanto formales como informales, implique el trasvase de fondos a nuevos canales e instrumentos financieros, como las monedas virtuales, las tarjetas prepago y los sistemas de pago electrónico, cuyo uso generalizado entraña unos riesgos cuyas evaluaciones trascienden el alcance del presente artículo, y que serán objeto de próximos estudios.

Cómo citar este artículo / How to cite this paper

Martínez, M. J. (2016). Riesgo de financiación del terrorismo: Vulnerabilidades de los canales de pago. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 1(1), 66-78. (www.cisdejournal.com)

Referencias

Banco de España (2015). Memoria anual sobre la vigilancia de los sistemas de pago 2014. Madrid.

Martínez, M. J. (2016). Riesgo de financiación del terrorismo: Vulnerabilidades de los canales de pago. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 1(1), 66-78.



- El-Qorchi, M. (2002). Hawala ¿Cómo funciona este sistema de transferencia informal de fondos? ¿Debe ser regulado? Finanzas & Desarrollo.
- Financial Action Task Force (2007). Guidance on the risk-based approach to combating money laundering and terrorist financing: High level Principles and Procedures. FATF, Paris.
- Financial Action Task Force (2012). International standards on combating money laundering and the financing of Terrorism & proliferation. FATF, Paris.
- Financial Action Task Force (2013a). Financial flows linked to the production and trafficking of Afghan opiates. FATF, Paris.
- Financial Action Task Force (2013b). National Money Laundering and Terrorist Financing Risk Assessment. FATF, Paris.
- Financial Action Task Force (2013c). The role of Hawala and other similar service providers in money laundering and terrorist financing. FATF, Paris.
- Financial Action Task Force (2015). Emerging Terrorist Financing Risks. FATF, Paris.
- Financial Action Task Force (2016). Money or Value Transfer Services. FATF, Paris.
- Ley 10/2010 (2010). De 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
- Lombardero Expósito, L. M. (2015). El nuevo marco regulatorio del blanqueo de capitales. Bosch, Barcelona.
- Presidencia del Gobierno. Departamento de Seguridad Nacional (2014). Informe anual de Seguridad Nacional 2014.
- Real Decreto 304/2014 (2014). De 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
- Sepblac (2008a). Factores clave para la prevención del blanqueo de capitales en la gestión de transferencias. Madrid. (http://www.sepblac.es/espanol/informes_y_publicaciones/La_gestion_de_transferencias.pdf)
- Sepblac (2008b). Tipologías de blanqueo de capitales. Madrid. (http://www.sepblac.es/espanol/informes_y_publicaciones/informe_sobre_tipologias.pdf)
- Sepblac (2013). Recomendaciones sobre las medidas de control interno para la prevención del blanqueo de capitales y de la financiación del terrorismo. Madrid. (http://www.sepblac.es/espanol/informes_y_publicaciones/documento%20recomendaciones_sobre_medidas%20control_interno_PBC_FT.pdf)
- Tofangsaz, H. (2015). Terrorism or not terrorism? Whose money are we looking for? *Journal of Financial Crime*, 22(3), 378-390.