El intercambio internacional de información financiera y la lucha contra la financiación del terrorismo: el acuerdo UE-EEUU sobre *Swift*

Ignacio Palicio [*]

Tema: Los acuerdos para la colaboración en el intercambio de información financiera son avances necesarios en la lucha contra la financiación del terrorismo. Pero deben cumplir una serie de requisitos y ser compatibles con un respeto absoluto a la protección de datos de las personas y la legalidad.

Resumen: El establecimiento de mecanismos que prevean y permitan el acceso y el intercambio fluido de la información financiera relevante entre las distintas agencias y autoridades competentes, eliminando las barreras que han permitido la falta de transparencia del sistema y los mercados financieros internacionales, es imprescindible para luchar eficazmente contra la financiación del terrorismo. En este sentido, la firma de acuerdos para la colaboración en el intercambio de información financiera con países que comparten los objetivos de dicha lucha aparece como un elemento de avance necesario. Aquí ha de enmarcarse un acuerdo entre la UE y EEUU sobre *Swift* (*Society for Worldwide Interbank Financial Telecommunication*). Los acuerdos de este tipo, no obstante, deben cumplir una serie de requisitos relacionados con la justificación de la obtención de la información, su concreción, las garantías de su utilización, el control de todo el proceso y la reciprocidad. Estos acuerdos tienen que ser compatibles con un respeto absoluto a la protección de datos de las personas y al cumplimiento de la legalidad por todos y cada uno de los países que participan en esta lucha contra la financiación del terrorismo.

Análisis: La falta de transparencia de los mercados y de los flujos financieros internacionales es, sin duda, uno de los factores determinantes para identificar las razones de la actual crisis económica. Las conclusiones de las reuniones celebradas por los líderes mundiales en el período más reciente incidían en un objetivo básico, que era el avance hacia la integridad y la transparencia del sistema financiero internacional; para ello, entre otras, proponían la adopción de medidas contra las jurisdicciones no cooperativas, incluidos los paraísos fiscales y señalaban que la era del secreto bancario había finalizado.

Un concepto tan amplio como es la integridad y la transparencia del sistema financiero permite distintas aproximaciones y numerosos matices. Partiendo de un principio básico, que es la necesidad de que todos los agentes del sistema deben conocer con exactitud y

[*] *Director del Servicio Ejecutivo de la Comisión de Prevención de Blanqueo de Capitales (Sepblac)*

puntualidad la información necesaria para tomar sus decisiones, estas aproximaciones, que deben ser complementarias, pueden centrarse, entre otras, en la eliminación de las barreras derivadas del interés de ciertas jurisdicciones por obtener ventajas injustificadas, en la erradicación de estructuras o vehículos opacos admitidos y utilizados en el tráfico mercantil de algunos países y mercados, o en la implantación de medidas para asegurar el flujo de información entre las autoridades de los distintos estados.

En el ámbito de esta última aproximación, la existencia de un sistema efectivo de intercambio de información que conecte todos los mercados geográficos aparece como uno de los elementos imprescindibles para la consecución de un objetivo tan ambicioso como la integridad y la transparencia del sistema financiero. Este intercambio de información debería producirse en tres grandes ámbitos: (1) blanqueo de capitales y financiación del terrorismo; (2) supervisión prudencial; y (3) fiscalidad.

A lo largo de este ARI quiero introducir reflexiones y realizar algunas propuestas que permitan sentar las bases para avanzar hacia un sistema eficaz de intercambio entre autoridades de distintos países en lo referente a unos fenómenos tan graves como el blanqueo de capitales y la financiación del terrorismo. Dentro de este marco general, me referiré con especial atención al "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", cuya aprobación fue denegada por el Parlamento Europeo el pasado 11 de febrero de 2010.

Características del sistema Swift

Como aspecto previo, creo importante exponer brevemente las características cualitativas y cuantitativas del más importante sistema de mensajería financiera existente a nivel internacional. La Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (*Swift*, por sus siglas en inglés) es una cooperativa propiedad de sus miembros, a través de la cual el sector financiero lleva a cabo buena parte de sus operaciones comerciales. Fue creada en Bélgica en 1973 y cuenta con oficinas en los principales centros financieros y mercados en desarrollo del mundo. Para llevar a cabo sus actividades, *Swift* se ha dividido en tres regiones: América, Asia-Pacífico y EMEA (Europa, Oriente Medio y África).

Su misión es doble. Por una parte, suministra una plataforma de comunicación privada, es decir, los productos y servicios que permiten que sus clientes puedan conectarse e intercambiar información financiera con seguridad y de forma fiable. En segundo lugar, también actúa como catalizador de la colaboración de la comunidad financiera con vistas a homogeneizar las prácticas del mercado, definir las normas y estudiar soluciones a los problemas de interés común.

Swift es únicamente un transmisor de mensajes que sirve de vehículo para los mensajes enviados entre dos instituciones financieras, con el objetivo de hacerlo de forma segura y de garantizar su confidencialidad e integridad. No posee fondos, no gestiona cuentas en nombre de los clientes, ni tampoco almacena información financiera de forma permanente; en la actualidad los mensajes se almacenan en los centros operativos solamente durante 124 días.

Swift permite a sus clientes automatizar y estandarizar transacciones financieras y, de este modo, reducir tanto los gastos como el riesgo operativo y eliminar ineficiencias en sus operaciones. Cada entidad adherida al sistema tiene una identificación única, el

código de identificación bancario, también denominado código *Swift*. Este código resulta imprescindible para automatizar los pagos entre entidades, de igual manera que es necesaria la inclusión en todos los mensajes de ciertos datos referidos a los intervinientes en las operaciones, con la finalidad de asegurar un tratamiento adecuado de la información y un funcionamiento eficiente del sistema.

Según datos del año 2009, más de 9.000 usuarios (entidades bancarias, instituciones de valores y clientes corporativos) de 209 países están adheridos a *Swift* para intercambiar millones de mensajes financieros estandarizados. En ese año se intercambiaron unos 3.700 millones de mensajes individuales.

Hasta finales del año 2009, *Swift* disponía de dos centros operativos situados uno en EEUU y el otro en los Países Bajos, en cuyas bases de datos se recogían todas las operaciones tramitadas a través del sistema, ya que el centro operativo de EEUU almacenaba todas las operaciones de su zona y una copia, por motivos de seguridad del sistema, de las operaciones de la otra plataforma; de igual manera, el centro operativo de los Países Bajos almacenaba las operaciones propias y una copia de las operaciones de la otra plataforma.

En la actualidad, tras la reestructuración de las plataformas informáticas abordada por el consejo de administración de *Swift* en septiembre de 2007 dentro del programa denominado "Arquitectura Distribuida Multizonal", existen dos plataformas, una para la zona europea y otra para la zona transatlántica, situadas en Suiza y EEUU respectivamente, que almacenan los mensajes intrazona. *Swift* asigna los distintos países a cada una de las plataformas de acuerdo con ciertos criterios, entre los que se incluye la localización geográfica.

En la nueva estructura, además de las dos plataformas zonales, se mantiene la plataforma de los Países Bajos, que se configura como centro global, al ser la única plataforma que almacena las operaciones de las dos plataformas zonales.

A la vista de las características y de la importancia que tiene *Swift* como principal proveedor de servicios de mensajería internacional sobre pagos, parece claro que cualquier programa relacionado con el control de determinados movimientos financieros que puedan vincularse con fenómenos graves de blanqueo de capitales o de financiación del terrorismo ha de apoyarse necesariamente en la extracción de los datos existentes que puedan figurar en este sistema.

Acuerdo de intercambio de datos entre la UE y EEUU: antecedentes
A raíz de los atentados del 11 de septiembre de 2001, el Departamento del Tesoro de EEUU inició el Programa de Seguimiento de la Financiación del Terrorismo (*Terrorist Finance Tracking Program*, o TFTP), que formaba parte del esfuerzo general por perseguir a los terroristas y sus redes utilizando los medios disponibles. En el marco de este Programa, el Departamento del Tesoro cursó requerimiento administrativo de notificación al centro operativo de *Swift* en EEUU para que le facilitara determinados datos de operaciones financieras que se utilizarían exclusivamente con una finalidad antiterrorista. Dado que este centro operativo de *Swift* reunía información de todo el sistema, la solicitud cursada afectaba a todos los datos disponibles a nivel mundial, incluyéndose los referidos a operaciones realizadas fuera de EEUU y los realizados por ciudadanos de otros países, incluidos los europeos.

A través de informaciones de prensa, se tuvo conocimiento público, a mediados del año 2006, del acceso a los datos de *Swift* por parte de las autoridades norteamericanas. A finales de 2006 las autoridades europeas de protección de datos emitieron un dictamen en el que afirmaban que, desde la óptica de la normativa europea en la materia, se habían producido ciertas irregularidades en el acceso a los datos.

En el mes de julio de 2007, la UE publicó un documento en el que analizaba en profundidad el alcance del programa y como signo de compromiso y colaboración en la lucha contra el terrorismo, acordaba designar a una personalidad europea para que confirmara que la aplicación del programa se atenía a las declaraciones recogidas en dicho documento (*Diario Oficial de la Unión Europea*, C 166/18 de 20/VII/2007) y verificara si se garantizaba la protección de los datos personales procedentes de la UE.

La personalidad europea designada, el juez francés Jean Louis Bruguière, tras el trabajo de campo realizado en EEUU a lo largo del año 2008, emitió en diciembre de ese año un informe con una primera conclusión importante: el programa ha supuesto una contribución real a los esfuerzos contra el terrorismo y Europa se ha beneficiado de sus resultados. Con respecto al funcionamiento concreto del programa, concluye que: (1) todas las consultas realizadas a *Swift* están sujetas a unas condiciones estrictas y auditadas externamente, son concretas y están definidas para asegurar que la extracción de los datos se realice con el objetivo exclusivo de luchar contra el terrorismo y que se minimice la cantidad de datos extraídos; (2) que se han establecido las medidas adecuadas para identificar y borrar los datos que no sean necesarios para luchar contra el terrorismo; y (3) que existen sistemas que garantizan la seguridad física de los datos requeridos y la seguridad lógica de acceso a los mismos.

A la vista de estas conclusiones cabe hacer una primera reflexión relacionada con consideraciones de carácter más global, referida a la vinculación entre las medidas de control necesarias para hacer frente a las amenazas globales y los límites de esos controles cuando puedan estar afectando a derechos individuales de las personas o restando eficiencia a los mercados financieros. Sin duda, será necesario establecer controles más efectivos sobre algunas operaciones de riesgo desarrolladas en estos mercados para evitar su utilización por personas o sociedades vinculadas con la financiación del terrorismo.

El desarrollo de la tecnología informática permite plantearse por primera vez que estos objetivos, que pueden parecer todavía contradictorios en el presente, tengan una solución que permita conjugar las aparentes contradicciones que puedan existir entre seguridad y libertad. Por ello, la tecnología no solo debería aplicarse al incremento de la eficiencia de los mercados, sino también a crear controles efectivos sobre determinados movimientos o transacciones de riesgo, estableciendo de manera simultánea estrictos controles tanto sobre las personas autorizadas a acceder a esa información, como a la legitimidad de las razones que motivan el acceso a la misma. Esos controles deben tener en cuenta no sólo distintos grados de acceso a la información restringida y definir con claridad y transparencia las personas autorizadas y los motivos de esos accesos, sino que también deben permitir la auditoría interna y externa del sistema a través de los controles *ex ante* y *ex post* de todos los accesos.

Acuerdo de intercambio de datos entre la UE y EEUU: situación actual

La reestructuración de las plataformas informáticas emprendida por *Swift* supuso que a finales de 2009 el centro operativo de EEUU ya no iba a disponer de la información relativa a las transacciones financieras de las entidades que transmitieran sus

operaciones a través de la plataforma europea, si esas transacciones no pasaban en algún momento por EEUU.

Por ello, las autoridades norteamericanas, dada la importancia del TFTP para prevenir y combatir el terrorismo y su financiación en la UE y en otros lugares del mundo, plantearon la necesidad de firmar un acuerdo con la UE para garantizar que los proveedores designados de servicios de mensajería financiera sobre pagos facilitaran a dichas autoridades los datos almacenados en el territorio de la UE que resultaran necesarios para prevenir y combatir el terrorismo y su financiación, siempre que se observaran de manera estricta las salvaguardias pertinentes en materia de privacidad y protección de datos personales.

El texto del acuerdo que fue negociado a lo largo del año 2009 constaba de 15 artículos en los que se contemplaban el contenido de las solicitudes de información, las salvaguardias aplicables al tratamiento de los datos facilitados y distintas cláusulas referidas a la revisión y denuncia del acuerdo. Su entrada en vigor estaba prevista inicialmente para el día 1 de febrero de 2010 y debía expirar y dejar de surtir efecto a más tardar el 31 de enero de 2011. El Parlamento Europeo, con fecha 11 de febrero de 2010, denegó su aprobación.

Reflexiones sobre el futuro del acuerdo

La situación que se ha producido tras esta decisión del Parlamento Europeo exige en primer lugar realizar algunas consideraciones sobre la conveniencia y la oportunidad del acuerdo. Posteriormente, pasaré a valorar los requisitos que en mi opinión debería cumplir el acuerdo para que fuera aceptable y asumible por parte de los responsables europeos.

Conveniencia y oportunidad del acuerdo

Por lo que se refiere a la conveniencia del acuerdo, me gustaría destacar ante todo la primera conclusión del informe Bruguière, en la que se afirma que el programa estadounidense había supuesto una contribución real a los esfuerzos contra el terrorismo y que Europa se había beneficiado de ello. Ante una afirmación de esta contundencia y teniendo en cuenta las dificultades existentes por parte de las autoridades encargadas de la lucha contra el blanqueo de capitales y la financiación del terrorismo para acceder en el ámbito internacional a informaciones completas sobre transacciones financieras vinculadas con estos fenómenos, parece indudable que un acuerdo de este tipo es imprescindible para asegurar la eficacia de este esfuerzo. Como se ha afirmado en muchas ocasiones, los mercados financieros han sufrido un proceso de globalización y de transformación en los últimos años que, a la vez que los ha hecho mucho más eficientes, ha posibilitado el desarrollo de prácticas que permiten una opacidad muy elevada. Ante una situación como esta, es preciso dotarse de sistemas eficaces, entre los que se incluyen acuerdos de acceso e intercambio de información financiera entre autoridades, que faciliten la eliminación de estas barreras cuando se cumplan determinados requisitos.

Con respecto a la oportunidad de plantear un acuerdo de estas características, parece claro que la gravedad de los hechos vinculados con el blanqueo de capitales y la financiación del terrorismo hace siempre oportuno el impulso de procedimientos más eficaces para evitarlos, pero indudablemente, a la vista de la preocupación puesta de manifiesto por los mandatarios mundiales en relación con la transparencia e integridad del sistema financiero, la adopción de medidas en este ámbito aparece ahora como especialmente oportuna.

Requisitos del acuerdo

Existen una serie de garantías que en mi opinión deberían imponerse a la extracción y utilización de los datos, con la finalidad de conseguir un funcionamiento adecuado de este procedimiento y evitar cualquier utilización del mismo para fines diferentes de la lucha contra el terrorismo y su financiación. Estas garantías ya están en gran parte recogidas en el texto del acuerdo discutido en el Parlamento Europeo, pero sería necesario incorporar otras cláusulas para que el acuerdo fuera plenamente aceptable.

Los principios básicos que deberían inspirar el acuerdo están relacionados con la justificación de las solicitudes, la concreción de las mismas, el tratamiento de los datos obtenidos, la auditoría y el control del proceso, y la reciprocidad. En mi opinión los tres primeros ya se recogen de forma bastante satisfactoria en el texto discutido, mientras que los dos últimos deberían ser objeto de un tratamiento más detallado. No obstante, en los párrafos siguientes me referiré a los cinco principios:

(1) Las solicitudes de acceso a los datos deben estar ante todo justificadas. Es decir, deberán basarse en investigaciones o análisis existentes sobre hechos u operaciones vinculados con el terrorismo y su financiación. La justificación de la solicitud, esto es, las informaciones previas o las pruebas que la motivan, debe incorporarse a la misma para facilitar su auditoría.
(2) Las solicitudes deben ser concretas y fijar claramente los datos que es necesario obtener. Para ello, deberá limitarse al máximo el volumen de los datos e identificar las personas, las entidades, las cuentas y el resto de los datos que puedan estar incorporados en los mensajes financieros, y a los que sea preciso tener acceso.
(3) Los datos obtenidos deberán conservarse en un entorno aislado y seguro, limitándose el acceso a los analistas autorizados y no realizándose ningún tipo de copia exceptuadas las que sean necesarias por seguridad de la información. Asimismo, deberán definirse unos protocolos claros que fijen los períodos de conservación de la información e impongan la destrucción de los datos cuando transcurran los períodos definidos o se demuestre que no son necesarios.
(4) Será preciso definir una autoridad con los poderes y los medios suficientes para controlar *ex ante* la adecuación y la justificación de las solicitudes; para realizar este control podrían aplicarse procedimientos de muestreo que eviten la revisión individualizada de todas y cada una de las solicitudes. Asimismo, esta autoridad podrá establecer controles *ex post* sobre el tratamiento, el uso y la destrucción, en su caso, de los datos extraídos. Es este uno de los aspectos que podría mejorarse en la redacción de un posible acuerdo futuro.
(5) La reciprocidad debería recogerse como un requisito necesario dentro del acuerdo, dado que no se contempla la posibilidad ni se establecen los mecanismos necesarios para que las autoridades europeas responsables de la investigación del terrorismo tengan acceso a los datos si no es a través de la autoridad norteamericana designada (el Departamento del Tesoro). Si bien es cierto que las legislaciones de los países europeos y la de EEUU son diferentes, y que sólo en este último país se ha definido y concretado un programa específico para la lucha contra el terrorismo y se ha designado a una autoridad administrativa como competente para el acceso a determinados datos financieros, al menos, hasta el establecimiento de un programa similar en la UE o en alguno de sus países miembros, debería designarse una autoridad europea o unas autoridades nacionales con competencias similares. En la actualidad ya existen en la UE mecanismos de cooperación en distintos niveles, judicial, policial y de unidades de inteligencia financiera, que permitirían asumir estas competencias.

Conclusiones: La importancia y la gravedad de la lucha contra el terrorismo y su financiación exigen una armonización de la normativa a nivel mundial y la aportación de los instrumentos necesarios para ello a los órganos encargados de la prevención y represión en cada uno de los países. Las resoluciones de las Naciones Unidas sobre la lucha contra el terrorismo, especialmente la 54/109 del año 1999 de la Asamblea General y la 1373 del año 2001 del Consejo de Seguridad, ya han puesto las bases para esta armonización y señalado algún instrumento para hacer más eficaz la lucha contra el terrorismo.

Entre los instrumentos para conseguir una mayor eficacia aparece en la actualidad como imprescindible el establecimiento de mecanismos que prevean y permitan el acceso y el intercambio fluido de la información financiera relevante para este fin entre las distintas agencias y autoridades competentes, eliminando las barreras que han permitido la falta de transparencia del sistema y los mercados financieros internacionales.

Para la consecución de estos objetivos, la firma de acuerdos para la colaboración en el intercambio de información financiera con países que los comparten aparece como un elemento de avance necesario. Estos acuerdos, no obstante, deben cumplir una serie de requisitos relacionados con la justificación de la obtención de la información, su concreción, las garantías de su utilización, el control de todo el proceso y la reciprocidad. En definitiva, estos acuerdos tienen que ser compatibles con un respeto absoluto a la protección de datos de las personas y al cumplimiento de la legalidad por todos y cada uno de los países que participan en esta lucha.

Ignacio Palicio
Director del Servicio Ejecutivo de la Comisión de Prevención de Blanqueo de Capitales (Sepblac)