Seguridad

Cuaderno Red de Cátedras Telefónica

Universidad de Salamanca

La trasferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos

Cátedra Telefónica de la Universidad de Salamanca

Juan Santos Vara

No. 7. Septiembre 2012

www.catedras.telefonica.es
http://catedraseguridad.usal.es

Telefónica

Cátedra de Seguridad Universidad de Salamanca
Dirección y Coordinación:
Prof. Dr. D. Fernando Pérez Álvarez, Profesor titular Derecho Penal. Director Ciencias de la Seguridad (CISE).
Profa. Dra. Dña. Angélica González Arrieta, Profesora titular Ciencias de la Computación e Inteligencia artificial.
Profa. Dra. Dña. Lina Mariola Díaz Cortés. Profesora Ciencias de la Seguridad (CISE).
Despacho:
291 Facultad de Derecho, Campus Miguel de Unamuno.
Teléfono:
923294400 Ext. 1622
Correo electrónico:
catedratelefonica@usal.es

Juan Santos Vara

Profesor Titular de Derecho Internacional Público y Relaciones Internacionales de la Universidad de Salamanca. Director del Master y del Doctorado en Estudios de la Unión Europea de la Universidad de Salamanca. Diplomado por el Centre for Studies and Research in International Law de la Hague Academy of International Law. Master en Altos Estudios Europeos por el College of Europe y Master en Derecho Comunitario Europeo por la Universidad Carlos III de Madrid. Ha realizado estancias de investigación en los últimos cinco años en el European University Institute de Florencia, la Harvard School of Law, el Watson Institute for International Studies de la Universidad de Brown, el Center of European Studies de la London King's College y en la Hague Academy of International Law. Ha participado en los últimos cinco años en seis proyectos de investigación financiados en los últimos años sobre temas internacionales y europeos (cinco nacionales y uno europeo).

El autor forma parte del proyecto de investigación "la dimensión exterior del Espacio de Libertad, Seguridad y Justicia de la Unión Europea", DER2009-13679, financiado por el Ministerio de Ciencia e Innovación. El objetivo del proyecto de investigación es examinar la proyección exterior del conjunto del Espacio de Libertad, Seguridad y Justicia. Uno de los ámbitos de investigación prioritaria en la cooperación policial y judicial en materia penal con terceros Estados y, en particular, con los Estados Unidos.

Índice

ISSN: 2174-7628

Abreviaturas

DOUE	Diario Oficial de la Unión Europea
SWIFT	Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales
TFTP	Terrorist Finance Tracking Program
TFUE	Tratado de Funcionamiento de la Unión Europea
TUE	Tratado de la Unión Europea

Resumen

La Unión Europea y los Estados Unidos celebraron en 2010 el Acuerdo entre la Unión Europea y los Estados Unidos 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 (*Terrorist Finance Tracking Program*), conocido como "Acuerdo SWIFT". La entrega de datos relativos a las transferencias financieras es uno de los ámbitos en los que se ha reflejado con más intensidad las distintas perspectivas de los EEUU y de la UE sobre la compatibilidad de algunas de las medidas antiterroristas con la protección de los derechos humanos. En el presente trabajo se examina el contenido del Acuerdo SWIFT con el objetivo de determinar si se ha alcanzado un equilibrio satisfactorio entre la necesidad de proceder a la transferencia de datos de mensajería financiera a los Estados Unidos y la protección de datos personales.

Palabras clave

Transferencia de datos de mensajería financiera - Terrorismo – datos personales – derechos humanos – Acuerdo SWIFT – cooperación policial y judicial en materia penal.

Abstract

The European Union and the United States concluded in 2010 the Agreement on the processing and transfer of financial messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program (*Terrorist Finance Tracking Program*), known as "SWIFT Agreement". The aim of this paper is to examine to what extend the SWIFT Agreement reached the right balance between the need to transfer personal data to the United States in order to fight against terrorism and the obligation to protect personal data.

Key - words

Transfer of financial messaging – Terrorism – personal data- human rights - SWIFT Agreement – Police and judicial cooperation in criminal matters.

1. Introducción

El objetivo del presente trabajo es examinar el proceso de negociación, renegociación y conclusión del Acuerdo entre la Unión Europea y los Estados Unidos 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 (*Terrorist Finance Tracking Program*, en adelante TFTP), conocido como "Acuerdo SWIFT". El Acuerdo entró en vigor el 1 de agosto de 2010 (publicado en el DOUE L 195, de 27.7.2010, p. 1). Se trata de uno de los acuerdos en los que se ha reflejado con más intensidad las distintas perspectivas de los EEUU y de la UE sobre la compatibilidad de algunas de las medidas antiterroristas con la protección de los derechos humanos. La transferencia de los datos de mensajería financiera a los Estados Unidos sigue constituyendo uno de los ámbitos más controvertidos de la cooperación transatlántica en la lucha contra el terrorismo.

El objeto del Acuerdo es establecer un marco jurídico que permita la entrega a los Estados Unidos de los datos de mensajería financiera sobre transferencias financieras almacenados en el territorio de la Unión Europea por los proveedores de servicios de mensajería financiera internacional designados en virtud del propio Acuerdo. Las partes contratantes han determinado que el proveedor internacional de pagos de mensajería financiera designado sea SWIFT. Con fin de limitar los efectos negativos que tiene la entrega masiva de datos, la información proporcionada sólo podrán ser utilizados para luchar contra el terrorismo y su financiación. Asimismo, los Estados Unidos se obligan a poner a disposición de las autoridades europeas responsables del mantenimiento del orden público o de la lucha contra el terrorismo de los Estados miembros, de Europol o de Eurojust de la información obtenida a través del Programa TFTP (artículo 1.1 del Acuerdo). En efecto, el Departamento del Tesoro se compromete a comunicar a las autoridades europeas, responsables del mantenimiento del orden público o de la lucha contra el terrorismo de los Estados miembros, la información obtenida a través del TFTP, que pueda ser de utilidad en la lucha contra el terrorismo (artículo 9 del Acuerdo). Asimismo, en el propio Acuerdo se señala que las autoridades europeas pueden solicitar la realización de búsquedas de información en relación con una persona o entidad que esté relacionada con el terrorismo (artículo 10 del Acuerdo).

La protección de los datos personales ha adquirido una relevancia aún mayor en la UE, tras la entrada en vigor del Tratado de Lisboa. El derecho fundamental a la protección de carácter personal, contemplado en el artículo 8 de la Carta de los Derechos Fundamentales ha adquirido valor jurídico vinculante, y el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE), además de reiterar el derecho a la protección de datos, otorga competencia al Parlamento y al Consejo para establecer "las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos". Sin embargo, como ha criticado el Supervisor Europeo de Protección de Datos, el artículo 16 TFUE no se ha incluido como base jurídica del Acuerdo SWIFT. El Acuerdo SWIFT revisado no sólo pretende facilitar el intercambio de datos personales, sino también garantizar la protección de los datos personales. Por lo tanto, se debería haber incluido, junto a los artículos 82, 87 y 218, el artículo 16 TFUE como fundamento legal.

A continuación, se realizará un examen minucioso del contenido del Acuerdo SWIFT con el objetivo de determinar si ofrece una respuesta satisfactoria a las preocupaciones expresadas por el Parlamento Europeo en relación con el respeto de los derechos y las libertades fundamentales, y si se ha alcanzado un equilibrio satisfactorio entre la necesidad de proceder a la transferencia de mensajería financiera a los Estados Unidos y la protección de datos personales.

2. ¿Por qué la UE ha autorizado la transferencia a los EEUU de los datos de mensajería financiera?

La Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT) es una cooperativa que fue creada en 1973 y es propiedad de sus miembros, que ofrece a escala mundial servicios de mensajería a las entidades financieras. Más de 9000 entidades financieras al día en 209 países utilizan SWIFT para intercambiar datos de mensajería financiera. Tiene su sede principal en Bélgica y cuenta con oficinas en los principales centros financieros y mercados en desarrollo del mundo, incluyendo los

Estados Unidos. Para llevar a cabo sus operaciones, se ha dividido el sistema SWIFT en tres regiones: América, Asia Pacífico y Europa, Oriente y África.

> Tras los atentados del 11 de septiembre de 2011, los Estados Unidos pusieron en marcha el TFTP con el objetivo de luchar contra la financiación del terrorismo. En el contexto de este Programa, el Departamento del Tesoro cursó requerimiento administrativo, entre otros, al centro de SWIFT en Estados Unidos para que le suministrara información relativa a la transferencia de datos de mensajería financiera. El centro operativo de SWIFT en los Estados Unidos tenía unos servidores que almacenaban toda la información de la zona europea de SWIFT, por lo que el Tesoro Norteamericano tuvo acceso a los datos relativos a las transferencias bancarias realizadas por cientos de miles de ciudadanos europeos, dado que los bancos europeos se sirven del sistema de mensajería SWIFT para la transferencia de fondos entre bancos a escala mundial.

En junio de 2006, la prensa reveló la existencia del TFTP y el acceso de forma secreta por parte de la Administración estadounidense a los datos almacenados por SWIFT. La flagrante y masiva violación de la legislación europea en materia de protección de datos y, en particular, la Directiva 95/46 del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de datos personales y a la libre circulación de estos datos (DOUE L 281, de 23.11.1995), así como la legislación de los Estados miembros por la que se aplicaba dicha Directiva, generó una gran controversia en Europa. A finales de 2006, el Grupo de Trabajo del Artículo 29 emitió un dictamen, en el que señalaba que SWIFT vulneraba las normas comunitarias de protección de datos al transferir los datos a los EEUU. El Grupo de Trabajo del Artículo 29 es un órgano consultivo compuesto por un representante de las autoridades de control de los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión. Además de su función consultiva, este órgano contribuye a la aplicación uniforme de las normas de protección de datos de la UE en los Estados miembros.

El Parlamento Europeo expresó también su profunda preocupación por la violación de la legislación comunitaria y nacional de protección de datos. En una Resolución adoptada en 2007, el Parlamento Europeo puso de manifiesto que “las empresas que operan a ambos lados del Atlántico se ven confrontadas cada vez con mayor frecuencia a requisitos jurídicos contradictorios de las jurisdicciones de los EE.UU y la CE”, por lo que solicitaba la celebración de un acuerdo con los Estados Unidos EEUU para poner fin a la incertidumbre legal y proporcionar garantías en materia de protección de datos.

Con el objetivo de poner de manifiesto que no se habían infringido las normas europeas en materia de protección de datos, las autoridades estadounidenses envían en junio de 2007 un memorándum al

Consejo y a la Comisión, en la que se describe el funcionamiento del TFTP y se suscriben una serie de compromisos unilaterales en materia de protección de datos personales respecto de la Unión Europea (el memorándum acordado entre la UE y los EEUU se publicó en el DO C 166/18, 20.7.2007, p. 1). Se señala que el programa TFTP ha demostrado ser un instrumento muy eficaz para luchar contra la financiación del terrorismo. Asimismo, se afirma que la información obtenida de SWIFT se utiliza exclusivamente para investigar delitos de terrorismo o la financiación del terrorismo, de modo que los datos entregados por SWIFT no son objeto de examen para recoger pruebas o detectar actividades que no tengan relación con el terrorismo o su financiación, aunque las propias actividades de que se trate puedan ser ilegales. Finalmente, los Estados Unidos aceptaron el nombramiento de una "personalidad eminente europea", que tendría como misión verificar que el funcionamiento del programa TFTP respeta la legislación de la UE en materia de protección de datos personales. En marzo de 2008, la Comisión nombró al juez francés Jean-Louis Bruguière como "personalidad eminente europea", quién emitió un primer informe en enero de 2009, en el que se concluía que el programa TFTP ha contribuido sustancialmente a la lucha contra el terrorismo y que los Estados miembros de la UE se han beneficiado de sus investigaciones. Asimismo, el juez francés señalo que en el funcionamiento del programa TFTP se respetan los compromisos asumidos por los EEUU en la carta enviada a las autoridades europeas en junio de 2007.

> Para comprender la génesis del Acuerdo entre la Unión Europea y los Estados Unidos relativo al tratamiento y la transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos, a efectos del Programa TFTP, es necesario también hacer referencia a la reestructuración de las plataformas informáticas de SWIFT emprendida en 2007 y culminada a finales de 2009. Tradicionalmente, el centro operativo de SWIFT en los Estados Unidos disponía de una copia por motivos de seguridad de las transferencias realizadas en la zona europea. Del mismo modo, el servidor informático de SWIFT situado en Europa conservaba también una copia de las operaciones de la otra plataforma. La modificación de la estructura de mensajería de SWIFT va a conllevar que las autoridades estadounidenses no van a tener acceso a los datos financieros almacenados en territorio europeo.

A efectos de satisfacer las demandas de las autoridades norteamericanas de seguir disponiendo de la información relativa a los datos europeos de mensajería financiera, se planteó la necesidad de celebrar un acuerdo entre la UE y los Estados Unidos. El 27 de julio de 2009, el Consejo autorizó a la presidencia, asistida por la Comisión, a abrir negociaciones para alcanzar un acuerdo con los EEUU sobre el tratamiento y transferencia de datos de mensajería financiera de la UE, a efectos del Programa TFTP, en el marco de los antiguos artículos 24 y 38 del Tratado de la Unión Europea (TUE). Los cambios introducidos

por SWIFT hicieron que fuera imprescindible la negociación de un acuerdo entre la UE y los EEUU, un acuerdo que exigiría la transferencia de datos por parte de la UE y el cumplimiento de las exigencias de protección de datos. La mayoría de los Estados miembros se mostraron favorables a la negociación del acuerdo SWIFT, no sólo porque querían demostrar su buena voluntad de cooperar con los EE.UU en la lucha contra el terrorismo, sino también porque se han beneficiado de la información obtenida por el programa TFTP.

3. El papel decisivo del Parlamento Europeo en la celebración del Acuerdo SWIFT

El devenir del Acuerdo SWIFT de 2009 va a estar indiscutiblemente ligado a la entrada en vigor del Tratado de Lisboa y a los importantes cambios introducidos en el procedimiento de adopción de decisiones en el ámbito del Espacio de libertad, seguridad y justicia. Se propuso que el acuerdo SWIFT fuera negociado y concluido en el marco del antiguo tercer pilar, en el que se atribuía un rol marginal al Parlamento Europeo en la celebración de tratados internacionales. En cambio, tras la entrada en vigor del Tratado de Lisboa es necesario recabar la previa aprobación del Parlamento Europeo para poder celebrar acuerdos internacionales en todas las materias relativas a la cooperación policial y judicial en materia penal. Así, el artículo 218.6 a) TFUE prevé que los acuerdos internacionales que se refieran a ámbitos en los que se aplique el procedimiento legislativo ordinario para la adopción de los actos internos, tal y como sucede en presente caso, es necesario obtener la previa aprobación del Parlamento.

Por esta razón, el Parlamento comienza a mostrar sus nuevas atribuciones durante el proceso de negociación del acuerdo SWIFT, aun cuando no estaban despejadas todas las incertidumbres que se cernían sobre la entrada en vigor del Tratado de Lisboa. Así, el 17 de septiembre de 2009, el Parlamento Europeo adoptó una resolución sobre el acuerdo propuesto. Aunque el Parlamento Europeo reconocía la importancia del acuerdo en la lucha contra el terrorismo, señaló también que era necesario “lograr un

equilibrio entre las medidas de seguridad y la protección de las libertades públicas y los derechos fundamentales, garantizando a la vez el máximo respeto por la protección de datos y la privacidad" (DOUE C 224 E/8, de 19.8.2010).

Sin tener en cuenta las reivindicaciones del Parlamento, el Consejo autorizó a la Presidencia a firmar el acuerdo interino de transferencia de datos de mensajería financiera entre los Estados Unidos y la UE el 30 de noviembre de 2009, esto es, un día antes de que entrara en vigor el Tratado de Lisboa, a reserva de su celebración en una fecha posterior (DOUE L 8, de 13.1.2010, p. 9). El acuerdo se aplicaría provisionalmente a partir del 1 de febrero de 2010, a la espera de su entrada en vigor, y tendría una duración máxima de nueve meses, pues estaba destinado a ser remplazado en su momento por un acuerdo a largo plazo. Asimismo, el 17 de diciembre de 2009, la Comisión presentó una propuesta al Consejo relativa a la celebración del Acuerdo entre la Unión Europea y los Estados Unidos sobre el tratamiento y transferencia de datos de mensajería financiera de la Unión Europea a efectos del TFTP.

> La necesidad de recabar la aprobación del Parlamento Europeo para poder celebrar el Acuerdo SWIFT fue aprovechada por el Parlamento para poner en práctica las nuevas prerrogativas otorgadas por el Tratado de Lisboa (SANTOS VARA, J., p. 359). En febrero de 2010, el Parlamento aprueba el informe de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior, en el que deniega su aprobación a la celebración del Acuerdo. Si bien el Parlamento reconoce la importancia de la cooperación transatlántica en la lucha contra el terrorismo, se afirma que el programa TFTP "debe ser considerado una desviación de la legislación y la práctica europeas en cuanto a cómo obtendrían los organismos policiales y judiciales los datos financieros de los individuos para las actividades policiales y judiciales, concretamente el recurso a órdenes judiciales o requerimientos aprobados por los tribunales para examinar transacciones específicas en lugar de basarse en requerimientos administrativos amplios para millones de registros".

Por ello, el Parlamento expresó su preocupación por la transferencia masiva de datos, la no intervención de las autoridades judiciales, la ausencia de control en relación con la transferencia futuras por los Estados Unidos a terceros países, la falta de información sobre el periodo en el que se conservan los datos, la inexistencia de un sistema de protección de los individuos y empresas europeas a las que se refieran los datos y la falta de una auténtica reciprocidad.

Ante la alarma generada por el posible rechazo del Acuerdo interino, la administración estadounidense trató de presionar al más alto nivel al Parlamento en los días anteriores a la votación (Vid. MONAR, J., p. 145). También la presidencia española del Consejo trató de convencer al Parlamento hasta el último momento de la necesidad de celebrar el Acuerdo, poniendo de manifiesto que se le otorgaría acceso

pleno a la información en la negociación del acuerdo permanente (EUROPEAN VOICE). Finalmente, a pesar de las garantías ofrecidas, el Parlamento Europeo rechazo el 10 de febrero de 2010 la celebración del Acuerdo. La consecuencia obvia fue que no era posible continuar con la aplicación provisional y la presidencia del Consejo tuvo que comunicar a las autoridades de los EEUU que no podía convertirse en parte contratante del Acuerdo interino.

El rechazo del Parlamento Europeo al primer Acuerdo SWIFT no supuso eliminar completamente las posibilidades de acceder a los datos de mensajería financiera de la Unión Europea. En efecto, el Acuerdo de Asistencia Judicial entre la Unión Europea y los Estados Unidos de América de 2003, que entró en vigor el 1 de febrero de 2010, introduce un mecanismo para facilitar el intercambio de datos relativos a las transferencias financieras. En virtud del artículo 4 del Acuerdo de 2003, una parte contratante puede solicitar a otro Estado parte si una persona física o jurídica sospechosa o acusada de una infracción penal es titular de una o varias cuentas bancarias y solicitarle detalles sobre sus transferencias financieras. Sin embargo, el Acuerdo de 2003 no posibilita la transferencia de forma masiva de datos de mensajería financiera. También seguían subsistiendo los acuerdos de asistencia judicial celebrados entre los Estados Unidos y cada uno de los Estados miembros de la UE.

Ante la delicada situación generada por el rechazo del Parlamento, la Comisión y el Consejo reaccionaron con gran rapidez. El 24 de marzo de 2010, la Comisión propuso un nuevo mandato de negociaciones que fue adoptado por el Consejo el 11 de mayo de 2010, comprometiéndose a consultar plenamente al Parlamento durante todo el proceso de negociaciones. El 5 de mayo de 2010, el Parlamento Europeo adoptó una Resolución sobre la recomendación de la Comisión al Consejo de autorizar el inicio de las negociaciones de un nuevo acuerdo sobre la transferencia de datos de mensajería financiera a los Estados Unidos, en la que "se felicita por el nuevo espíritu de cooperación demostrado por la Comisión y el Consejo y por su voluntad de hacer participar al Parlamento, teniendo en cuenta sus obligaciones en virtud del Tratado de mantenerle informado de forma inmediata y plena en todas las etapas del procedimiento". Asimismo, el Parlamento reitera que la transferencia de datos en masa no es coherente con los principios en los que se basa la legislación y la práctica de la UE y recomienda que se encargue a una "autoridad pública judicial en la UE" la responsabilidad de recibir las solicitudes del Departamento del Tesoro de los Estados Unidos.

Finalmente, las negociaciones concluyeron el 11 de junio de 2011 y el 28 de junio del mismo se firmó el Acuerdo. El Parlamento Europeo dio su aprobación al tratado revisado el 8 de julio de 2010, lo que

permitió al Consejo celebrar el 13 de julio de 2010 el Acuerdo sobre el tratamiento y la transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos a efectos del TFTP. El Acuerdo entró en vigor el 1 de agosto de 2010. No cabe duda que el cambio de opinión del Parlamento Europeo en relación con el Acuerdo se debe tanto a las mejoras introducidas en el contenido del mismo, de las que se dará cuenta a continuación, como al hecho de que en esta ocasión se informó y proporcionó al Parlamento la posibilidad de participar activamente en el proceso de negociaciones (CREMONA, p. 25)

4. Características del Acuerdo SWIFT de 2010

4.1 El procedimiento a seguir por parte de los EEUU para obtener datos de los proveedores designados

El procedimiento para la obtención por parte de las autoridades estadounidenses de datos de los proveedores designados se articula en torno a una doble fase. En primer lugar, el Departamento del Tesoro de los Estados Unidos solicitará al proveedor designado que se encuentre en el territorio de los 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 identificar de la forma más clara posible los datos, motivar claramente la necesidad de los datos, circunscribir claramente la cantidad de datos requeridos, quedando en todo caso al margen del Acuerdo los datos sobre el espacio único de pagos en euros. Sin embargo, estas limitaciones no van a evitar la transferencia de forma masiva de datos personales a las autoridades estadounidenses. Los datos se transfieren en función de categorías de datos pertinentes y no de forma individualizada en relación con una o varias personas, pues SWIFT no dispone de los instrumentos informáticos necesarios para proceder a realizar búsquedas y análisis específicos. Además, el programa TFTP no puede funcionar de forma efectiva sin la entrega masiva de

datos, pues no es posible predecir con antelación que parte de los datos serán necesarios para llevar a cabo una investigación terrorista.

> A partir de los datos transferidos en masa se pueden obtener los datos requeridos para luchar contra el terrorismo, como por ejemplo nombres, direcciones y/o números de facturas relativos a personas individuales. En estas circunstancias, la transferencia de datos de mensajería financiera a los Estados Unidos constituye una vulneración de los principios fundamentales en los que se basa la legislación de la UE en materia de protección de datos, a saber, los principios de necesidad y de proporcionalidad.

En segundo lugar, el Departamento del Tesoro ha de enviar a Europol una copia de la solicitud, quien habrá de comprobar que la solicitud cumple los requisitos exigidos por el Acuerdo. Una vez que Europol haya comprobado el vínculo de los datos de mensajería financiera con el terrorismo, la solicitud tendrá los efectos jurídicos vinculantes previstos en la legislación de los Estados Unidos, tanto en la UE como en los Estados Unidos. A partir de ese momento, "el proveedor designado queda autorizado para facilitar y debe facilitar los datos al Departamento del Tesoro de los EEUU", conforme a un sistema de transmisión *push*, que es el mismo que se utiliza para la entrega de los datos de los pasajeros de vuelos con destino o que hacen escala en los Estados Unidos. Por lo tanto, no se ha atribuido a una autoridad judicial la función de recibir las solicitudes de las autoridades estadounidenses para evaluar el cumplimiento del Acuerdo, tal y como había exigido reiteradamente el Parlamento Europeo y se había previsto en el mandato de negociación. Es evidente que Europol no es una autoridad judicial. Además, el cumplimiento de este mandato puede entrar en contradicción con las funciones asignadas en la Decisión de creación de esta agencia de la UE e incluso con las previsiones incluidas en el propio Acuerdo. En efecto, en el artículo 10 del Acuerdo se prevé que Europol podrá solicitar información obtenida a través del Programa TFTP si considera que una persona o entidad está relacionada con el terrorismo. A este respecto, el Supervisor Europeo de Protección de Datos ha señalado el 29 de diciembre de 2010 que "resulta difícil conciliar esta facultad de Europol, que puede ser importante para el cumplimiento de la función de Europol, y que requiere mantener buenas relaciones con el Tesoro de los Estados Unidos, con la función de Europol de asegurar una supervisión independiente" Asimismo, se debe resaltar que no se contempla expresamente en el propio Acuerdo la posibilidad de que Europol rechace la entrega de los datos requeridos por los Estados Unidos.

4.2 Salvaguardias aplicables al tratamiento de los datos facilitados

El Departamento del Tesoro de los Estados Unidos se compromete a garantizar que el tratamiento de los datos de mensajería financiera se lleva a cabo de conformidad con lo previsto en el texto del Acuerdo. Por ello, "los datos facilitados se tratarán exclusivamente a efectos de prevenir, investigar, detectar o perseguir el terrorismo o su financiación", sin discriminación, en particular, por motivos de nacionalidad o de país de residencia (artículo 5 del Acuerdo).

Para garantizar la seguridad e integridad de los datos, se prevé expresamente en el texto del Acuerdo que: los datos facilitados se conservarán en un entorno físico seguro y no se interconectarán con otras bases de datos, se ha de limitar el acceso a los datos a los analistas dedicados a la investigación del terrorismo, no se podrán modificar o manipular los datos facilitados y no se podrán realizar copias de los datos facilitados.

> En aras de lograr un tratamiento proporcionado de los datos se especifica en el Acuerdo que toda búsqueda de los datos facilitados se ha de basar en información y pruebas existentes previamente que demuestren que existen motivos para creer que el objeto de la investigación tiene una relación con el terrorismo o su financiación. En el Acuerdo se presta especial atención al tratamiento de los datos sensibles. Se señala que los datos facilitados, además de identificar al emisor o al destinatario de una transacción (nombre y apellidos, el número de cuenta, la dirección y el número de identificación nacional) podrán referirse también a datos sensibles que muestran el origen étnico o racial, la opiniones políticas y religiosas u otras creencias, la pertenencia a un sindicato, o la salud y la vida sexual.

En el caso de que se faciliten datos sensibles, el Departamento del Tesoro "protegerá dichos datos de conformidad con las salvaguardias y medidas de seguridad establecidas en el presente Acuerdo, dentro del mayor respeto y teniendo debidamente en cuenta su carácter particularmente sensible" (artículo 5 del Acuerdo).

> Si bien se contempla la puesta a disposición de las autoridades norteamericanas de los datos sensibles con carácter excepcional, es indudable que la entrega de este tipo de datos puede constituir una grave intromisión en la esfera más íntima de las personas, vulnerando de forma flagrante la protección que proporcionan el artículo 8 de la Carta de los Derechos Fundamentales y el artículo 16 del TFUE (vid. en este sentido también ESCRIBANO ÚBEDA-PORTUGUÉS, J., p. 9).

La existencia de mecanismos de supervisión independiente es un elemento fundamental del derecho a la protección de datos personales, tal y como se prevé en el artículo 16 TFUE y en el artículo 8 de la Carta de los Derechos Fundamentales. Las búsquedas realizadas por las autoridades estadounidenses serán objeto de seguimiento en tiempo real y de forma retrospectiva por supervisores independientes, incluida una persona designada por la Comisión Europea. A los supervisores independientes se les otorga la facultad de suspender alguna o la totalidad de las búsquedas que infrinjan la exigencia de estar relacionadas con el terrorismo o su financiación. Sin embargo, el Acuerdo de 2010 ha supuesto un retroceso respecto al Acuerdo de 2009 en relación con las competencias de las autoridades europeas de protección de datos. En el Acuerdo anterior se preveía que "el presente Acuerdo no menoscaba los poderes existentes de las autoridades de protección de datos de los Estados miembros para proteger a las personas en relación el tratamiento de sus datos personales". En cambio, el Acuerdo de 2010 se refiere a la supervisión de las autoridades competentes de protección de datos y en consonancia con las disposiciones específicas del presente Acuerdo, lo que supone claramente limitar los poderes de las autoridades europeas de protección de datos.

4.3La protección de los derechos de las personas afectadas

En relación con la conservación y supresión de los datos facilitados, se prevé que las autoridades estadounidenses realizarán una evaluación continua y al menos una vez al año, con el objetivo de identificar los datos que no sean ya necesarios para luchar contra el terrorismo, procediéndose a su supresión definitiva. Si bien es preciso reconocer que, en algunos casos, resulta necesario conservar los datos por largos períodos de tiempo para llevar a cabo investigaciones que se prolongan durante mucho tiempo, la conservación sistemática de los datos facilitados antes del 20 de julio de 2007, por un período que puede llegar hasta los cinco años, puede ser excesiva. Como ha señalado el Supervisor Europeo de Protección de Datos, dado que se trata de datos que se han transferido de forma masiva y no han sido utilizados en relación con una investigación específica, el período de almacenamiento de estos datos debería ser mucho más limitado.

En los artículos 14 a 18 del Acuerdo se establece una serie de derechos de los interesados, como el derecho a ser informado, el derecho de acceso, el derecho de rectificación, supresión o bloqueo, así como el derecho de reparación. En relación con la información que se ha de facilitar a los interesados, se prevé que el Departamento del Tesoro publicará en su sitio web oficial información detallada sobre el TFTP y sus objetivos, debiéndose incluir información sobre los recursos administrativos y judiciales disponibles en los Estados Unidos en relación con el tratamiento de los datos personales recibidos. En cumplimiento de esta previsión, el Departamento del Tesoro de los Estados Unidos ha creado un página web específica, en la que se incluye información de carácter general sobre el sistema TFTP, disponible en http://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Pages/tftp.aspx (consultado el 12 de septiembre de 2012).

Por loque se refiere al derecho de acceso a los propios datos personales, el Acuerdo señala que cualquier persona podrá solicitar a su autoridad responsable de la protección en la Unión Europea, que le confirme si se han llevado a cabo las comprobaciones necesarias para verificar que se han respetado sus derechos en materia de protección de datos, de conformidad con lo previsto en el Acuerdo. Es lógico que, en el contexto de la lucha contra el terrorismo, puedan establecerse limitaciones a los derechos del interesado. Así, se prevé que la revelación a una persona de sus datos personales podrá limitarse en las circunstancias que prevea la legislación nacional "para salvaguardar la prevención, detección, investigación o persecución de delitos, así como para proteger el orden público o la seguridad nacional, teniendo debidamente en cuenta los intereses legítimos del interesado" (articulo 15 del acuerdo). La solicitud presentada por el interesado ante la autoridad nacional de control será enviada al responsable de la protección de la privacidad del Departamento del Tesoro, quien informará a la autoridad remitente si los datos personales pueden ser revelados al interesado y si los derechos de éste han sido debidamente respetados. En el caso de que se deniegue o limite el acceso a los datos personales, la decisión se ha de motivar por escrito y facilitar información sobre las vías de recurso administrativo o judicial disponibles en los Estados Unidos.

Es lamentable que no se prevea en el Acuerdo la posibilidad de revelar la información a las autoridades europeas de protección de datos en todos los casos a fin de que puedan cumplir efectivamente las funciones de supervisión encomendadas. Esta situación nos muestra la desconfianza de las autoridades estadounidenses hacia los sistemas de protección de datos

cuando se trata de información que es utilizada para luchar contra el terrorismo o su financiación.

Asimismo, cualquier persona podrá solicitar la rectificación, la supresión o el bloqueo de sus datos personales cuando sean inexactos o su tratamiento infrinja el Acuerdo. El procedimiento a seguir es idéntico al previsto en relación con el derecho de acceso. Además, "siempre que sea posible, la Parte que haya tenido conocimiento de que, con arreglo al presente Acuerdo, se ha transmitido a la otra Parte o se ha recibido de la misma, información significativa inexacta o no fiable, lo notificará a la otra Parte" (artículo 16.2 del acuerdo). A este respecto, el Supervisor Europeo de Protección de Datos ha puesto claramente de manifiesto la importancia de establecer mecanismos que permitan dicha rectificación en todo caso, pues se trata de una cuestión que no sólo afecta a la persona interesada, sino también a la eficacia de las fuerzas y cuerpos de seguridad en la lucha contra la lacra del terrorismo.

En cuanto al derecho a la reparación del daño causado, cualquier persona que estime que se han tratado sus datos sin respetar lo dispuesto en el Acuerdo podrá solicitar su reparación por la vía administrativa y judicial en el marco de la legislación de la UE, sus Estados miembros y los Estados Unidos. El procedimiento a seguir para exigir el respeto del derecho a la reparación, así como el resto de los derechos examinados anteriormente, presenta una gran incertidumbre, pues el Acuerdo se limita a remitirse a la legislación de la UE, sus Estados miembros y de los Estados Unidos.

En el artículo 20 del Acuerdo se ha introducido una previsión muy llamativa en relación con los derechos de las personas interesadas, que podría mermar, o incluso anular, la eficacia práctica de la protección que proporcionan las cláusulas anteriormente analizadas. Se señala que el Acuerdo "no generará ni conferirá derecho ni beneficio alguno a ninguna otra persona o entidad, pública o privada". De este modo, esta disposición podría conducir a poner en cuestión el efecto vinculante de los derechos de los interesados que no estén también reconocidos en virtud de la legislación de los Estados Unidos.

4.4 La transferencia ulterior de los datos a terceros Estados

Como se ha señalado anteriormente, la información obtenida a través del Programa TFTP sólo se compartirá con las fuerzas y cuerpos de seguridad, las autoridades responsables del mantenimiento del orden público o de la lucha contra el terrorismo de los Estados Unidos, los Estados miembros, o con los terceros países, o con Europol o Eurojust, o con otros organismos internacionales que tengan competencias en la lucha contra el terrorismo y su financiación.

Cuando la información obtenida afecte a un ciudadano o residente de un Estado miembro, se han introducido en el Acuerdo una serie de cautelas destinadas a protegerles, que, como se pondrá de manifiesto a continuación, no proporcionan una protección real. En principio, la transferencia ulterior a las autoridades de un tercer país estará supeditada al consentimiento previo del Estado miembro en cuestión o a lo dispuesto en los protocolos vigentes sobre el hecho de compartir dicha información entre el Departamento del Tesoro y ese Estado miembro. Sin embargo, se introduce una excepción en virtud de la cual no es preciso obtener el consentimiento previo del Estado afectado "si el compartir datos es esencial para la prevención de una amenaza grave e inmediata contra la seguridad pública de una Parte del presente Acuerdo, un Estado miembro o un tercer país" (artículo 7 del acuerdo). En consecuencia, las autoridades de los Estados Unidos podrán valorar libremente cuando concurren estas circunstancias, estando únicamente obligadas a informar a la mayor brevedad posible al Estado miembro interesado.

5. Conclusiones

Todas las instituciones europeas, incluido el Parlamento Europeo, y los actores implicados en el proceso de celebración del Acuerdo SWIFT coinciden en admitir la significativa aportación del programa TFTP en la lucha contra el terrorismo y su financiación, de la que se han beneficiado también las autoridades de los Estados miembros de la Unión Europea. Sin embargo, la transferencia de forma masiva de datos de mensajería financiera ha dado lugar a un intenso debate en relación con sus efectos sobre los derechos fundamentales de los ciudadanos europeos, debate que, en modo alguno, se puede considerar cerrado.

Es preciso señalar que la gran mayoría de los datos transferidos se refieren a personas que no tienen nada que ver con la financiación del terrorismo, pues no parece posible actualmente evitar las transferencias de datos de forma masiva. Así, debido a que SWIFT no dispone de los equipos técnicos necesarios para llevar a cabo búsquedas específicas de datos personales, el Acuerdo se basa en la transferencia masiva de datos personales a las autoridades norteamericanas, lo que resulta difícilmente compatible con los principios de necesidad y proporcionalidad.

Por ello, es imperioso encontrar soluciones lo antes posible, que permitan filtrar los datos de mensajería financiera en la UE, de forma que sólo se envíen a las autoridades de los Estados Unidos los datos necesarios. Un paso en la buena dirección sería el desarrollo de un sistema equivalente al TFTP en la UE. A petición del propio Parlamento, el Consejo se ha comprometido en la misma Decisión de celebración del Acuerdo SWIFT a establecer el marco jurídico y técnico que permita en el futuro la extracción de datos en la UE. El desarrollo de un sistema equivalente al TFTP en la UE eliminaría la necesidad de proceder a transferencias masivas de datos, pues las autoridades europeas serían capaces de responder a solicitudes específicas de datos, tal y como hacen las autoridades estadounidenses en relación con las solicitudes europeas. Incluso, en el propio Acuerdo SWIFT se prevé que, durante la vigencia del mismo, la Comisión Europea realizará un estudio sobre la posible introducción de un sistema equivalente en la UE que permita una transferencia más selectiva de los datos (artículo 11 del Acuerdo).

Los Estados Unidos se han comprometido en el propio Acuerdo a cooperar y prestar asistencia en el establecimiento de dicho sistema. Al mismo tiempo, es preciso garantizar la complementariedad y la eficiencia de ambos sistemas en su operatividad práctica. A mediados de julio de 2011, la Comisión presentó un estudio preliminar sobre las distintas opciones existentes para desarrollar su propio sistema TFTP. El sistema europeo de seguimiento de la financiación del terrorismo tendría dos objetivos principales: contribuir a la lucha contra la financiación del terrorismo dentro de la UE y reducir significativamente el volumen de datos transferidos a los Estados Unidos. No está claro aun cuando se podrá en marcha este proyecto. Mientras tanto, los ciudadanos europeos tendremos que resignarnos a aceptar la vulneración de nuestro derecho a la protección de datos personales, protegido por el artículo 8 de la Carta de los Derechos Fundamentales y el artículo 16 del TUE. Si el futuro sistema europeo se sigue basando en la extracción en forma masiva de datos de mensajería financiera, sin estar sometido a las

garantías y controles judiciales adecuados, seguirá presentando serías incertidumbres en relación con la protección de los datos personales.

Este tema forma parte de una cuestión más amplia que versa sobre la transferencia de datos personales entre la Unión Europea y los Estados Unidos en el marco de la lucha contra el terrorismo y el crimen organizado, y sus implicaciones para la protección de los derechos fundamentales. La regulación de la protección de datos en las transferencias de información a terceros países en el ámbito de la cooperación policial y judicial en materia penal presenta aún claras limitaciones. Ciertamente, no es fácil lograr un acomodo satisfactorio entre la necesidad de luchar contra el terrorismo y su financiación, valiéndose de todos los medios técnicos disponibles, y el respeto del derecho a la protección de los datos personales. Sin embargo, del análisis de la génesis y el contenido del Acuerdo SWIFT se deduce claramente que se sigue dando prioridad a la seguridad sobre la protección de los derechos fundamentales.

6. Bibliografía

CREMONA, M.: "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, Austrian Academy of Sciences,* Working Paper Nº 04/2011.

ESCRIBANO ÚBEDA-PORTUGUÉS, J.: "El refuerzo de los mecanismos de cooperación entre la Unión Europea y los Estados Unidos en el ámbito del tratamiento y la transferencia de datos de mensajería financiera de la UE a Estados Unidos en materia de lucha contra la financiación del terrorismo", *Revista General de Derecho Europeo*, 2011, nº 3.

EUROPEAN VOICE, "New Offer to Save EU-US Data Deal", 9 de febrero de 2010.

MONAR, J.: "The Rejection of the EU-US SWIFT Interim Agreement by the European Parliament: A Historic Vote and Its Implications", *European Foreign Affairs Review*, 2010, vol. 15.

SANTOS VARA, J.: "The External Dimension of the Area of Freedom, Security and Justice in the Lisbon Treaty", *European Journal of Law Reform*, 2008 vol. 10, nº 4, pp. 557-598.

SANTOS VARA, J.: "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*, Ed. Iustel, Madrid, 2012, pp. 351-376.

Fuentes documentales y legislativas:

Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Decisión del Consejo, relativa a la celebración del Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el 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, DOUE C 355, de 29.12.2010, p. 10.

Directiva 95/46 del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de datos personales y a la libre circulación de estos datos, DOUE L 281, de 23.11.1995.

Resolución del Parlamento Europeo sobre SWIFT, el acuerdo PNR y el diálogo trasatlántico sobre estas cuestiones, DOUE C 287E, 29.11.2007, p. 349.

Resolución del Parlamento Europeo, de 17 de septiembre de 2009, sobre el acuerdo internacional previsto para poner a disposición del Departamento del Tesoro de los Estados Unidos datos de mensajería financiera sobre pagos con un fin de prevención y lucha contra el terrorismo y la financiación del terrorismo, P7_TA(2009)0016, DOUE C 224 E/8, de 19.8.2010.

Decisión del Consejo 2010/16/PESC/JAI del Consejo, de 30 de noviembre de 2009, relativa a la firma, en nombre de la Unión Europea, 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, DOUE L 8, de 13.1.2010, p. 9.

Resolución legislativa del Parlamento Europeo, de 11 de febrero de 2010, sobre la propuesta de Decisión del Consejo relativa a la celebración del Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el 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 (05305/1/2010 REV 1– C7-0004/2010 – 2009/0190(NLE)).

Resolución del Parlamento Europeo, de 5 de mayo de 2010, sobre la Recomendación de la Comisión al Consejo de autorizar el inicio de las negociaciones relativas a un Acuerdo entre la Unión Europea y los Estados Unidos de América para poner a disposición del Departamento del Tesoro de los Estados Unidos datos de mensajería financiera con el fin de prevenir y luchar contra el terrorismo y la financiación del terrorismo, P7_TA (2010)0143.

Decisión del Consejo de 28 de junio de 2010 relativa a la firma 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, DOUE L 195, de 27.7.2010, p. 1.

Resolución legislativa del Parlamento Europeo, de 8 de julio de 2010, sobre la propuesta de Decisión del Consejo relativa a la celebración del Acuerdo entre la Unión Europea y los Estados Unidos de América relativo al tratamiento y la transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos a efectos del Programa de Seguimiento de la Financiación del Terrorismo (11222/1/2010/REV 1 y COR 1 – C7-0158/2010 – 2010/0178(NLE)).

Decisión del Consejo de 13 de julio de 2010 relativa a la celebración del Acuerdo entre la Unión Europea y los Estados Unidos de América relativo al tratamiento y la transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos a efectos del Programa de Seguimiento de la Financiación del Terrorismo, DO L 195, de 27.7.2010, p. 3.

Decisión del Consejo de 6 de abril de 2009 por la que se crea la que se crea la Oficina Europea de Policía (Europol), *DO* n.º L 121, de 15.5.2009, p. 37.

Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Decisión del Consejo relativa a la celebración del Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el 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, DO C 355, de 29.12.2010, p. 10.

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones - Sistema europeo de seguimiento de la financiación del terrorismo: posibles opciones, COM (2011) 429 final, 13.7.2011