(Traducción)

Tratamiento de los datos personales procedentes de la UE por el Departamento del Tesoro de Estados Unidos a efectos de la lucha contra el terrorismo — «SWIFT»

(2007/C 166/09)

Programa de seguimiento de la financiación del terrorismo — Declaraciones Departamento del Tesoro de Estados Unidos

En las presentes declaraciones se describe el Programa de seguimiento de la financiación del terrorismo («Terrorist Finance Tracking Program») (TFTP) del Departamento del Tesoro de Estados Unidos y, en particular, los rigurosos controles y garantías aplicables al tratamiento, utilización y difusión de los datos recibidos de SWIFT en ejecución de requerimientos administrativos. Los citados controles y garantías se aplican a todas las personas que tengan acceso a los datos entregados por SWIFT, a menos que se indique otra cosa en los ejemplos específicos, tales como al compartir con gobiernos extranjeros información sobre pistas procedentes de datos obtenidos de SWIFT.

El programa TFTP se basa en la legalidad, tiene objetivos específicos, es efectivo y respeta la normativa impuesta en materia de privacidad. El TFTP representa lo que los ciudadanos esperan exactamente que hagan sus gobiernos para protegerlos de las amenazas terroristas.

Programa de seguimiento de la financiación del terrorismo del Departamento del Tesoro

Poco después de los atentados del 11 de septiembre de 2001 el Departamento del Tesoro inició el programa TFTP, que forma parte del esfuerzo general por perseguir a los terroristas y sus redes utilizando todos los medios disponibles. En el marco del TFTP el Departamento del Tesoro cursó requerimiento administrativo de notificación de datos relacionados con el terrorismo al centro operativo en EEUU de la «Society for Worldwide Interbank Financial Telecommunication» («SWIFT»), una empresa belga que cuenta con un sistema de mensajería que opera en todo el mundo utilizado para la transmisión de información relacionada con operaciones financieras. Mediante dicho requerimiento administrativo se exigía a SWIFT que facilitara al Departamento del Tesoro determinados datos de operaciones financieras — en posesión del centro operativo de SWIFT en EEUU en circunstancias normales de funcionamiento — que se utilizarían exclusivamente con una finalidad antiterrorista, tal como se precisa en las siguientes secciones.

Principios fundamentales en los que se basa el programa TFTP

Desde su inicio, el programa TFTP ha sido concebido y se aplica respetando los requisitos legales aplicables en Estados Unidos, con el fin de contribuir de manera significativa a la lucha contra el terrorismo y respetar y proteger la posible sensibilidad comercial y los intereses de privacidad en relación con los datos procedentes de SWIFT en posesión de Estados Unidos. El programa TFTP tiene en cuenta la posible sensibilidad comercial y los intereses de privacidad de las personas en la información correspondiente; las garantías ofrecidas en estas declaraciones se ofrecen independientemente de la nacionalidad o lugar de residencia de las personas. El programa contiene múltiples capas de control, que se superponen unas a otras, a nivel gubernamental e independiente, con el fin de garantizar que el examen de los datos, que por naturaleza son limitados, se realiza únicamente a efectos de la lucha contra el terrorismo y que todos los datos se conservan en un entorno seguro y reciben un tratamiento adecuado.

Todas las actuaciones del Departamento del Tesoro en el sentido de obtener información específica del centro operativo de SWIFT en EEUU y de utilizar esta información exclusivamente para investigar, detectar, prevenir o perseguir delitos de terrorismo o la financiación del terrorismo o las investigaciones y procedimientos relacionados con el terrorismo se llevan a cabo respetando la legislación estadounidense. Más aún, 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. El Departamento del Tesoro no examina los datos proporcionados por SWIFT, ni utiliza la información correspondiente en relación con investigaciones generales en el ámbito de la evasión fiscal, el blanqueo de dinero, el espionaje económico, el tráfico de drogas o demás actividades delictivas, a menos que en un caso determinado se trate de una actividad que haya tenido relación con el terrorismo o su financiación.

Los datos recibidos de SWIFT en ejecución de requerimientos administrativos consisten en copias de mensajes completos de operaciones financieras, a saber, copias electrónicas de registros de operaciones en posesión del centro operativo de SWIFT en EEUU en circunstancias normales de funcionamiento. Aunque estos datos pueden ser objeto de algún tipo de tratamiento en el sentido de una capacidad muy limitada de búsqueda y recuperación con fines antiterroristas, tal como aquí se describe, en la base de datos de búsqueda no se modifican, ni se manipulan, ni se añaden o suprimen datos de los mensajes de cada una de las operaciones.

El programa TFTP ha demostrado ser un instrumento eficaz de investigación que ha contribuido significativamente a la protección de ciudadanos estadounidenses y de todo el mundo y a la protección de la seguridad nacional de América y de otros países. El papel del programa ha sido decisivo para identificar y capturar a terroristas y a sus mecenas, y ha desvelado muchas pistas que han sido difundidas a expertos antiterroristas de servicios de inteligencia y cuerpos y fuerzas de seguridad del Estado de todo el mundo.

Preocupaciones expresadas por la Unión Europea

Al desvelar la prensa en junio de 2006 la existencia del programa TFTP, la noticia suscitó preocupación en la UE y, en particular, la posibilidad de que el Departamento del Tesoro pudiera tener acceso a datos personales en relación con personas físicas identificadas o identificables que figuraran en operaciones financieras procesadas por SWIFT. En particular, se planteó la cuestión de la compatibilidad del programa TFTP con las obligaciones existentes derivadas de la Directiva de protección de datos (Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos), así como de las normativas de los Estados miembros que aplican la Directiva.

Naturaleza de los datos de SWIFT

Los registros de operaciones financieras facilitados por SWIFT por requerimiento administrativo pueden incluir información por la que se identifique al ordenante y/o al destinatario de la operación, incluido el nombre, número de cuenta, dirección, número de documento nacional de identificación y otros datos personales. Sería bastante extraño que los registros financieros de SWIFT incluyeran datos «sensibles» tales como los que se contemplan en el artículo 8 de la Directiva 95/46/CE (a saber, datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como datos relativos a la salud o a la sexualidad).

Principios aplicados a nivel internacional contra la financiación del terrorismo

Los datos financieros entregados por SWIFT que utiliza el programa TFTP resultan extremadamente valiosos en la lucha global contra el terrorismo y su financiación, así como en la ejecución de la responsabilidad gubernamental de defensa pública y protección de la seguridad nacional y para detectar, prevenir, investigar y perseguir delitos terroristas.

La comunidad internacional y las autoridades nacionales reconocen que el dinero forma parte vital del terrorismo. Así lo recoge el Convenio Internacional de las Naciones Unidas para la Represión de la Financiación del Terrorismo, de 1999, y numerosas resoluciones de Naciones Unidas en relación con la prevención y represión de la financiación de actos terroristas, en particular, la Resolución nº 1373 del Consejo de Seguridad de las Naciones Unidas. En Estados Unidos, el Departamento del Tesoro y el Congreso establecieron en 2004 la Oficina de Terrorismo e Inteligencia Financiera con el fin de reunir las funciones ejecutiva y de inteligencia del Departamento con el doble objetivo de proteger el sistema financiero contra el uso ilícito y luchar, entre otras cosas, contra los terroristas y demás amenazas contra la seguridad nacional. Las distintas partes de la Oficina recopilan y analizan información de organismos de represión, inteligencia y financieros en relación con la forma de recaudar, transferir y guardar el dinero por los terroristas (y otros delincuentes). Gracias a estas actividades la Oficina puede congelar activos de terroristas, combatir el terrorismo en general y elaborar y promover normas en el ámbito de la lucha contra la financiación del terrorismo en Estados Unidos y en el extranjero.

Estas y otras iniciativas reflejan la realidad cotidiana, a saber, que los terroristas deben contar con liquidez para financiar las operaciones, viajar, entrenar a nuevos miembros, falsificar documentos, sobornar, comprar armas y preparar atentados. Al remitir dinero a través del sistema bancario, ofrecen a menudo información que revela tipos de pistas específicas que pueden hacer avanzar una investigación en el ámbito de la lucha contra el terrorismo. Por este motivo los expertos en la lucha contra el terrorismo conceden gran importancia a la inteligencia financiera, incluida la que resulta de programas tales como TFTP, que ha demostrado tener un valor incalculable en la lucha contra el terrorismo global.

Por este motivo también se está sometiendo cada vez más al sector financiero a la obligación de registrar la información y notificarla, con el fin de apoyar los esfuerzos del gobierno en la lucha contra el terrorismo. Países de todo el mundo han establecido esta obligación mediante ley, lo que es coherente con las recomendaciones del Grupo de Acción Financiera Internacional. Por ejemplo, en Estados Unidos, el fundamento jurídico primario es la Ley de secreto bancario («Bank Secrecy Act»). En Europa se aplican a nivel nacional disposiciones similares, que son coherentes con la tercera Directiva sobre blanqueo de dinero y, más recientemente, con el Reglamento (CE) nº 1781/2006 del Parlamento Europeo y del Consejo, de 15 de noviembre de 2006, relativo a la información sobre los ordenantes que acompaña a las transferencias de fondos.

Autoridad legal para recabar y utilizar datos procedentes de SWIFT

Los requerimientos cursados a SWIFT se basan en fundamentos jurídicos aplicados desde hace tiempo y en decretos correspondientes de lucha contra el terrorismo y su financiación. La Ley de poderes económicos en caso de emergencia internacional («International Emergency Economic Powers Act») de 1977 (IEEPA) autoriza al Presidente de Estados Unidos, durante un período declarado de emergencia nacional, a investigar las transferencias bancarias y demás operaciones en las que participe una persona extranjera. Del mismo modo, la Ley de participación en las Naciones Unidas («United Nations Participation Act»), de 1945 (UNPA) autoriza al Presidente, al aplicar las Resoluciones del Consejo de Seguridad de las Naciones Unidas, a investigar las relaciones económicas o medios de comunicación entre personas extranjeras y Estados Unidos.

El 23 de septiembre de 2001, el Presidente aprobó el decreto nº 13224, sobre la base de IEEPA y UNPA y mencionando Resoluciones del Consejo de Seguridad de las Naciones Unidas que designaban a los talibanes y Al Qaeda. Mediante dicho decreto, el Presidente declaraba un período de emergencia nacional para abordar la cuestión de los atentados terroristas del 11S y la amenaza persistente e inmediata de nuevos atentados, y bloqueó los haberes de las personas que habían cometido los atentados, constituían una amenaza o apoyaban el terrorismo, y prohibió realizar operaciones con dichas personas.

A los efectos del decreto nº 13224, la sección 3 contiene la definición siguiente:

el término «terrorismo» significa una actividad que:

i) implique un acto violento o un acto peligroso para la vida humana, la propiedad o las infraestructuras y

ii) tenga como objetivo:

A) intimidar o coaccionar a la población civil;

B) influir en la política de un gobierno mediante intimidación o coacción, o

C) influir en la conducta de un gobierno mediante destrucción masiva, asesinato, secuestro o toma de rehenes.

En la sección 7 del decreto, el Presidente autoriza al Secretario del Departamento del Tesoro a utilizar todas las competencias que IEEPA y UNPA otorgan al Presidente, que resulten necesarias para conseguir los objetivos del decreto. También autoriza al Secretario del Tesoro a subdelegar cualesquiera de esas funciones a otros funcionarios y agencias del Gobierno de EEUU, y ordena a todas las agencias del Gobierno de EEUU que adopten todas las medidas adecuadas dentro del ámbito de sus responsabilidades para llevar a cabo las disposiciones del decreto. IEEPA y el decreto, tal como se aplican mediante la Reglamentación de sanciones contra el terrorismo global («Global Terrorism Sanctions Regulations»), autoriza al Director de la Oficina de control de activos extranjeros (OFAC) del Departamento del Tesoro a exigir a cualquier persona información sobre operaciones financieras u otros datos en relación con una investigación económica relacionada con sanciones. Estas son los fundamentos jurídicos en los que se basan los requerimientos expedidos por OFAC a SWIFT para que proporcione datos financieros relacionados con investigaciones en el ámbito de la lucha contra el terrorismo.

Control de acceso y seguridad del sistema informático

A los datos obtenidos de SWIFT, que cumplen los procedimientos del Gobierno de EEUU para la manipulación de información relacionada con la investigación del terrorismo y su financiación en general, se les aplican estrictas medidas técnicas y de organización con el fin de proteger la información contra la destrucción accidental o ilícita, la pérdida, modificación o acceso a dichos datos. Todas las medidas de seguridad que se exponen a continuación son objeto de auditorías independientes.

Los datos procedentes de SWIFT se conservan en un entorno físico seguro, se mantienen separados de otros datos y los sistemas informáticos disponen de controles de alto nivel para impedir las intrusiones y disponen de otros sistemas de protección para que el acceso a los datos se limite a lo exclusivamente previsto. No se hacen copias de los datos procedentes de SWIFT distintas de las que se hacen para la recuperación de datos en caso de accidente y el acceso a los datos y equipos informáticos está limitado a las personas con los niveles adecuados de habilitación de seguridad. Incluso para esas personas, el acceso a los datos de SWIFT se realiza únicamente en modo de lectura y el propio programa TFTP limita el acceso a los analistas dedicados a la investigación del terrorismo y personas que participan en el apoyo técnico, gestión y supervisión del TFTP y únicamente a la información estrictamente necesaria.

Extracción y uso limitado a la investigación del terrorismo

El programa TFTP no conlleva extracción de datos ni cualquier otro tipo de algoritmo, reseña automatizada o filtro informático. El TFTP dispone de múltiples capas de controles estrictos para limitar la información recopilada, garantizar que la información obtenida se utiliza únicamente a efectos de lucha contra el terrorismo y proteger la privacidad de las personas no relacionadas con el terrorismo o su financiación. Las garantías, que se superponen, reducen constantemente el ámbito y limitan significativamente el acceso y la utilización de los datos financieros procesados por SWIFT en sus operaciones cotidianas.

De entrada los requerimientos cursados a SWIFT están cuidadosamente y estrictamente diseñados para limitar la cantidad de datos que deben facilitarse al Departamento del Tesoro. Se requiere a SWIFT que facilite únicamente los datos que el Departamento del Tesoro considera necesarios para luchar contra la financiación del terrorismo, sobre la base de análisis anteriores centrados en tipos de mensaje e indicaciones geográficas, así como contra amenazas y vulnerabilidades. Además, las búsquedas se diseñan estrictamente para minimizar la extracción de mensajes que no sean pertinentes a efectos de la investigación del terrorismo. La exploración de los datos facilitados por SWIFT tiene únicamente como finalidad la información relacionada con una determinada investigación que exista previamente en el ámbito del terrorismo, lo que supone que toda exploración realizada debe mencionar específicamente y hacer constar pruebas fehacientes de que el objetivo tiene alguna relación con el terrorismo o su financiación. Todas y cada una de las búsquedas de los datos SWIFT con arreglo al TFTP quedan registradas al mismo tiempo, incluida la afirmación sobre la relación con el terrorismo necesaria para iniciar la búsqueda.

De las garantías anteriormente expuestas se desprende que únicamente se ha tenido acceso a un porcentaje mínimo (a saber, muy inferior al 1 %) del subconjunto de mensajes de SWIFT facilitados al Departamento del Tesoro, y únicamente debido a que estos mensajes respondían directamente a una búsqueda específica en relación con el terrorismo.

Supervisión independiente

Además de los controles descritos del Departamento del Tesoro, el programa TFTP incluye múltiples supervisiones independientes de carácter complementario: los propios representantes de SWIFT, una empresa de auditoría independiente y otras instancias gubernamentales independientes estadounidenses, incluido el Congreso de EEUU.

SWIFT y los auditores externos elegidos por la empresa ejercen una supervisión independiente del programa TFTP de diferentes maneras que son mutuamente complementarias. En primer lugar, se ha concedido habilitación de seguridad a determinados representantes de SWIFT con el fin de que tengan acceso en cualquier momento del día a los equipos y datos, y se les ha concedido la facultad de supervisar en tiempo real y restrospectivamente la utilización de los datos con el fin de garantizar que sólo se utilizan a efectos de la lucha contra el terrorismo. Además, los representantes de SWIFT pueden detener inmediatamente cualquier búsqueda específica, e incluso pueden apagar el sistema si algo no les satisface.

Por lo que se refiere a los auditores externos independientes, el mantenimiento, acceso y utilización de los datos de SWIFT son objeto permanentemente de auditorías periódicas con arreglo a protocolos cuidadosamente diseñados que respetan la normativa internacional en materia de auditoría. Las auditorías se refieren al control del acceso y a las garantías de seguridad del sistema informático, así como a la limitación de la utilización de los datos para fines exclusivamente de lucha contra el terrorismo, tal como se ha explicado anteriormente. Los auditores independientes transmiten sus conclusiones al comité de auditoría y financiero del consejo de administración de SWIFT.

Además, en cumplimiento de la legislación de Estados Unidos, se ha informado en varias ocasiones a diferentes comités del Congreso sobre el programa TFTP y sobre su funcionamiento, y periódicamente se sigue informando al respecto a dichos comités. El programa TFTP también ha sido objeto de varias comparecencias en el Congreso.

Por último, el Consejo de supervisión de las libertades civiles y de la privacidad («Privacy and Civil Liberties Oversight Board»), creado con arreglo a la Ley de reforma de la inteligencia y de prevención del terrorismo («Intelligence Reform and Terrorism Prevention Act») de 2004 ejerce la supervisión del TFTP. La misión del Consejo de supervisión es garantizar que en la aplicación de todas las leyes, reglamentaciones y políticas del poder ejecutivo en relación con los esfuerzos de protección de Estados Unidos contra el terrorismo se toman en consideración de forma adecuada las cuestiones relacionadas con la privacidad y las libertades civiles. El Consejo de supervisión tiene también la responsabilidad de examinar las prácticas en la puesta en común de información entre departamentos y agencias públicas con el fin de determinar si se están siguiendo las orientaciones aprobadas para la protección de la privacidad y de las libertades civiles.

Como se expone a continuación, esta supervisión general e independiente se aplica conjuntamente con controles para restringir la difusión mediante los cuales se restringe el acceso a la información procedente de los registros financieros de SWIFT y se ofrece una mayor protección de la privacidad.

Difusión y puesta en común de la información

La Comunidad internacional ha reconocido que compartir la información en el ámbito del terrorismo tiene una importancia fundamental. La RCSNU nº 1373 exhorta a todos los Estados a encontrar medios para intensificar y agilizar el intercambio de información operativa en el ámbito de la lucha contra el terrorismo y a intercambiar información para impedir la comisión de actos de terrorismo. De la misma forma, la sección 6 del decreto 13224 impone al Secretario del Tesoro (y demás funcionarios) la obligación de realizar todos los esfuerzos pertinentes para cooperar y coordinar su actuación con otros países con el fin de lograr los objetivos del decreto, incluida la prevención y supresión de actos de terrorismo, impedir la financiación y servicios financieros a los terroristas y poner en común la inteligencia sobre actividades de financiación en apoyo del terrorismo. En este contexto la información procedente de datos de SWIFT se comparte de la forma pertinente con otros socios nacionales e internacionales. Como ocurre con otros aspectos del TFTP, esta puesta en común de la información se realiza de conformidad con la legislación estadounidense y se le aplican una serie de garantías destinadas a proteger los datos de SWIFT y la privacidad de las personas a las que se refieren los datos.

Los expertos de la lucha contra el terrorismo que realizan búsquedas en el marco del TFTP comprueban la pertinencia de la información obtenida en respuesta a la búsqueda antes de preparar esta información para su divulgación a través de canales seguros. El Departamento del Tesoro también ejerce un control en origen de toda difusión ulterior de la información, lo que significa que ningún receptor está autorizado a divulgar la información sin la autorización explícita previa del Departamento del Tesoro. A este respecto, y también en caso de que se acceda sin autorización a los datos de SWIFT, toda difusión no autorizada de información relacionada con el TFTP puede dar lugar a estrictas medidas disciplinarias o a la imposición de sanciones civiles o penales.

La información procedente de los datos entregados por SWIFT se comparte con otras agencias y servicios de inteligencia y fuerzas y cuerpos de seguridad bajo controles estrictos de que se utiliza exclusivamente con fines de investigación, detección, prevención o persecución del terrorismo o su financiación o con investigaciones y procesos relacionados. La Ley Nacional de Seguridad («National Security Act») y Ley de Reforma de la Inteligencia y de Prevención del Terrorismo («Intelligence Reform and Terrorism Prevention Act») de 2004, así como una serie de memorandos de acuerdo y los correspondientes decretos imponen la obligación de compartir la información. Según la legislación estadounidense, las agencias receptoras tienen las mismas obligaciones que el Departamento del Tesoro de proteger la información originada a partir del programa TFTP. Cabe señalar también que la información originada a partir del programa TFTP se comparte con otras agencias estadounidenses a efectos de utilización como pistas, lo que implica que sólo se pueda utilizar en procesos judiciales como «prueba afirmativa». Las agencias receptoras disponen de sus propios fundamentos jurídicos para realizar sus investigaciones, incluida la obtención de documentación de otras fuentes que puedan utilizarse más adelante como pruebas en los procesos judiciales.

Esas otras agencias gubernamentales también comparten la información sobre pistas extraída de los datos procedentes de SWIFT con otros socios extranjeros con la misma finalidad y la aprobación para cada caso específico del Departamento del Tesoro, cuando esté justificado por motivos de seguridad nacional y de aplicación de la ley. En general, en el contexto del TFTP, se ha compartido mucha información sobre pistas con autoridades extranjeras sin revelar que la información tenía su origen en el TFTP.

Por lo que respecta a la posible difusión pública de datos de SWIFT, el Departamento del Tesoro trata los datos como información clasificada, sensible para fuerzas y cuerpos de seguridad e información comercial confidencial. Por consiguiente, el Departamento del Tesoro no divulga ni divulgaría públicamente los datos, a menos que sea preceptivo por ley. A este respecto, en caso de un posible procedimiento administrativo o judicial que tenga su origen en una solicitud de datos del TFTP presentada por una tercera parte al amparo de la Ley de Libertad de Information (Freedom of Information Act) (FOIA) el Departamento del Tesoro abogaría por que dichos registros estuvieran exentos de la obligación de divulgación con arreglo a la FOIA.

Derecho de reparación

El carácter limitado de los datos que figuran en un mensaje específico de una operación SWIFT, la forma limitada de acceso a determinados datos SWIFT a través del TFTP como parte de una investigación preexistente en el ámbito del terrorismo y los límites a la divulgación de información sobre pistas reducen significativamente la pertinencia de un mecanismo de reparación como parte del propio TFTP. A pesar de todo, de conformidad con la legislación estadounidense, existen medios adecuados para la reparación en caso de uso incorrecto por parte de las autoridades gubernamentales.

Por lo que se refiere al interés de una persona física concreta sobre la utilización de datos y su derecho de reparación en caso de uso incorrecto, debe realizarse una distinción entre los datos que pueden ser objeto de búsquedas presentados por SWIFT y los mensajes extraídos que forman parte de una investigación específica relacionada con el terrorismo, que pueden servir de base para una decisión administrativa u otra intervención gubernamental. Los datos obtenidos de SWIFT mediante requerimiento administrativo de OFAC son copias de mensajes completos de operaciones financieras, a saber, copias electrónicas de registros de operaciones existentes en las instalaciones de SWIFT en EEUU en circunstancias normales de funcionamiento. Aunque estos datos pueden ser objeto de algún tipo de tratamiento en el sentido de una capacidad muy limitada de búsqueda y recuperación con fines antiterroristas, tal como aquí se describe, en la base de datos de búsqueda no se modifican, ni se manipulan, ni se añaden o suprimen datos de los mensajes de cada una de las operaciones.

Además, conviene subrayar de nuevo que la inmensa mayoría de los mensajes de operaciones entregados por SWIFT ni siquiera serán vistos nunca por expertos de la lucha contra el terrorismo y, por consiguiente, se ignoran. Por consiguiente, responder a una posible pregunta en relación con la privacidad de una persona física para saber si la base de datos incluye información sobre dicha persona requeriría, en casi todos los casos, acceder a datos a los que no se habría accedido nunca en el funcionamiento normal del programa TFTP, lo que entra en contradicción con el requisito establecido por el TFTP de que cada búsqueda tenga un nexo previo con el terrorismo. Por último, habida cuenta de que no se modifican, ni se manipulan, ni se añaden o suprimen datos de la base de datos de búsqueda, no existe una base para «rectificar» la información. Más aún, serviría para modificar los registros completos de las operaciones requeridas por OFAC.

Un tratamiento ulterior de los datos incluidos en un mensaje correspondiente a una operación específica sólo se produce en el caso de los relativamente escasos mensajes de operaciones específicas que resultan directamente de una búsqueda específica en relación con el terrorismo, extraídos de la base de datos de búsqueda. Una vez extraídos y supeditados a los múltiples controles que limitan la difusión a los objetivos de la lucha contra el terrorismo, se podría tratar de ejercer el derecho de reclamación al amparo de los procedimientos administrativos y judiciales correspondientes con respecto a la actuación gubernamental en la difusión de la información.

El ejercicio del derecho de reparación puede ilustrarse de la siguiente forma en relación con una actuación administrativa de OFAC de bloqueo de activos con arreglo a la Reglamentación de sanciones contra el terrorismo global («Global Terrorism Sanctions Regulations») mediante la cual se aplica el decreto nº 13224. Una persona puede solicitar a OFAC que reconsidere, desde el punto de vista administrativo, su designación como terrorista global con mención especial, de esta forma se brinda a esta persona la oportunidad de demostrar que «las circunstancias que dieron lugar a la designación ya no existen» y de «presentar argumentos o pruebas que la persona considere demuestran que la designación se realizó sobre una base insuficiente». Un terrorista global con mención especial también puede reclamar la revisión judicial de una decisión de la agencia con arreglo a las disposiciones pertinentes de la Ley de Procedimiento Administrativo («Administrative Procedures Act»). Estos procedimientos administrativos y judiciales por los que se ejerce el derecho de reparación se aplicarían a cualquier persona que sea objeto de la decisión gubernamental, independientemente de su nacionalidad.

Período de conservación

El período de conservación de la información relacionada con la lucha contra el terrorismo (o de cualquier otro tipo) depende de numerosos factores establecidos, entre los que cabe destacar las exigencias de la investigación, la normativa de limitación aplicable y los límites obligatorios para la interposición de demandas o de acciones judiciales. La aplicación y el funcionamiento de estos y otros factores difieren de una agencia a otra, en función de la naturaleza de su misión específica y los cometidos de la agencia. Por consiguiente, los períodos de conservación para determinados tipos de información relacionada con el terrorismo recopilados por distintas agencias dependen de la naturaleza de la información y de la investigación con la cual se relacionan.

En el gobierno de Estados Unidos, la Administración de Archivos y Registros Nacionales («National Archives and Records Administration») (NARA) aprueba los calendarios de conservación y disposición aplicables a los registros de las agencias con arreglo a diferentes estatutos y normativas. Todos los registros que no se considere que tienen un valor permanente deben estar programados para su destrucción después de un plazo específico establecido sobre la base de parámetros administrativos, fiscales y jurídicos. Entre los factores que considera NARA a la hora de aprobar los períodos de conservación de registros en una agencia destacan las normativas de limitación aplicables, los límites obligatorios para la interposición de demandas o de acciones judiciales, el potencial de fraude, los riesgos de impugnación y los derechos sustantivos y las normativas o estatutos que conceden o limitan un derecho jurídico específico.

Por lo que se refiere a los plazos de conservación de la información relacionada con el TFTP, cabe hacer de nuevo una distinción entre los datos obtenidos de SWIFT bajo requerimiento y los datos extraídos que sirven de base para una decisión administrativa u otra acción gubernamental.

De forma continua y sobre una base anual, como mínimo, el Departamento del Tesoro tratará de identificar y suprimir todos los datos no extraídos que no resulten necesarios para lograr los objetivos mencionados en las presentes declaraciones. Supeditados a los resultados de los mencionados análisis para determinar su necesidad, todos los datos no extraídos recibidos por el Departamento del Tesoro procedentes de SWIFT después de la fecha de publicación de las presentes declaraciones serán suprimidos por el Departamento del Tesoro, a más tardar, cinco años después de su recepción por el Departamento del Tesoro. Supeditados a los resultados de los mencionados análisis para determinar su necesidad, todos los demás datos no extraídos serán suprimidos, a más tardar, cinco años después de la fecha de publicación de las presentes declaraciones.

A los datos extraídos que responden directamente a una búsqueda específica en relación con la lucha contra el terrorismo y que han sido objeto de los múltiples controles para la divulgación anteriormente expuestos se les aplicarán los períodos de conservación aplicables a la autoridad gubernamental específica de que se trate con respecto a sus registros de investigación específicos.

Por ejemplo, los datos de SWIFT extraídos en el marco del programa TFTP podrían utilizarse en la investigación de una persona para su posible designación con arreglo a la Reglamentación de sanciones contra el terrorismo global («Global Terrorism Sanctions Regulations») de la OFAC. Con arreglo al calendario de conservación de registros aprobado por NARA con respecto a OFAC, si se adopta una decisión administrativa final de designación de una persona (decisión que se haría pública), la información en la que se basa la decisión se conservaría con carácter permanente como registro escrito de la prueba de base de la acción de la agencia. El registro de la prueba se conservaría para una posible revisión administrativa o judicial en caso de que se cuestionara la designación, y como base de investigaciones ulteriores en el ámbito de la lucha contra el terrorismo. Y al contrario, en caso de que la investigación concluyera sin designación, se procede a la destrucción in situ del registro de investigación a más tardar un año después de haber concluido la investigación.

Por último, con arreglo al marco jurídico de Estados Unidos anteriormente descrito, el período de conservación de información sobre pistas procedente del TFTP que hayan sido objeto de difusión estará establecido por la normativa y plazos aplicables a la agencia o gobierno receptor. Por ejemplo, a la información procedente del TFTP utilizada en una acción judicial emprendida por el Departamento de Justicia se le aplicarán los períodos de conservación aplicables al Departamento de Justicia.

Cooperación actual en el marco de la lucha contra el terrorismo

La contribución del programa TFTP a la lucha contra el terrorismo global ha sido muy valiosa, incluso en Europa. El Gobierno de Estados Unidos seguirá evaluando con buen criterio si la información obtenida en el marco del programa TFTP puede contribuir a la investigación, prevención, lucha y persecución del terrorismo y su financiación en uno o más Estados miembros de la Unión Europea y, en todos los casos adecuados, pondrá esta información a disposición de las autoridades competentes de la forma más oportuna.

Como signo de nuestro compromiso y colaboración en la lucha contra el terrorismo global, se designará a una personalidad eminente europea para que confirme que la aplicación del programa se atiene a lo expuesto en las presentes declaraciones y verifique la protección de los datos personales procedentes de la UE. En particular, esta personalidad supervisará que se llevan a cabo los procesos de supresión de los datos no extraídos.

Esta personalidad eminente, que será designada por la Comisión Europea consultando al Departamento del Tesoro, tendrá un nivel adecuado de experiencia y la habilitación de seguridad y un mandato de un período de dos años renovable. Actuará con total independencia en el ejercicio de sus funciones, no pedirá instrucciones a nadie ni las aceptará y se abstendrá de todo tipo de acción que sea incompatible con el ejercicio de sus funciones tal como se recogen en su nombramiento.

Esta personalidad eminente remitirá sus conclusiones y los resultados de su trabajo por escrito una vez al año a la Comisión. La Comisión a su vez informará al Parlamento Europeo y al Consejo de la forma adecuada.

El Departamento del Tesoro permitirá el acceso de esta personalidad eminente a la información y los datos necesarios para el ejercicio de sus funciones. La personalidad eminente respetará en todo momento las obligaciones de secreto y de confidencialidad impuestas por la ley. Las disposiciones prácticas de funcionamiento se convendrán con el Departamento del Tesoro.

El Departamento del Tesoro advertirá a la Unión Europea de los posibles cambios en las garantías expuestas en las presentes declaraciones y de la elaboración de toda posible normativa de Estados Unidos que tenga repercusiones materiales en lo expuesto en las declaraciones.

El Departamento del Tesoro se encargará de que estas declaraciones se publiquen en el Registro Federal y acepta que se publiquen en el *Diario Oficial de la Unión Europea*.