La dimensión exterior de Europol desde el punto de vista de la protección de datos. El caso del acuerdo TFTP

Alba Bosch Moliné [*]

1. Introducción

En el momento de escribir este artículo [1], las revelaciones sobre las actividades de vigilancia masiva por parte de EEUU y de varios países miembros de la UE [2] ponían de actualidad la aparente disyuntiva entre la protección de datos y la seguridad, especialmente en relación a terceros países. Sin embargo, estos dos objetivos no constituyen siempre un juego de suma cero.

El marco europeo de protección de datos, actualmente en revisión, trata de proporcionar un equilibrio. Bajo ciertas condiciones [3], permite restricciones a los derechos a la privacidad y a la protección de datos, por ejemplo para llevar a cabo una investigación policial concreta o para salvaguardar la seguridad del Estado [4]. A su vez, un buen nivel de protección de datos asegura su calidad y exactitud, evita el almacenamiento de datos innecesarios y permite el intercambio información personal

---

[*] Jefa interina de Cooperación Internacional del Supervisor Europeo de Protección de Datos. Cualquier opinión expresada en este artículo es propia y no representa a ninguna organización. La autora desea expresar su agradecimiento a Emilio Aced, Jefe de Área en la Agencia Española de Protección de Datos y a Andy Goldstein, miembro del equipo de Tecnología de la Información del Supervisor Europeo de Protección de Datos.

[1] Primera versión del artículo finalizada en junio de 2013. Actualizado en diciembre de 2013 y abril de 2014.

[2] Ver las primeras noticias basadas en las revelaciones de Edward Snowden en *The Guardian* y *The Washington Post* el 6 de Junio de 2013 (disponibles respectivamente en http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ y http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order, último acceso el 04.04.2014).

[3] Ver los criterios de necesidad, proporcionalidad y base legal en el artículo 8(2) del Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales de 4 de Noviembre de 1950 y el artículo 52(1) de la Carta de Derechos Fundamentales de la UE (2013/C 326/02), DO C 326, 26.10.2012.

[4] Ver el artículo 13(1)(d) de la Directiva 95/46/EC del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y la libre circulación de estos datos (en adelante: "Directiva 95/46/EC"), DO L 281, 23.11.1995, p.31. Ver también la interpretación del SEPD, según la cual las excepciones relativas a la seguridad nacional o a la seguridad del Estado en la legislación europea se refieren a la seguridad de los países miembros de la UE, no a la de terceros países (Opinión del SEPD sobre el restablecimiento de la confianza en los flujos de datos entre la UE y EEUU, disponible en www.edps.europa.eu). En cualquier caso, toda limitación a un derecho fundamental tiene que ser interpretada de forma restrictiva, de acuerdo con la jurisprudencia de la Corte Europea de Derechos Humanos, y debe cumplir con las condiciones del Artículo 52(1) de la Carta de Derechos Fundamentales de la UE.

con la confianza de que no será utilizada de forma inapropiada[5]. Todo ello cobra una relevancia particular cuando los datos deben transferirse a países terceros. En este sentido, Europol y su acción exterior proporcionan un caso de estudio interesante, en el que entran en juego las relaciones y el intercambio de datos entre autoridades policiales dentro y fuera de la UE.

Este artículo analiza la acción exterior de Europol desde el punto de vista de la protección de datos. En primer lugar se presenta la agencia europea de policía y sus sistemas de tratamiento de datos. A continuación, se analiza cómo Europol desempeña su acción exterior, concretamente cuando transfiere datos personales a terceros países y organizaciones internacionales. En el tercer capítulo se describen las normas aplicables a las transferencias de datos por parte de Europol. En cuarto lugar, se examina el cumplimiento de estas normas sobre la base de los informes de evaluación y de inspección disponibles. En este punto se dedica una atención especial al papel de Europol en la aplicación del acuerdo entre la UE y EEUU (TFTP)[6], debido a la mayor disponibilidad de información sobre su inspección. Finalmente, se anticipan los posibles desarrollos futuros a la luz de la nueva propuesta de reglamento de Europol y de los debates en el Parlamento Europeo sobre el acuerdo TFTP.

2. Europol, el tratamiento de datos y su acción exterior

2.1. ¿Qué es Europol?

La Oficina Europea de Policía (Europol) es actualmente una agencia de la UE, aunque fue fundada como una organización internacional, financiada directamente por el presupuesto de sus miembros. Su objetivo es apoyar la acción de las policías nacionales y reforzar su cooperación mutua en la prevención y la lucha contra la delincuencia organizada, el terrorismo y otros delitos graves que afecten a dos o más Estados. Tiene competencia sobre un amplio abanico de formas de delincuencia grave, tales como el tráfico de drogas, el blanqueo de capitales, los delitos informáticos, el tráfico de inmigrantes clandestinos, la corrupción y la trata de seres humanos.

A diferencia de las policías nacionales, Europol carece de poderes coercitivos, a pesar de la imagen proyectada en ocasiones en los medios[7]. En realidad, su valor añadido

---

5 El tratamiento de los datos personales por parte de las autoridades policiales y judiciales de acuerdo con la ley también asegura, por ejemplo, que puedan usarse como evidencia en un juicio.

6 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. (Decisión del Consejo 2010/412/UE, de 13 de julio de 2010, DO L 195, 27.7.2010, p.3.

7 Ver el filme Ocean's Twelve (2004), en el que la actriz Catherine Zeta-Jones encarna a una agente de Europol que amenaza con realizar una detención. La página web de Europol expone orgullosa esta y otras apariciones de la agencia en producciones de ficción en https://www.europol.europa.eu/content/page/tv-films-and-books-195, (último acceso el 25.05.2013).

radica en su capacidad de análisis, intercambio de información e inteligencia[8], y en el apoyo operativo que proporciona a los Estados miembros. Europol también actúa como centro de conocimiento sobre el crimen, realiza evaluaciones de amenazas e informes estratégicos y, desde principios de 2013, hospeda el Centro Europeo de Ciberdelincuencia (EC3, por sus siglas en inglés).

Europol está gestionada por su director, nombrado por cuatro años por el Consejo de la UE por mayoría cualificada, a partir de una lista de candidatos proporcionada por el consejo de administración de Europol, formado por representantes de los 27 Estados miembros y de la Comisión Europea. Cada Estado miembro nombra en su país al menos una unidad nacional de Europol como punto de contacto con sus autoridades de policía, dedicada principalmente al intercambio de información con Europol y con las policías nacionales.

Además, cada Estado envía funcionarios de enlace a la sede de Europol en la Haya para constituir las oficinas nacionales de enlace, encargadas de defender los intereses de las unidades nacionales, intercambiar información entre éstas y Europol, y contribuir también al intercambio de información entre unidades nacionales y funcionarios de enlace de otros países. En total, Europol emplea cerca de 800 personas, incluyendo alrededor de 140 funcionarios de enlace procedentes de los Estados miembros de la UE y de países terceros con los cuales colabora mediante acuerdos de cooperación.

2.1.1. De organización internacional a agencia de la UE

Europol fue creada por el Tratado de Maastricht de 1992[9]. En 1994, un año antes de ser formalmente establecida por el Convenio de Europol,[10] inició sus operaciones de forma limitada como unidad de drogas de Europol. El Convenio entró en vigor en 1998 y la agencia inició plenamente su actividad en 1999. Sin embargo, el Convenio era un instrumento demasiado inflexible, dependiente para su adopción y modificación de las ratificaciones de todos los Estados miembros, como demostró la lenta ratificación de los tres protocolos adicionales[11]. En 2006, la presidencia

---

8 Según el CNI, la inteligencia es el resultado de valorar, analizar, integrar e interpretar la información. La información, en cambio, es la noticia en su sentido más amplio y la base para la elaboración de inteligencia (http://www.cni.es/es/preguntasfrecuentes/pregunta_010.html?pageIndex=10&faq=si&size=15, último acceso el 25.05.2013).

9 Tratado de la Unión Europea, Maastricht, 7.02.1992, DO C 191, 29.07.1992, p.1.

10 Convenio de 26 de julio de 1995 basado en el artículo K.3 del Tratado de la Unión Europea, por el que se crea una Oficina Europea de Policía, DO C 316 de 27.11.1995. (en adelante "el Convenio de Europol" o "el Convenio").

11 Firmados en 2000, 2002 y 2003, no entraron en vigor hasta 2007, extendiendo el mandato de Europol en el ámbito del lavado de capitales, permitiendo la participación de Europol en los *equipos conjuntos de investigación* (JIT en sus siglas en inglés) e introduciendo cambios en el Convenio de Europol.

austríaca del Consejo puso en cuestión que un convenio fuera el instrumento legal más apropiado para Europol, alimentando el debate, no sólo sobre la base jurídica de Europol, sino también sobre su falta de control parlamentario[12], una cuestión que deviene más acuciante a medida que aumentan las competencias y la capacidad operativa de Europol. Finalmente, y ante el fracaso de la llamada Constitución europea[13], que hubiera permitido adoptar una "ley europea" para Europol, el Consejo Europeo acordó reemplazar el Convenio por una decisión del Consejo de ministros, que se adoptaría en 2009.[14]

La nueva Decisión de Europol[15] transformó esta organización intergubernamental en una agencia de la UE, financiada a cargo del presupuesto de la Unión y sometida, por tanto, al escrutinio del Parlamento Europeo, tanto respecto a la adopción del presupuesto -incluida la plantilla de personal- como para el procedimiento de adopción de la gestión. La decisión aumentó las competencias y la capacidad operacional e investigativa de Europol, introdujo la posibilidad de crear nuevos sistemas de tratamiento de datos e incrementó su capacidad de acción exterior.

2.2. Los sistemas de tratamiento de información de Europol

Teniendo en cuenta las funciones de Europol, el tratamiento de la información, incluidos los datos personales, es clave para lograr sus objetivos. Estos tratamientos se realizan mediante sistemas establecidos previamente por el Convenio y actualmente por la Decisión. También pueden ser creados por decisiones ad hoc del consejo de administración (siempre que se trate de datos no sensibles), aunque esta posibilidad no se ha utilizado.[16]

---

12 Ver el informe del grupo "Amigos de la Presidencia" sobre el futuro de Europol de 19 de mayo de 2006, pág.13, 32 y 33, disponible en http://register.consilium.europa.eu/pdf/en/06/st09/st09184-re01.en06.pdf (último acceso el 25.05.2013).

13 Tratado por el que se establece una Constitución para Europa, firmado en 2004 y nunca ratificado (DO C 310, 16.12.2004).

14 Cabe destacar que, a pesar de su lentitud, el proceso de enmienda anterior mediante la ratificación de protocolos, permitía al menos a los parlamentos nacionales bloquear su adopción. Ver sobre este tema el análisis de Steve Reeves (Centro de Derechos Humanos de la Universidad de Essex) para Statewatch: "Europol: the final step in the creation of a European Police Force", 2007, pág. 3-4, disponible en http://www.statewatch.org/news/2007/jan/europol-analysis.pdf (último acceso el 25.05.2013). Ver también el informe para la audiencia del Parlamento Europeo sobre el futuro de Europol: "Increasing Europol's Accountability and Improving Europol's Operational Capacity", pág.2, disponible en http://www.europarl.europa.eu/meetdocs/2004_2009/documents/nt/630/630339/630339en.pdf

15 Decisión del Consejo de 6 de abril de 2009 por la que se crea la Oficina Europea de Policía (Europol) (2009/371/JAI), DO L 121, 15.5.2009, p.37. (En adelante, "la Decisión de Europol" o "la Decisión").

16 Ver el dictamen de la ACC de 10 de junio de 2013 (Opinion 13/31 of the Joint Supervisory Board with respect to the proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law enforcement Cooperation and Training (Europol)), p. 9, disponible en http://europoljsb.consilium.europa.eu/media/257072/13-

2.2.1. Intercambio de información

Para dar respuesta a los cambios introducidos por los protocolos, la Decisión y la "iniciativa sueca"[17], la Aplicación Segura de la Red de Intercambio (SIENA, en sus siglas en inglés) sustituyó en 2009 a la aplicación Info-Ex como sistema seguro de intercambio de datos sobre personas sospechosas o condenadas entre Europol, los Estados miembros de la UE y terceras partes a través de las Oficinas de Enlace de Europol y las Unidades Nacionales de Enlace.

El Sistema de Información de Europol (EIS, en sus siglas en inglés) contiene una base de datos europea de inteligencia criminal alimentada principalmente por los Estados miembros[18] a través de las Unidades Nacionales de Enlace, aunque de forma desigual[19]. Desde 2005, facilita la detección automática de coincidencias (sistema hit/ no-hit) entre investigaciones y el intercambio seguro de información relacionada.

2.2.2. Análisis operativo

Los ficheros de análisis de trabajo (AWF, en sus siglas en inglés) son el instrumento usado por Europol para apoyar las investigaciones realizadas en los Estados miembros. Permiten alertar a las policías nacionales de cualquier conexión identificada relacionada con crímenes e investigaciones específicas. No sólo contienen información proporcionada por los Estados miembros, si no también un análisis por parte Europol, lo cual le aporta un gran valor añadido. La función de índice (IxS) proporciona una función de búsqueda entre los contenidos de los AWF, ya que contiene datos relevantes para una determinada investigación o tarea.

Además, Europol hospeda desde enero de 2013 el EC3, dedicado a la lucha contra la ciberdelincuencia mediante la provisión de apoyo operativo y capacidad analítica a los Estados miembros y a las instituciones europeas. Con este fin, tiene la función de cooperar con éstos y otros actores relevantes, incluyendo terceros países y organizaciones internacionales.[20]

2.2.3. Acceso a otros sistemas de información de la UE

31%20jsb%20opinion%20on%20europol's%20regulation%20proposal.pdf (último acceso el 29.06.2013).

17 Decisión 2006/960/JAI del Consejo de 18 de diciembre de 2006 sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea ("la iniciativa sueca"), DO L 386, 29.12.2006, p.89.

18 Europol también introduce información procedente de terceros Estados.

19 En 2011, Alemania fue el país que más datos introdujo en el EIS, seguido de Bélgica, Francia, España y la misma Europol (que introduce datos proporcionados por terceras partes).

20 El EC3 también tiene la función de cooperar con los órganos de gobernanza de Internet, la sociedad civil, los proveedores de servicios, empresas de seguridad de internet, el sector financiero, y los equipos de respuesta ante emergencias informáticas (los CERTs nacionales y el CERT-EU). Para más información ver https://www.europol.europa.eu/ec3, último acceso el 1.07.2013.

Cabe añadir que Europol también tiene acceso al Sistema de Información Schengen (SIS II) y al Sistema de Información de Aduanas (CIS). Además, en junio de 2013 el Parlamento Europeo y el Consejo aprobaron la polémica propuesta para permitir el acceso de Europol (y el de las policías nacionales) a EURODAC, la base de datos de huellas digitales de solicitantes de asilo[21]. Asimismo, desde septiembre de 2013, tanto Europol como las policías nacionales pueden tener acceso al Sistema de Información de Visados (VIS).[22]

2.3. La acción exterior de Europol y las transferencias de datos personales a terceros países

El marco de la acción exterior de la agencia se define en su estrategia externa, que se basa en los objetivos generales de la dimensión externa del espacio de Libertad, Seguridad y Justicia de la UE[23]. Respecto a la relación entre ambos instrumentos, es interesante destacar que existen opiniones encontradas sobre si la acción exterior de Europol debería servir a las relaciones externas de la UE o si la elección de los países con os cuales Europol establece acuerdos debería depender únicamente de las necesidades operativas de la agencia.[24]

2.3.1. La evolución de la acción exterior de Europol

La Convención de Europol ya permitía a la agencia mantener relaciones con terceros países y organizaciones internacionales[25]. Las normas generales que regulan estas relaciones se establecieron en el Acto del Consejo del 3 de noviembre de 1998[26] y en

---

21 Ver el procedimiento en detalle y los documentos relacionados en http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2008/0242(COD), último acceso el 01.07.2013.

22 Permitido por la decisión del Consejo 2008/633/JAI de 23 de junio de 2008 sobre el acceso para consultar el Sistema de Información de Visados (VIS) por las autoridades designadas de los Estados miembros y por la Oficina Europea de Policía (Europol) con fines de prevención, detección e investigación de los delitos de terrorismo y otros delitos graves y "activado" por la decisión del Consejo 2013/392/EU de 22 de julio de 2013 por la que se establece la fecha a partir de la cual surtirá efecto la Decisión 2008/633/JAI sobre el acceso para consultar el Sistema de Información de Visados (VIS) por las autoridades designadas de los Estados miembros y por Europol, con fines de prevención, detección e investigación de delitos de terrorismo y otros delitos graves.

23 Como requiere el capítulo 7 del Programa de Estocolmo - "Una Europa abierta y segura que sirva y proteja al ciudadano", DO C 115, 4.05.2010, p.1.

24 RAND Europe, *op.cit.*, p.114.

25 Artículo 42(2) del Convenio de Europol.

26 Acto del Consejo de 3 de noviembre de 1998 por el que se establecen las normas para las relaciones exteriores de Europol con los terceros Estados y los organismos no relacionados con la Unión Europea, DO C 88, 30.01.1999.

el Acto del Consejo de 12 de marzo de 1999[27]. Sobre esta base, el 27 de marzo de 2000, el Consejo de Ministros de justicia y asuntos de interior autorizó al director de Europol a iniciar negociaciones con una serie de países no europeos y organizaciones internacionales para concluir acuerdos bilaterales de cooperación, dando prioridad a los países candidatos y a los socios de la cooperación Schengen (entonces Islandia y Noruega), a Suiza y a Interpol.[28] A finales de 2004, ya habían entrado en vigor catorce acuerdos de cooperación[29].

La firma de un acuerdo de cooperación con Europol puede a menudo implicar reorganizaciones dentro de los ministerios de interior de los terceros países y la adopción de nuevas leyes nacionales.[30] Además, Europol organiza actividades de formación, intercambios, prácticas y seminarios durante los cuales acoge a funcionarios de terceros países y seminarios. De esta forma, Europol ha contribuido también a construir o reformar los sistemas de seguridad de terceros países, especialmente en zonas post-conflicto con instituciones débiles. Esta acción ha tenido más influencia en los países que miran o miraban hacia la ampliación. En particular, Europol ha contribuido a preparar a los países candidatos para la accesión a la UE para firmar acuerdos de cooperación.[31]

La entrada en la UE de trece nuevos países miembros entre 2004 y 2013 ha tenido como primera consecuencia directa que las relaciones con estos países hayan dejado de formar parte de la actividad exterior de Europol. Áreas del crimen organizado que se consideraban fuera de la UE han pasado a considerarse un asunto interno, y a la vez Europol se beneficia de la experiencia en esos sectores de los nuevos miembros que incorpora.

En 2007 entraron también en vigor los tres protocolos que modificaron la Convención de Europol. El tercero de ellos, el llamado "protocolo danés",[32] permite que los

---

27 Acto del Consejo de 12 de marzo de 1999 por el que se fijan las normas para la transmisión por Europol de datos personales a Estados y organismos terceros, DOUE C 88, 30.03.1999.

28 Decisión del Consejo de 27 de marzo de 2000 por la que se autoriza al director de Europol a entablar negociaciones sobre acuerdos con terceros Estados y organismos no relacionados con la Unión Europea (DO C 106, 13.4.2000, p.1). La lista se ha ido actualizando mediante sucesivas decisiones del Consejo. Decisión del Consejo 2009/935/JHA de 30 de noviembre de 2009 que determina la lista de terceros Estados y organizaciones con las que Europol debe concluir acuerdos, OJ L 325, 11.12.2009, p. 12.

29 Ver www.europol.europa.eu.

30 Gregory Mounier, "Europol: A New Player in the EU External Policy Field?", publicado en *Perspectives on European Politics and Society*, Vol.10, No.4, 582-602, Diciembre 2009. Routledge, Taylor & Francis Group, p.591.

31 Gregory Mounier, *op.cit.*

32 Protocolo establecido sobre la base del apartado 1 del artículo 43, del Convenio por el que se crea una Oficina Europea de Policía (Convenio EUROPOL) por el que se modifica el mencionado Convenio, Bruselas, 27 de noviembre de 2003 (BOE núm. 56/2007, de 6 de marzo de 2007).

terceros Estados que han concluido acuerdos de cooperación con Europol puedan participar en los ficheros de trabajo de análisis. La lista de terceros Estados y organizaciones con los que Europol puede celebrar acuerdos es elaborada por el consejo de administración y adoptada por el Consejo de la UE por mayoría cualificada, previa consulta del Parlamento Europeo.

2.3.1. Los acuerdos de cooperación estratégica y operativa

El envío de información a terceros países se enmarca en acuerdos con terceros Estados y organizaciones. En el momento de escribir este artículo, Europol cooperaba con diecinueve países terceros y tres organizaciones internacionales no europeas (ver fig.1).

Fig.1. Acuerdos de Europol con terceros países y organizaciones internacionales

Acuerdos de cooperación	
Operativa	**Estratégica**
Antigua República Yugoslava de Macedonia	Albania
Australia	Bosnia y Herzegovina
Canadá	Federación Rusa
Colombia	Moldavia
Croacia	Montenegro
EEUU	Serbia
Islandia	Turquía
Liechtenstein	Ucrania
Mónaco	Organización Mundial de Aduanas (OMA)
Noruega	Oficina de Naciones Unidas contra la Droga y el Delito (ONUDD)
Suiza	
Organización Internacional de Policía Criminal (Interpol)	

Fuente: https://www.europol.europa.eu

Europol puede concluir dos tipos de acuerdos: de cooperación estratégica y de cooperación operativa. Los primeros permiten el intercambio de información estratégica y técnica que no contiene datos personales. Pero los más codiciados por actores externos son los acuerdos operativos, puesto que incluyen el intercambio de datos personales, aportando un mayor valor añadido a las investigaciones[33].

Cuando un tercer país u organización internacional se incluye en la lista adoptada por el Consejo de Ministros, Europol ya puede iniciar negociaciones con éste/a. Sin embargo, en el caso de los acuerdos operativos, Europol debe previamente evaluar si la tercera parte en cuestión dispone de un nivel adecuado de protección de datos y obtener un dictamen de la Autoridad Común de Control (ACC)[34]. Una vez obtenida la

33 Gregory Mounier, *op.cit.*

34 Autoridad independiente de supervisión en materia de protección de datos, ver su composición en el apartado 3.3.b.

luz verde del consejo de administración, en función del resultado de la evaluación y del dictamen, el director inicia las negociaciones. Cuando éstas finalizan, el proyecto de acuerdo es sometido de nuevo a la ACC y al consejo de administración, que debe aprobarlo antes de someterlo al Consejo de ministros para su conclusión.[35]

Además, como veremos más adelante[36], Europol ejerce también un papel en la implementación del llamado "acuerdo TFTP" entre la UE y los EEUU relativo al tratamiento y la transferencia de datos de mensajería financiera (SWIFT) a efectos del programa del Departamento del Tesoro estadounidense relativo al seguimiento de la financiación del terrorismo (en adelante, "el acuerdo TFTP").[37]

3. La protección de datos en la acción exterior de Europol en contexto: el marco europeo de protección de datos y el antiguo tercer pilar

Como cualquier otro tratamiento de datos personales, las transferencias conllevan un riesgo de violación de los derechos fundamentales a la privacidad y a la protección de datos personales. En el caso de Europol, dichos tratamientos pueden incluir datos relativos a infracciones, condenas penales o medidas de seguridad, cuyo tratamiento conlleva riesgos mayores y es por tanto sujeto de una mayor protección. Si los datos son transferidos a terceros países u organizaciones, a ello se añaden otros riesgos específicos, como la posible pérdida de control sobre los datos una vez son enviados o el peligro de que los datos se expongan a regímenes de protección menos exigentes.[38]

A continuación analizaremos cuales son las normas de protección de datos que Europol debe respetar al transferir datos a terceros países y organizaciones y las situaremos en el sistema general de protección de datos europeo. Una vez establecido el contexto, examinaremos el marco aplicable a Europol.

Nos centraremos en las normas aplicables al tratamiento de datos operativos, dejando

---

35 El procedimiento para concluir acuerdos de cooperación se establece en la Decisión de Europol y la Decisión del Consejo 2009/934/JAI de 30 de noviembre de 2009 por la que se adoptan las normas de desarrollo que rigen las relaciones de Europol con los socios, incluido el intercambio de datos personales y de información clasificada (OJ L 325, 11.12.2009, p.6).

36 Ver el apartado 4.2.

37 *Op. cit.*

38 Ver, por ejemplo, la lista de riesgos que menciona la Comisión de Servicios Estatales de Nueva Zelanda con respecto a las transferencias internacionales, que incluye el incumplimiento de la ley nacional, la imposibilidad de garantizar la protección de los datos personales en países sin leyes de privacidad o de protección de datos, la posibilidad de conflictos entre leyes nacionales y leyes extranjeras, y el acceso a los datos por parte de gobiernos extranjeros, entre otros. (State Services Commission of New Zealand, "Government Use of Offshore Information and Communication Technologies (ICT) Service Providers: Advice on Risk Management", 2009, www.e.govt.nz/library/offshore-ICT-service-providers-april-2007.pdf, pp. 6-7, 14-15, and pp. 26-27, citado en Christopher Kuner, "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future", OECD Digital Economy Papers, No. 187, OECD Publishing, 2011, disponible en http://dx.doi.org/10.1787/5kg0s2fk315f-en, último acceso el 9.06.2013).

de lado el tratamiento de datos administrativos y de personal de Europol, y en las normas específicas relativas a las transferencias de datos. No profundizaremos, por tanto en otros principios y normas aplicables a los tratamientos en general (y por tanto, también a las transferencias), como los relativos a la calidad, la limitación de la finalidad, la protección de los datos sensibles, los derechos de información, acceso, rectificación y bloqueo, o la reparación judicial.

3.1. El marco europeo de protección de datos

En 1950, el Convenio Europeo de Derechos Humanos y Libertades Fundamentales (CEDH) sienta las bases del derecho al respeto de la vida privada[39]. En 1981, casi al mismo tiempo que las Directrices de la OCDE[40], el Convenio 108 del Consejo de Europa[41] se convierte en el primer instrumento regional vinculante de protección de datos, estableciendo unos principios que serán retomados, 14 años más tarde, por la Directiva 95/46/CE de protección de datos[42]. En 2001 al Convenio 108 se le añade un protocolo adicional dedicado a las transferencias internacionales y a las autoridades independientes encargadas de su supervisión[43] (en adelante "el Protocolo Adicional"). A diferencia del Protocolo Adicional, ambos convenios han sido ratificados por todos los Estados miembros de la UE. Además, la misma UE debería ser pronto parte del CEDH[44] y podría acceder también al Convenio 108[45]. Los tres instrumentos se aplican en principio a la totalidad del sector público y privado, incluyendo la cooperación judicial y policial e incluso el ámbito de la seguridad nacional[46].

---

39 Artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales de 4 de Noviembre de 1950.

40 Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales, 23.09.1980.

41 Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal, ETS No. 108, 28.01.1981.

42 Directiva 95/46/EC del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y la libre circulación de estos datos (DO L 281, 23.11.1995, p.31).

43 Protocolo adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de los datos personales, ETS No. 181, 8.11.2001.

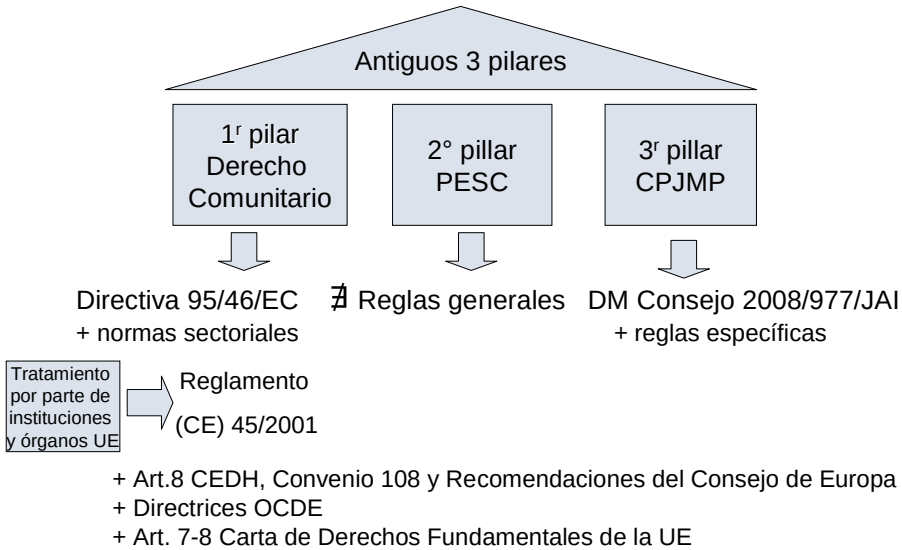
44 El Tratado de Lisboa convirtió la accesión de la UE al CEDH en una obligación. El 5 de abril de 2013 se llegó a un acuerdo sobre el borrador del acuerdo de accesión (ver https://wcd.coe.int/ViewDoc.jsp?Ref=DC-PR041(2013)&Language=lanEnglish&Ver=original&BackColorInternet=F5CA75&BackColorIntranet=F5CA75&BackColorLogged=A9BACE, última consulta el 1.06.2013).

45 Enmiendas al Convenio para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal (ETS No.108) para permitir la accesión de las Comunidades Europeas, 15.06.1999.

46 Sin embargo, algunos países han presentadas declaraciones de acuerdo con el artículo 3(2) del Convenio 108 para restringir su ámbito de aplicación.

Tanto el derecho a la vida privada como el derecho a la protección de datos han sido reconocidos también por la Carta de Derechos Fundamentales de la UE, que deviene vinculante con la entrada en vigor del Tratado sobre el Funcionamiento de la Unión Europea (TFUE)[47]. El TFUE, además, reconoce explícitamente el derecho a la protección de datos en su artículo 16, sentando las bases para la adopción de un nuevo marco legal en este ámbito. En el momento de escribir este artículo, podemos considerar que nos encontramos en un momento de transición entre la situación pre-Lisboa[48] y el marco post-Lisboa. Para entender la situación actual, partiremos por tanto de la situación anterior a la adopción del Tratado. Si tomamos como referencia la antigua estructura de pilares, con el derecho comunitario en el primer pilar, la política exterior y de seguridad común (PESC) en el segundo y la política de cooperación judicial y policial en materia penal (CPJMP) en el tercero, tenemos una imagen bastante clara de cómo se ha estructurado el marco de protección de datos (ver fig.2).

Fig.2. El marco de protección de datos pre-Lisboa



Fuente: elaboración propia

La Directiva 95/46/CE[49] de protección de datos se concibió como norma general de protección de los datos personales en los Estados miembros para el sector público y

47 Versión consolidada del Tratado de Funcionamiento de la Unión Europea, DO C 83, 30.03.2010, p.47.

48 En relación al Tratado de Lisboa por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea, firmado en Lisboa el 13 de diciembre de 2007, DO C 306, 17.12.2007, p.1. Ver también la nota 49 sobre las disposiciones transitorias.

49 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, 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 (DO L 281, 23.11.1995, p.31).

privado en el ámbito comunitario (primer pilar), implementada por leyes nacionales de protección de datos. Las instituciones y órganos de la UE disponen de un marco especifico, el Reglamento (EC) N° 45/2001[50] que, sobre la base de la Directiva 95/46/CE, regula aspectos específicos de este ámbito como la transferencia entre instituciones europeas, y crea el Supervisor Europeo de Datos (SEPD). Existen también normas para sectores concretos como las comunicaciones electrónicas[51].

En el antiguo tercer pilar, en cambio, no existe un marco general, sino una decisión marco del Consejo que cubre solamente las transferencias entre Estados miembros, dejando fuera los tratamientos dentro de cada Estado (en adelante, "la Decisión marco")[52], y normas específicas como la Decisión de Europol. En particular, la Decisión de Europol establece un régimen autónomo de protección de datos para dicha agencia. Si bien se inspira en el marco general de protección de datos, trata de responder a las necesidades específicas del tratamiento de datos en el ámbito de la cooperación policial.

La entrada en vigor del Tratado de Lisboa no sólo elimina la estructura de pilares[53], sino que además crea una nueva base legal, el artículo 16 del TFUE, para adoptar un marco casi comprehensivo de protección de datos mediante codecisión. La excepción es la PESC, cuyas normas de protección de datos deben adoptarse mediante una decisión del Consejo.[54] Además, las declaraciones anexas reconocen la especificidad de los ámbitos de la CPJMP y de la seguridad nacional[55].

La Comisión Europea propuso el 25 de enero de 2012 un nuevo marco de protección de datos, actualmente sujeto de acaloradas discusiones en el Parlamento Europeo y en

---

50 Reglamento (CE) N° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 2.01.2001, p.1)

51 Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (DO 201 de 31.7.2002, p. 37).

52 Decisión marco 2008/977/JAI del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, 27.11.2008, DO L 350, 30.12.2008, p.60).

53 Sometiendo los actos adoptados en este ámbito al control del Tribunal de Justicia de la UE (TJUE) y reemplazando para gran parte de las áreas de justicia y asuntos de interior el procedimiento de consulta al Parlamento y adopción por unanimidad del Consejo, por el procedimiento de codecisión y adopción por mayoría cualificada en el Consejo. Sin embargo, las nuevas competencias de la Comisión (como los procedimientos de infracción) y del TJUE sólo serán plenamente aplicables al acervo existente en el antiguo tercer pilar cinco años tras la entrada en vigor del TFUE, es decir, en diciembre de 2014 (ver el artículo 10 del Protocolo 36 del TFUE sobre disposiciones transitorias).

54 Ver el artículo 39 del TUE (DO C 83, 30.03.2010, p.13).

55 Declaraciones 20 y 21 anexas al Acta Final de la Conferencia intergubernamental que adoptó el Tratado de Lisboa (DO C 83, 30.03.2010, p.345).

el Consejo[56]. Sin embargo, en lugar de un marco único y prácticamente comprehensivo como permitía el TFUE, la propuesta contiene dos instrumentos legislativos distintos: un reglamento, dirigido tanto al sector privado y como al sector público (con algunas excepciones, como la CPJMP), y una directiva sólo para el ámbito de la CPJMP.

Además, tanto el reglamento como la directiva propuestos excluyen de su ámbito de aplicación a las instituciones y órganos de la UE[57] los actos específicos en el área de la cooperación policial y judicial -como las decisiones de Europol y Eurojust[58] - y el ámbito de la PESC, para el cual todavía no se ha propuesto ningún instrumento sobre la base del artículo 39 del TUE.

Poco antes de la última actualización de este artículo, ambas propuestas habían aprobadas, con numerosas enmiendas, por el pleno del Parlamento Europeo en primera lectura[59] y estaban siendo discutidas por el Consejo de la UE.

3.2. Las transferencias internacionales en el marco de protección de datos de Europol

3.2.1. Los principios: El Convenio 108 y la Recomendación 87(15)

La Decisión de Europol obliga a respetar los principios del Convenio 108 y de la Recomendación 87 (15) del Consejo de Europa sobre el uso de datos personales en el sector de la policía.[60] La decisión precisa que dichos principios también se aplicarán

---

56 Ver por ejemplo, el artículo "Legisladores se enfrentan en público sobre la propuesta de ley de protección de datos de la UE", publicado en *Euractiv* el 4-5.06.2013 (disponible en http://www.euractiv.com/infosociety/meps-clash-publicly-closed-doors-news-528285?utm_source=EurActiv%20Newsletter&utm_campaign=c2d92f5f52-newsletter_daily_update&utm_medium=email&utm_term=0_bab5f0ea4e-c2d92f5f52-245739993, último acceso el 8.06.2013).

57 El Reglamento (EC) No 45/2001 seguirá de aplicación mientras la Comisión no proponga un nuevo instrumento.

58 La Comisión ha publicado recientemente una propuesta para reformar esta última y planea proponer un nuevo reglamento sobre Eurojust (ver el Programa de Trabajo de la Comisión Europea para 2013, disponible en http://ec.europa.eu/atwork/pdf/cwp2013_es.pdf, último acceso el 8.06.2013).

59 Resoluciones legislativas del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) y sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos (COM(2012)0010 – C7-0024/2012 – 2012/0010(COD)).

60 Recomendación 87 (15) del Comité de Ministros del Consejo de Europa a los Estados miembros que regula el uso de los datos personales en el sector de la policía, 17.09.1987.

al tratamiento de datos *no* automatizados, de modo que amplía su ámbito de aplicación, a pesar de que sólo se somete a sus principios.

El Convenio 108 únicamente regula las transferencias a Estados no contratantes de forma indirecta, es decir, si se realizan a través de otro Estado parte. Según su artículo 12, una parte sólo podrá restringir las transferencias a otra parte si su legislación regula específicamente determinadas categorías de datos o ficheros (y la parte receptora no dispone de una legislación equivalente), o si éstas se envían a un Estado no contratante por intermedio del territorio de otra parte.

Las transferencias directas a terceros países se regulan en el Protocolo Adicional, todavía no ratificado por todos los Estados miembros de la UE. El protocolo establece el principio de que sólo pueden transmitirse datos personales a Estados u organizaciones que no son parte del Convenio si éstos garantizan “un nivel adecuado de protección”. Se permiten excepciones en el derecho interno para defender intereses concretos del afectado o intereses legítimos, especialmente los de carácter público; o si el destinatario proporciona “suficientes garantías”, por ejemplo mediante cláusulas contractuales. Este principio de "adecuación" se ha retomado en prácticamente todos los instrumentos legislativos de protección de datos en el ámbito de la UE.

La Recomendación 87(15)[61] se añade al Convenio 108 como marco específico para el tratamiento de datos en el ámbito de la policía. Sin embargo, a diferencia del Convenio, no tiene carácter vinculante. Aún así, su peso se demuestra en las numerosas referencias a la recomendación incluidas en instrumentos de la UE relativos a la cooperación policial.[62] El principio 5 de la Recomendación 87 (15) limita las "comunicaciones internacionales" a los cuerpos de policía y sólo las permite si existe una base legal clara bajo derecho nacional o internacional, o si son necesarias para la prevención de un peligro grave e inminente o para la supresión de un delito grave de acuerdo con la ley nacional. Las solicitudes de datos deben estar debidamente justificadas, los datos deben verificarse antes de comunicarse y no deben usarse para fines distintos a los de la comunicación. Además, la interconexión con ficheros destinados a otros fines sólo se permite bajo autorización de la autoridad independiente de protección de datos para una investigación concreta o si está previsto por ley.

3.2.2. El papel limitado de la Decisión marco del Consejo

El ámbito de aplicación de la Decisión marco incluye las transferencias de datos entre los Estados miembros, y entre los Estados miembros y las autoridades y sistemas de información creados bajo el antiguo tercer pilar[63]. Sin embargo, la Decisión de Europol especifica que ésta no se verá afectada por la Decisión marco, puesto que la Decisión de Europol "contiene disposiciones específicas sobre protección de datos

---

61 Recomendación No. 87(15) del Comité de Ministros del Consejo de Europa a los Estados miembros dirigida a regular la utilización de los datos de carácter personal en el sector de la policía.

62 Els de Busser, *Data Protection in EU and US Criminal Cooperation*, Maklu, 2009.

63 Artículo 2 de la Decisión marco.

personales que regulan estas cuestiones de forma más pormenorizada“.[64]

La Decisión marco se concibió para regular el tratamiento de datos personales en el antiguo tercer pilar, puesto que el marco general, la Directiva 95/46/EC, sólo se aplicaba al ámbito del derecho comunitario. Sin embargo, tras largas negociaciones, su ámbito de aplicación se limitó al intercambio transfronterizo de datos en la UE, dejando fuera el tratamiento de datos por parte de las autoridades policiales y judiciales dentro de los Estados miembros.

Esta limitación era de esperar, dada la sensibilidad y complejidad del área en cuestión. Sin embargo, un marco comprehensivo hubiera sido preferible, puesto que es complicado saber con exactitud con antelación qué datos recogidos por la policía a nivel nacional van a ser posteriormente enviados a otro Estado miembro. Además, esta limitación podría llevar a una paradójica situación de protección de los titulares de los datos recibidos de otros Estados miembros y de desprotección de aquellos cuyos datos son recabados y tratados a nivel nacional.[65]

A pesar de que la Decisión marco no se aplica a las transferencias directas por parte de un Estado miembro o de Europol a un tercer país u organización internacional, veremos brevemente las condiciones que requiere cuando un Estado miembro transmite datos personales a otro Estado miembro, y éste a su vez los transmite a un tercer Estado u organización.

En principio, los datos sólo pueden transmitirse si el tercer Estado u organismo internacional garantiza un nivel adecuado de protección y si la transferencia es necesaria para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o para la ejecución de sanciones penales. Además, la autoridad receptora debe ser competente para las mismas tareas relacionadas las infracciones penales y sanciones penales; y el Estado miembro que proporcionó los datos en primer lugar debe consentir la transferencia de acuerdo con su Derecho nacional.[66] De forma similar al Protocolo Adicional, la Decisión marco prevé excepciones, de acuerdo con la ley, si el receptor ofrece garantías adecuadas o si existen intereses legítimos del interesado o intereses superiores, refiriéndose en particular a "importantes intereses públicos".

3.2.3. La Decisión de Europol

La Decisión del Consejo de 2009, que reemplazó al Convenio de Europol, rige el funcionamiento de Europol y establece un marco legal específico para el tratamiento de datos por parte de esta agencia.

---

64 Ver el considerando 12 de la Decisión de Europol.

65 Emilio Aced Félez, “Principio de Disponibilidad y protección de datos en el ámbito policial”, *Noticias Jurídicas*, abril 2010 (disponible en http://noticias.juridicas.com/articulos/15-Derecho%20Administrativo/201004-123095321697634.html, última consulta el 2.06.2013)

66 Artículo 13 de la Decisión marco.

El principal requisito que la Decisión de Europol establece para la transferencia de datos a terceros países es la celebración de un acuerdo de cooperación operativo si, tras una evaluación del nivel de protección de datos ofrecido por la entidad receptora, se concluye que éste es adecuado.[67] Además, los datos transmitidos a Europol por un Estado miembro sólo pueden transferirse a terceros países y organizaciones internacionales con el acuerdo de ese Estado miembro[68]. Para el resto de datos, Europol debe cerciorarse de que su transferencia no supone un peligro para ningún Estado miembro[69]. En cualquier caso, la transferencia debe ser necesaria en el caso particular para prevenir y luchar contra las infracciones penales competencia de Europol[70]. Este último requerimiento es importante puesto que tiene el objetivo de evitar la transferencia masiva de datos y requiere la existencia de una sospecha o una investigación concreta para justificar el intercambio de datos.

En casos excepcionales, la Decisión de Europol permite la transferencia de datos incluso si no existe un acuerdo internacional, pero sólo si el director considera que es absolutamente necesario para proteger los intereses esenciales de los Estados miembros o para prevenir un peligro inminente relacionado con el terrorismo. De todas formas, antes de autorizar la transferencia, el director debe evaluar el nivel de protección de datos del organismo receptor. La Decisión impone un control independiente a posteriori mediante la obligación de informar a la ACC, así como al consejo de administración, de su decisión y de la base de la evaluación del carácter adecuado del nivel de protección de datos del destinario.

3.2.4. Reglas específicas

El Acto del Consejo de 12 de marzo de 1999 que establece las normas generales para la transmisión por parte de Europol de datos personales a Estados y organismos terceros, citado más arriba, es analizado en el capítulo X. Pero las reglas específicas en relación a cada tercer Estado u organización se establecen en cada uno de los doce acuerdos operativos, cuyo contenido no se entra a analizar en este libro.

3.3. Supervisión

Para asegurar que estas normas de protección de datos se cumplen, la Decisión de Europol establece un sistema de supervisión interna, mediante el responsable de la protección de datos (DPO, en sus siglas en inglés), y uno externo, a través de las autoridades nacionales de control y de la autoridad común de control (ACC). Este apartado examina las tareas de supervisión del DPO y la ACC, puesto que las autoridades nacionales de control no supervisan el tratamiento y transferencia de datos por parte de Europol, sino la introducción, consulta y transmisión de datos a

67 Artículos 23(2) y 23(6)(b).

68 Artículo 24(1).

69 Artículo 24(1)(a-b).

70 Artículo 23(6)(a).

Europol por parte de los Estados miembros.[71]

3.3.1. El responsable de la protección de datos (DPO)

Dentro de la estructura de Europol, el DPO se encarga de controlar que el tratamiento de datos personales se efectúe conforme a la Decisión de Europol y de asesorar a la agencia en este sentido. Dicha decisión establece que debe realizar sus tareas de forma independiente[72], pero la oficina del DPO se compone de miembros del personal de Europol, de modo que lleva a más exactamente una función de control interno.

El DPO también debe asegurarse de que cada transmisión y recepción de datos quede registrada, y de que se informe a las personas interesadas sobre el tratamiento de sus datos y sobre sus derechos al respecto. Para tal propósito, debe cooperar tanto con el personal de Europol, al que debe asesorar, como con la ACC, y debe tener acceso a todos los locales y a todos los datos tratados por Europol.

Si considera que se están incumpliendo las normas de protección de datos, el DPO debe informar al director y pedirle que resuelva el problema. Si aun así el director no lo resuelve, el DPO debe informar al consejo de administración. Aunque este caso prácticamente no se da, funciona muy bien como factor disuasorio.[73] En el caso de que el consejo de administración tampoco solucionara el problema, la última instancia sería la ACC. Además, cada año, el DPO debe elaborar un informe y transmitirlo a la ACC y al consejo de administración de Europol.

El DPO también asesora a Europol en sus negociaciones con terceros países y organizaciones y, en particular, en la evaluación de su nivel de protección de datos. La oficina del DPO no sólo analiza las normas de protección de datos de dichas terceras partes sino que también realiza visitas y evaluaciones sobre el terreno para verificar si se cumplen en la práctica.[74]

3.3.2. La Autoridad Común de Control (ACC)

El artículo 34(1) de la Decisión de Europol crea la ACC, encargada de supervisar, de forma independiente, el tratamiento de datos personales por parte de Europol para garantizar que no vulnere los derechos de las personas afectadas. La ACC está compuesta por entre uno y dos representantes (más los respectivos suplentes, en algunos casos) de cada una de las autoridades independientes de protección de datos de los Estados miembros. La Decisión de Europol prohíbe de forma explícita a los miembros de la ACC recibir instrucciones de cualquier otra autoridad, con el fin de garantizar su independencia. Los representantes son nombrados por un periodo de

71 Por falta de espacio, tampoco trataremos el ejercicio de los derechos de acceso y rectificación de los datos.

72 Artículo 28(1).

73 Entrevista en Bruselas, 14.06.2013.

74 Europol, *Data protection at Europol*, Oficina de Publicaciones de la UE, 2012.

cinco años y cada delegación dispone de un voto. La ACC elige su presidente y vicepresidente entre sus miembros[75].

La competencia de supervisión de la ACC se complementa con la obligación de Europol de facilitar su tarea, por ejemplo mediante la facilitación a la ACC del acceso libre en todo momento a los locales de Europol, así como a todos sus expedientes, documentos y datos almacenados.

En caso de que la ACC descubra que Europol no ha tratado los datos de acuerdo con la Decisión de Europol, debe comunicárselo al director de Europol y solicitarle una respuesta, fijando ella misma un plazo. Si el problema persiste, puede dirigirse directamente al consejo de administración, aunque en la práctica, no suele ser necesario.[76]

En relación a los acuerdos operativos con países y organizaciones terceros, la ACC debe emitir un dictamen antes del inicio de las negociaciones por parte del director de Europol, y otro antes de la conclusión del acuerdo. El consejo de administración debe tener en cuenta estos dictámenes en su decisión de autorizar el inicio de las negociaciones y de someter el acuerdo al Consejo de la UE.[77]

La ACC está obligada a presentar regularmente informes de su actividad al Parlamento Europeo y al Consejo de la UE. El consejo de administración tiene el derecho de adjuntar sus comentarios al informe, pero es la propia ACC la que decide si deben publicarse estos informes y cómo. En la práctica la ACC los elabora cada dos años y los publica en su página web[78].

3.3.3. El nivel de cumplimiento

Para evaluar si los tratamientos de datos por parte de Europol y, en particular, las transferencias internacionales cumplen con las normas de protección de datos, deberíamos tener acceso a los informes de las inspecciones del DPO y de la ACC, que no son públicos. No obstante, la ACC publica informes de su actividad y resúmenes de sus informes anuales de inspección que proporcionan información general. En este sentido, el informe de actividad de 2008-2012 concluye que, en general, el tratamiento de datos por parte de Europol cumple con el marco legal.

---

75 En el momento de escribir este artículo la presidenta de la ACC era la eslovena Nataša Pirc Musar.

76 Entrevista en Madrid, 20.05.2013.

77 Artículo 23(2) de la Decisión de Europol y Artículo 6 de la Decisión del Consejo 2009/934/JAI, de 30 de noviembre de 2009, por la que se adoptan las normas de desarrollo que rigen las relaciones de Europol con los socios, incluido el intercambio de datos personales y de información clasificada, DO L 325, 11.12.2009, p.6.

78 Ver http://europoljsb.consilium.europa.eu/reports/activity-report.aspx?lang=en, último aceso el 29.06.2013.

Sin embargo, las inspecciones se basan necesariamente en "porciones" del tratamiento de datos y suelen centrarse en temas y AWF concretos, de modo que, incluso si tuviéramos acceso a los informes, sería difícil evaluar el nivel real de cumplimiento. Por su parte, la evaluación de RAND Europe concluye que la percepción que existe es que Europol dispone de un régimen de protección de datos robusto y en el cual los actores relevantes (Estados miembros, ACC, personal de Europol, etc.) tienen confianza. Los actores entrevistados consideran que ello contribuye a la credibilidad de la agencia y facilita el intercambio de datos.[79]

Respecto a las transferencias internacionales, parece que Europol cumple en general con la obligación de celebrar acuerdos y de involucrar a la ACC en su evaluación. Las recomendaciones de la ACC suelen ser tomadas en cuenta por Europol en la negociación de los acuerdos.[80] Es interesante mencionar que Europol -como la ACC-, a través de su experiencia en la negociación de acuerdos y de los sucesivos dictámenes de la ACC, se ha beneficiado de un aprendizaje progresivo. Así, los acuerdos propuestos son cada vez mejores desde el punto de vista de protección de datos y la ACC necesita cada vez hacer menos recomendaciones para su mejora.[81]

La posibilidad, en casos excepcionales, de realizar transferencias a terceros países fuera del marco de los acuerdos, permitida por la Decisión de Europol, se ha interpretado adecuadamente de forma restrictiva.[82] Según el DPO, no está claro en qué debe basarse la decisión del director de autorizar una transferencia y, además del nivel de protección de datos del país receptor, deberían tomarse en cuenta criterios como el respeto de los derechos humanos, el sistema judicial, la efectividad de las investigaciones, el nivel de corrupción o la existencia de la pena de muerte. La ACC, en cambio, opina que el artículo 23(8-9) es suficientemente claro en este sentido y suficientemente amplio como para permitir tomar en cuenta otros factores.[83]

Sin embargo, tanto el control por parte del DPO como por parte de la ACC se limita a la realización de la transferencia por parte de Europol. Una vez los datos están en

---

79 RAND Europe, *op.cit.*, p.92. Uno de los problemas detectados por la evaluación de impacto de la Comisión Europea sobre la nueva propuesta de Reglamento de Europol es que los Estados miembros no proporcionan a Europol toda la información necesaria para luchar contra el crimen transfronterizo, o no la proporcionan a tiempo, a pesar de que la Decisión de Europol les obliga a ello. Sin embargo, las causas apuntadas en la evaluación no se refieren a la preocupación sobre la protección de los datos, sino más bien a la imprecisión de la legislación, a factores sociológicos y culturales (falta de concienciación, cultura policial cautelosa con el intercambio de información), y a factores organizativos (efectividad de las Unidades Nacionales de Europol establecidas en cada Estado miembro) (Ver el Documento de trabajo de la Comisión. Resumen ejecutivo de la evaluación de impacto sobre la adaptación del marco legal de Europol al Tratado de Lisboa (SWD(2013) 99 final)).

80 Entrevista en Madrid, 20.05.2013.

81 *Idem.*

82 Entrevista en Bruselas, 14.06.2013.

83 RAND Europe, *op.cit.*, p.114.

manos del tercer país u organización internacional, es complicado controlar si cumple con las condiciones del acuerdo (por ejemplo, si los datos se utilizan para fines diferentes a los permitidos o si se conserva durante más tiempo del necesario).[84]

El papel de Europol en la implementación del acuerdo TFTP, que veremos a continuación, también es supervisado por la ACC, la cual le dedica informes de inspección específicos. A pesar de que en su mayoría tampoco son públicos, la ACC ha decidido realizar versiones públicas de dichos informes, debido al interés y a las críticas que ha suscitado este acuerdo. De hecho, la transparencia de los informes de la ACC ha sido objeto de controversia entre la ACC, el consejo de administración de Europol, el Parlamento Europeo, la Comisión Europea y los EEUU[85].

Teniendo en cuenta esta mayor disponibilidad de información, su relevancia tanto por lo que respecta a la protección de datos como a las relaciones con terceros países, y la implicación de Europol, el acuerdo TFTP resulta un caso de estudio interesante. Su negociación en pleno proceso de entrada en vigor del TFUE y de adaptación al nuevo equilibrio institucional merece también una atención particular.

4. El acuerdo TFTP o el caso "SWIFT"

4.1. Antecedentes

4.1.1. SWIFT, el 11S y el inicio del TFTP

La Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT, en sus siglas en inglés) es una cooperativa localizada en Bélgica, activa en el tratamiento de mensajes financieros y controlada por varios bancos centrales. Se trata de una plataforma privada de intercambio de información en la cual cada miembro dispone de un código único, el llamado código "SWIFT", que permite a sus clientes enviar la información necesaria para realizar transferencias.

---

84 Entrevista en Bruselas, 14.06.2013.

85 Por ejemplo, el gobierno estadounidense ha criticado la decisión de la ACC de permitir a miembros del Parlamento Europeo el acceso a su informe de inspección sin consultar ni a Europol ni a EEUU, en lo que consideró "una clara violación de las reglas de seguridad aplicables y un quebrantamiento de la confianza mutua". (Ver el informe de la segunda revisión de la implementación del acuerdo TFTP (SWD(2012) 454 final, p.16, disponible en http://ec.europa.eu/dgs/home-affairs/pdf/20121214_joint_review_report_tftp_en.pdf, último acceso el 8.06.2013). La eurodiputada Sophie In't Veld ha llevado sus demandas de transparencia sobre documentos relacionados con el acuerdo TFTP al Tribunal de Justicia de la UE (caso T-529/09 Sophie in 't Veld v. Consejo de la UE). Ver también la solicitud confirmatoria de la misma diputada sobre el informe de inspección de la ACC, (31.08.2012), disponible en http://site.d66.nl/internationaal/document/brief_europol/f=/vj2ihwdrggl7.pdf, último acceso el 9.06.2013). Encontramos otro ejemplo en uno de los informes de actividad de la ACC, en el que el consejo de administración considera contradictorio que la ACC decida no publicar sus informes de inspección a causa de su contenido, pero que al mismo tiempo justifique la versión pública del informe de inspección de la implementación del TFTP por el "interés público" que suscita. (Ver el quinto informe de la actividad de la ACC, 2008-2012, disponible en http://www.privacycommission.be/sites/privacycommission/files/documents/gco-europol-5e-activiteitenverslag.pdf, último acceso el 8.06.2013).

Con cada transferencia de dinero, los clientes de los bancos miembros transmiten también datos personales del remitente y el destinatario de la transferencia. Estos datos pueden incluir, por ejemplo, su nombre, número de identificación nacional, dirección y número de cuenta. Hasta finales de 2009, SWIFT disponía de dos centros de operaciones, uno en Europa (Países Bajos) y otro en Estados Unidos. Por motivos de seguridad, todos los mensajes procesados por SWIFT se almacenaban en ambos centros mediante un sistema de almacenaje "en espejo".

Tras los ataques terroristas del 11 de septiembre de 2001, la Administración Bush estableció el Programa de Seguimiento de la Financiación del Terrorismo ("TFTP", por sus siglas en inglés). En el marco de este programa, el Departamento del Tesoro de EEUU ("UST") cursó requerimiento administrativo al centro operativo de SWIFT en EEUU solicitando datos de transferencias bancarias dentro y fuera de EEUU que pudieran estar relacionados con el terrorismo. Teniendo en cuenta la arquitectura de SWIFT y el tipo de requerimiento del UST, ello implicaba transferir al UST incluso datos sobre transferencias intraeuropeas, sin la autorización de las agencias nacionales de protección de datos, y por supuesto, sin el conocimiento de los ciudadanos europeos.

4.1.2. El TFTP sale a la luz

El escándalo se desató cuando el programa llegó a conocimiento de la prensa estadounidense a finales de junio de 2006[86]. En julio de ese mismo año el Parlamento Europeo adoptó una resolución requiriendo explicaciones a las autoridades nacionales y europeas sobre la legalidad de dichas transferencias y sobre la ausencia de reacción del Banco Central Europeo ante esta posible violación de la protección de datos. Al mismo tiempo, varias denuncias fueron presentadas ante las agencias de protección de datos de diferentes países[87].

Puesto que SWIFT estaba establecida en Bélgica, la agencia belga de protección de datos se encargó de la investigación, concluyendo en septiembre de 2006 que se había "sometido a vigilancia durante años a una cantidad masiva de datos personales de forma secreta y sistemática, sin justificación suficiente y clara y sin control independiente conforme al derecho belga y europeo"[88]. En lugar de recurrir los requerimientos del UST ante los tribunales estadounidenses, SWIFT decidió negociar directamente con el Tesoro para obtener algunas garantías de protección de datos. La agencia de protección de datos consideró que éstos no cumplían con los requisitos

86 Ver Eric Lichtblau y James Risen, "Bank Data Is Sifted by U.S. in Secret to Block Terror", *The New York Times*, 23 de junio de 2006, disponible en http://www.nytimes.com/2006/06/23/washington/23intel.html?hp&ex=1151121600&en=18f9ed2cf37511d5&ei=5094&partner=homepage&_r=0, último acceso el 9.06.2013)

87 Dictamen del SEPD sobre el papel del Banco central Europeo en el caso SWIFT.

88 Dictamen 37/2006 del 27 de septiembre de 2006 de la Comisión Belga para la Protección de la Intimidad relativa a la transferencia de datos personales por parte de SWIFT por los requerimientos del UST (OFAC), pág.27, disponible (en francés y en holandés) en http://www.privacycommission.be/sites/privacycommission/files/documents/avis_37_2006_0.pdf.

establecidos por la Convención Europea de Derechos Humanos, la Convención 108, la Directiva 95/46/CE y la ley belga. Aunque reconoció que SWIFT se encontraba en una situación de conflicto entre el derecho estadounidense y el derecho europeo, le acusó de graves errores de evaluación en el tratamiento de los requerimientos del UST. El dictamen argumenta que si las agencias de protección de datos, el gobierno belga y la Comisión Europea hubieran sido informados, se hubiera podido buscar a tiempo una solución a escala europea.

Por su parte, el Supervisor Europeo de Protección de Datos (SEPD) se encargó de examinar la implicación del Banco Central Europeo (BCE). Como el resto de miembros del grupo supervisor de SWIFT (el G-10), el BCE fue informado en 2002 de las transferencias a los EEUU, pero decidió no comunicarlo por motivos de confidencialidad y porque consideraba que quedaba fuera de sus tareas como supervisor. En su dictamen, el Grupo del Artículo 29[89] acusó también a las instituciones financieras de la UE, como responsables de los datos, de no haberse asegurado de que SWIFT cumplía con la ley.[90]

En 2007 el UST accedió a una serie de compromisos unilaterales (las "declaraciones TFTP")[91] sobre la protección de los datos tratados en el marco del TFTP. Sin embargo, dos hechos cambiarían el curso de los eventos.

4.1.3. El Parlamento Europeo entra en acción

Como consecuencia de las críticas y tras negociaciones con la agencia belga de protección de datos y con las autoridades europeas y estadounidenses[92], SWIFT adoptó una nueva estructura a partir del 1 de enero de 2010. Tal como había anunciado anteriormente,[93] SWIFT abandonaría el almacenamiento de datos de transferencias intra-europeas en su centro de EEUU, dejándolos fuera del alcance de los requerimientos administrativos del UST a menos que se alcanzara un acuerdo con las autoridades europeas.

Prácticamente al mismo tiempo, el 1 de diciembre de 2009 entró en vigor el Tratado

---

89 Grupo independiente con funciones de asesoramiento que reúne a un representante de cada agencia nacional de protección de datos de la UE, al SEPD y a la Comisión Europea. Fue creado por el artículo 29 de la Directiva 95/46/EC.

90 Dictamen del Grupo del Artículo 29 de 22 de noviembre de 2006.

91 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 (DO 166, 20.07.2007, p.18).

92 Resumen del informe de la primera inspección de la ACC sobre la implementación del acuerdo TFTP por parte de Europol.

93 Ver el anuncio público de SWIFT, disponible en http://www.swift.com/about_swift/legal/swift_announces_plans_for_system_re_architect, último acceso el 9.06.2013).

de Lisboa. Una de sus consecuencias sería el requisito del consentimiento del Parlamento Europeo para la conclusión de acuerdos internacionales. De repente, la decisión sobre el acceso del Departamento del Tesoro a los datos de SWIFT estaba en manos del Parlamento Europeo.

A finales de 2009 el Consejo de la UE firmó un acuerdo provisional con el UST[94] para dar continuidad al programa a partir del 1 de febrero de 2010. La Comisión Europea se mostraba convencida de la utilidad del TFTP, justificada por los informes del juez Bruguière (ver más adelante), y deseaba garantizar la continuación del programa tras el cambio de arquitectura de SWIFT. Sin embargo, el acuerdo provisional de 2009 preveía que, tan pronto como entrara en vigor el Tratado de Lisboa, las partes empezaran las negociaciones para reemplazar el acurdo interino por un acuerdo a largo plazo.

Haciendo uso de sus nuevas competencias, y tras duras críticas al Consejo y a la Comisión por la falta de información sobre las negociaciones, el Parlamento Europeo rechazó el acuerdo propuesto en febrero de 2010, considerando que no respetaba los derechos fundamentales de los ciudadanos europeos[95]. La Comisión, el Consejo y el UST se dieron cuenta rápidamente de que, a partir de ese momento, deberían respetar la opinión del Parlamento Europeo, con una competencia nueva en el ámbito de la UE, pero que no era extraña al Congreso americano[96]. Las reacciones no se hicieron esperar. El mismo día, la Comisión aseguró que empezaría a trabajar con los EEUU para conseguir un acuerdo aceptable para el Parlamento[97].

Por su lado, la Administración Obama advirtió que el rechazo al acuerdo perturbaría los esfuerzos de seguimiento de sospechosos de terrorismo y supondría un retroceso en la cooperación antiterrorista.[98] Además, la urgencia para concluir un nuevo acuerdo también estaba motivada por el hecho de que SWIFT almacenaba los datos únicamente durante 124 días, con lo cual, si Estados Unidos dejaba de tener acceso al sistema durante un periodo más largo, perdería la oportunidad de analizar parte de los

---

94 Ver la decisión del Consejo de 27 de noviembre de 2009, disponible en http://register.consilium.europa.eu/pdf/en/09/st16/st16110.en09.pdf, último acceso el 1.07.2013.

95 Ver los detalles del procedimiento y las exigencias del Parlamento Europeo en http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?id=579849, último acceso el 1.07.2013.

96 Sobre la percepción del Congreso americano sobre el Parlamento Europeo ver Kristin Archick, *The European Parliament*, Congressional Research Service, 2013, disponible en http://www.fas.org/sgp/crs/row/RS21998.pdf (último aceso el 29.06.2013), donde menciona el ejemplo del TFTP para ilustrar las consecuencias de las nuevas competencias del Parlamento Europeo adquiridas bajo el Tratado de Lisboa.

97 Comunicado de prensa de la Comisión Europea del 11 de febrero de 2010: "El Parlamento Europeo vota contra el acuerdo provisional entre la UE y los EEUU sobre la transferencia de datos bancarios para la lucha contra el terrorismo: reacción de la Comisión" (IP/10/152).

98 Washington Post, "U.S. blasts E.U. rejection of deal to share bank data", 12.02.2010, disponible en http://articles.washingtonpost.com/2010-02-12/news/36871701_1_european-parliament-bank-data-obama-administration, último acceso el 9.06.2013).

datos transmitidos.

En menos de un mes, la Comisión propuso un nuevo mandato de negociación para un acuerdo[99] que reflejara, en la medida de lo posible, las exigencias del Parlamento Europeo. Estos requerimientos incluían la limitación estricta del objetivo de las transferencias a la lucha contra el terrorismo, la exclusión de los datos del sistema europeo de pagos (SEPA), la prohibición de las transferencias en bloque, la limitación a cinco años el periodo de conservación de los datos, la posibilidad de denunciar el acuerdo en caso de incumplimiento de las normas de protección de datos y el derecho a la reparación administrativa y judicial.

Además, el Consejo y la Comisión se comprometieron a establecer un marco técnico y legal que permitiera la extracción y selección de los datos SWIFT en suelo europeo, evitando la transferencia masiva a EEUU para su análisis: el "Sistema Europeo de Seguimiento del Terrorismo" (TFTS en sus siglas en inglés). Sin embargo, tras una Comunicación en 2011[100] y otra a finales de 2013, acompañada de un análisis de impacto, la Comisión ha concluido que la necesidad de establecer tal sistema no está claramente demostrada[101].

El nuevo acuerdo TFTP fue firmado el 28 de junio de 2010 para un periodo de cinco años renovable. El Parlamento Europeo otorgó su consentimiento un mes más tarde, posibilitando la conclusión del acuerdo.

Cabe destacar que a finales de 2010 la Comisión obtuvo también el mandato del Consejo para negociar con los EEUU un acuerdo marco para el intercambio y la protección de datos personales en la lucha contra el terrorismo y la criminalidad,[102] sobre la base del trabajo del Grupo de Contacto de Alto Nivel entre la UE y EEUU sobre intercambio de información y protección de datos (EU-U.S. HLCG en sus siglas en ingles), establecido en 2006. Tras años de negociación sin grandes avances, las revelaciones de Snowden en verano de 2013 parecen haber dado un impulso a la voluntad política de ambas partes para lograr un acuerdo.

4.2. El papel de Europol en la gestión del acuerdo TFTP

---

99 Recomendación de la Comisión al Consejo del 24 de marzo de 2010 para autorizar la apertura de negociaciones entre la Unión Europea y los Estados Unidos de América para poner a disposición del Departamento del Tesoro de los Estados Unidos los datos de mensajería financiera necesarios para la prevención y la lucha contra el terrorismo y la financiación del terrorismo. Ver el comunicado de prensa de la misma fecha: “La Comisión Europea prepara nuevas negociaciones con los EEUU sobre la transferencia de datos bancarios para la lucha contra el terrorismo” (IP/10/348) y el MEMO/10/101.

100 Comunicación de la Comisión Europea 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.

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

102 Ver el comunicado de prensa de la Comisión de 3 de diciembre de 2010, disponible en http://europa.eu/rapid/press-release_IP-10-1661_en.htm, último acceso el 1.07.2013.

Una de las demandas del Parlamento Europeo era la verificación por parte de una autoridad judicial de cada una de las solicitudes de datos por parte del UST. A pesar de que la segunda propuesta de mandato de la Comisión de 2010 incluía este punto[103], en el texto final este requisito fue sustituido por una verificación por parte de Europol, establecida en el artículo 4(3-5) del acuerdo TFTP.

Esta elección se criticó, en primer lugar, porque evidentemente Europol no es una autoridad judicial. En segundo lugar, se argumentó que Europol no puede ser imparcial en esta tarea, ya que el acuerdo le permite beneficiarse también de los datos enviados al UST. Esta reciprocidad se establece en los artículos 7(d), 9 y 10, según los cuales el UST debe enviar información espontáneamente o bajo demanda a los Estados miembros de la UE, a Europol o a Eurojust.

4.3. La supervisión del acuerdo

4.3.1. Supervisión independiente del papel de Europol: la ACC

Como parte de sus tareas de supervisión, la ACC supervisa el papel de Europol en la implementación del acuerdo TFTP, con el fin de asegurar que respeta los principios y normas de protección de datos contenidos en el Convenio 108, la Recomendación 87 (15), la Decisión de Europol, el acuerdo TFTP y los procedimientos internos de tratamiento de información operativa. En concreto, controla que los datos sean adecuados, pertinentes, no excesivos, correctos y exactos en relación a las finalidades para las que se recabaron y trataron posterioremente.

Entre noviembre de 2010 y junio de 2013 la ACC dedicó tres inspecciones a la aplicación del TFTP. Los informes revelan que Europol ha aprobado todas las solicitudes de datos de SWIFT por parte del UST. En un primer momento, el UST proporcionaba información oral sobre las solicitudes, de modo que la ACC no podía evaluar realmente si la verificación por parte de Europol se había realizado de forma correcta.[104] Esta deficiencia se corrigió tras las recomendaciones de la ACC. Los informes también confirman que Europol no tiene acceso a los datos solicitados, de acuerdo con lo que estipula el acuerdo, y que no conoce la magnitud de las transferencias. El UST tampoco proporcionó a la ACC información concreta sobre la cantidad de datos enviados.

Tras los primeros informes de inspección, Europol mantuvo contactos con el UST con el fin de poner en práctica las recomendaciones de la ACC. Ello se refleja, por ejemplo, en el papel del DPO, que aconsejó al UST sobre como mejorar las solicitudes. Sin embargo, la ACC considera que el hecho de que las recomendaciones

---

103 La propuesta no se publicó, pero su resumen puede consultarse en http://europa.eu/rapid/press-release_MEMO-10-101_en.htm?locale=en, última consulta el 9.06.2013.

104 ACC, "US and EU agreement on exchanging personal data for the purposes of the Terrorist Finance Tracking Program (the TFTP Agreement1) – first inspection performed by the Europol Joint Supervisory Body (JSB) raises serious concerns about compliance with data protection principles", p.2, disponible en http://europoljsb.consilium.europa.eu/media/112160/jsb%20tftp%20inspection%20-%20website%20notice,%20march%202011.pdf, último acceso el 1.07.2013.

del DPO se repitan constantemente muestra que su consejo no se tiene en cuenta.[105]

La conclusión más polémica es que Europol recibe de media por parte de EEUU una solicitud al mes que cubre datos relativos a un periodo aproximado de un mes, como también explica el documento de trabajo de la Comisión sobre la segunda revisión conjunta del acuerdo en 2012[106]. Los datos que SWIFT está enviando a EEUU cubren "cada día del año, año tras año"[107] y las solicitudes comprenden un ámbito geográfico parecido. Y es que aparentemente el TFTP no permite realizar solicitudes más acotadas.[108]

Sobre la base de estos hechos, la ACC concluye que, si se confirma que la naturaleza del TFTP impide acotar el periodo de tiempo o las zonas geográficas concernidas por las solicitudes, resulta imposible en la práctica dar cumplimiento al requisito de que las solicitudes sean específicas y acotadas.

4.3.2. Supervisión por parte de una persona nombrada por la Comisión Europea

En su compromiso unilateral, el UST accedió, "como signo de compromiso y colaboración en la lucha contra el terrorismo global", a que una "personalidad europea eminente" verificara si el UST cumplía con sus declaraciones, en particular en lo que se refiere al tratamiento de datos procedentes de la UE. Las declaraciones del UST mencionan, por ejemplo, que los datos no pueden tratarse para fines diferentes a la lucha contra el terrorismo, que deben eliminarse tras un periodo de tiempo determinado y que no se pueden realizar búsquedas sobre los datos obtenidos excepto en casos en que hay razones para creer que existe una relación con el terrorismo.

En 2008 el juez Bruguière fue nombrado como "personalidad eminente" por la Comisión Europea, tras consultar al UST, con la obligación de informar una vez al año sobre su trabajo a la Comisión, la cual debe a su vez informar al Parlamento Europeo y al Consejo. Los informes no son públicos, pero la Comisión Europea presenta comunicados de prensa sobre éstos. Según estos comunicados, el UST

---

105 ACC, "Europol inspects for the second year the implementation of the TFTP agreement – Public statement", disponible en http://europoljsb.consilium.europa.eu/media/205081/tftp%20public%20statement%20-%20final%20-%20march%202012.pdf, p.2 (último acceso el 9.06.2013).

106 Commission staff working document - Report on the second joint review of the implementation of the Agreement between the European Union and the United States of America 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, octubre de 2012 (disponible en http://ec.europa.eu/dgs/home-affairs/pdf/20121214_joint_review_report_tftp_en.pdf, p. 6, último acceso el 5.04.2014).

107 ACC, *op.cit.*

108 ACC, "Implementation of the TFTP Agreement: assessment of the follow-up of the JSB recommendations" (Ref. 13-01), p.2. disponible en http://europoljsb.consilium.europa.eu/media/250972/13-01%20report%20art%204%20tftp%20inspection%202012.pdf, último acceso el 1.07.2013.

respeta sus compromisos y el TFTP proporciona un valor añadido considerable a la lucha contra el terrorismo tanto en EEUU como en la UE. También mencionan que el informe establece recomendaciones para mejorar la implementación del acuerdo, pero no especifican cuáles [109]. Una versión filtrada del informe de 2010 revela que una de estas recomendaciones se refiere a actividades de formación para acotar mejor las búsquedas y reducir así la cantidad de datos solicitados. Aún así, el informe concluye con una muy buena valoración de la implementación del acuerdo. [110]

El artículo 12 del acuerdo TFTP de 2010 establece una supervisión "independiente" por parte de una persona designada por la Comisión Europea, con el acuerdo y la autorización de los EEUU. Sin embargo, esta supervisión se ve limitada respecto a su independencia, puesto que está designada por las partes interesadas en el acuerdo y respecto a su alcance, ya que controla el uso de los datos ya enviados a EEUU, no el envío de dichos datos o el alcance o la proporcionalidad de las solicitudes del UST.

a) Supervisión conjunta del acuerdo por parte de la UE y EEUU (UST)

El artículo 13 del acuerdo TFTP establece una revisión conjunta por parte de representantes de la UE y del UST (que forman el equipo conjunto de revisión o JRT, en sus siglas en inglés) seis meses después de la entrada en vigor del acuerdo, y posteriormente de forma regular. A petición de una de las partes, el equipo conjunto de revisión debe examinar las garantías, los controles y las cláusulas de reciprocidad que contiene el acuerdo. El equipo de revisión europeo está liderado por la Comisión Europea pero incluye dos representantes de las autoridades nacionales de protección de datos de la UE.

La primera revisión, realizada a principios de 2011, concluyó que las normas de protección de datos del acuerdo se habían respetado y que el JRT había obtenido información convincente sobre el valor añadido del TFTP en la lucha contra el terrorismo. [111] Sin embargo, y de forma un tanto contradictoria con lo anterior, aconsejaba mejorar la verificación de las solicitudes realizadas por los EEUU y solicitaba más evidencias sobre el valor añadido de la información derivada del acuerdo TFTP. También recomendaba una mayor transparencia sobre el funcionamiento del programa, especialmente en relación a la cantidad de datos proporcionada a EEUU y el número de mensajes financieros consultados por el UST, y mejorar la difusión de los derechos de que disponen los ciudadanos.

---

109 "EU Review of the United States' "Terrorist Finance Tracking Programme" confirms privacy safeguards (IP/09/264), 17.02.2009.

110 Disponible en http://www.statewatch.org//news/2010/aug/eu-usa-swift-2nd-bruguiere-report.pdf, último acceso el 9.06.2013).

111 Commission report on the joint review of the implementation of the Agreement between the European Union and the United States of America 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, 16.03.2011, disponible en http://ec.europa.eu/dgs/home-affairs/news/intro/docs/commission-report-on-the-joint-review-of-the-tftp.pdf, último acceso el 9.06.2013).

El segundo informe fue publicado a finales de 2012. Concluía que las recomendaciones efectuadas en la primera revisión se habían implementado en gran medida, y confirmaba el valor añadido del acuerdo y notaba mejoras de los mecanismos de verificación y de supervisión.[112] La tercera revisión conjunta tuvo lugar en marzo de 2014. El informe no se había publicado en el momento de escribir el presente artículo.

Por otra parte, según el artículo 6(6) del acuerdo TFTP, la Comisión y el UST deben preparar un informe conjunto sobre su valor añadido tres años tras la entrada en vigor del acuerdo TFTP (1 de agosto de 2013). La Comisión presentó dicho informe el 27 de noviembre de 2014.[113] Según el informe, los datos provistos por el acuerdo TFTP, incluidos los datos conservados durante varios años, han tenido un valor muy importante en los esfuerzos antiterroristas en EEUU, la UE y terceros países. Sin embargo, tal como requiere el acuerdo, el informe se centra en el valor añadido de los datos, sin entrar a valorar el cumplimiento del acuerdo.

4.4. La evaluación de la implementación del acuerdo TFTP

A pesar de que la mayoría de los informes de supervisión no son públicos, las versiones disponibles se muestran contradictorias en sus conclusiones generales. Los informes del JRT, liderado en su componente europea por la Comisión, y los del juez Bruguière, nombrado también por la Comisión como "personalidad eminente europea" previa consulta del UST, son, en general, positivas. En cambio, las versiones públicas de los informes de la ACC, compuesta por las autoridades independientes de protección de datos de la UE, muestran una conclusión mucho más negativa.

Estas tensiones entre equipos de supervisión se han hecho palpables en las acusaciones públicas de la Comisión Europea a dos miembros de la ACC de conflicto de intereses, con el argumento de que si éstos supervisan la implementación del acuerdo por parte de Europol en el marco de la ACC, no deberían participar en el JRT.[114] Sin embargo, es posible encontrar puntos en común. Mientras los últimos informes de la ACC valoran, como los del JRT y el juez Bruguière, las mejoras observadas respecto a las primeras inspecciones, algunas de las críticas de la ACC

---

112 Commission staff working document. "Report on the second joint review of the implementation of the Agreement between the European Union and the United States of America 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, 14.12.2012" (SWD(2012) 454 final), disponible en http://ec.europa.eu/dgs/home-affairs/pdf/20121214_joint_review_report_tftp_en.pdf, último acceso el 9.06.2013.

113 Joint Report from the Commission and the U.S. Treasury Department regarding the value of TFTP Provided Data pursuant to Article 6 (6) of the Agreement between the European Union and the United States of America 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 (COM(2013)843 final).

114 Nicolaj Nielsen, "Terrorist data oversight tainted by potential conflict of interest", *EU observer*, 20.12.2012, disponible en http://euobserver.com/justice/118593, último acceso el 9.06.2013).

pueden intuirse también en los informes del JRT[115] y del juez Brouguière.

Finalmente, respecto al papel de Europol, los informes coinciden también en que la agencia nunca ha rechazado una solicitud del UST sobre la base de que no cumple con los requisitos del artículo 4(2) del acuerdo. No obstante, Europol ha proporcionado recomendaciones y en ocasiones ha requerido al UST más información en sus solicitudes. Como hemos visto en el apartado 4.2, para evitar conflictos de intereses en la verificación de las solicitudes del UST, la Comisión y el Parlamento Europeo habían recomendado que dicha verificación fuera realizada por una autoridad judicial, no por Europol. De todas formas, el papel que el acuerdo TFTP otorga a Europol es limitado, puesto que no puede tener acceso a los datos enviados y por tanto le es muy difícil evaluar con precisión la magnitud real y la exactitud de las solicitudes.[116]

5. El futuro de Europol y del TFTP

5.1. La propuesta de Reglamento de Europol. Un nuevo marco para las transferencias internacionales

El Tratado de Lisboa requiere una nueva base legal para Europol. El artículo 88 del TFUE exige que ésta sea adoptada por el Parlamento Europeo y por el Consejo y que ambos colegisladores adopten procedimientos de control de las actividades de Europol, tanto por parte del Parlamento Europeo como de los parlamentos nacionales.

Sobre esta base, el 27 de marzo de 2013 la Comisión presentó la propuesta de Reglamento de Europol[117]. La propuesta fue adoptada, con enmiendas, por el Parlamento Europeo en primera lectura el 25 de febrero de 2014. En el momento de escribir este artículo se encontraba en manos del Consejo de Ministros. Cuando finalice el proceso de codecisión, el reglamento finalmente adoptado puede tener un aspecto muy diferente al de la propuesta inicial de la Comisión.

La propuesta refuerza la obligación de que los Estados miembros suministren datos a Europol, prevé incentivos financieros para las investigaciones conjuntas y obliga Europol a informar anualmente sobre la cantidad y la calidad de la información suministrada por los Estados miembros. El Parlamento Europeo y los parlamentos nacionales serán consultados sobre el programa de trabajo plurianual estratégico de Europol y recibirán los informes anuales de actividad, las cuentas finales anuales, las evaluaciones de las amenazas, los análisis estratégicos y los informes de situación generales.

---

115 El informe del JRT de 2012, por ejemplo, menciona que Europol recibe de media una solicitud cada mes que cubre un periodo de cuatro semanas, es decir, todo el mes.

116 Entrevista en Bruselas, 14.06.2013.

117 Propuesta de Reglamento relativo a la Agencia de la UE para la cooperación y la formación policiales (Europol) y por el que se deroga la Decisión 2009/371/JAI (por la que se crea Europol) y 2005/681/JAI (por la que se crea la CEPOL) (COM(2013) 173 final).

Entre otras novedades, el reglamento propuesto rediseña la estructura de tratamiento de datos de Europol, sustituye la supervisión de la ACC por la del Supervisor Europeo de Protección de Datos y propone una fusión con la Escuela Europea de Policía (CEPOL), cambios que han suscitado críticas desde varios frentes.[118]

En cuanto al nuevo marco para las transferencias internacionales, el capítulo VI de la propuesta establece que, en principio, las transferencias de datos personales a terceros países y organizaciones sólo pueden tener lugar si existe una decisión de la Comisión que acredite que el destinatario garantiza un nivel adecuado de protección de datos, o si se aseguran garantías adecuadas mediante un acuerdo internacional concluido sobre la base del artículo 218 del TFUE, que requiere la aprobación del Parlamento Europeo. También será posible la transferencia en base a los acuerdos de cooperación operativa concluidos antes de la entrada en vigor del nuevo reglamento.

Cuando los datos han sido proporcionados por un Estado miembro, Europol debe obtener el consentimiento del Estado en cuestión, excepto si ya ha proporcionado una autorización previa, o si la autorización puede considerarse implícita (Art.29(4)5ª)). El SEPD ha criticado en su dictamen esta última excepción, puesto que el consentimiento del Estado miembro puede contribuir a asegurar la calidad y la exactitud de los datos.[119] El SEPD recomendó, además, añadir que los datos sólo deben transmitirse si el destinatario se compromete a que la información se use únicamente para el propósito para el que fueron transferidos. Esta condición existe actualmente en la Decisión de Europol y no se ha incluido en la nueva propuesta.

La posibilidad de transferencias fuera del marco de los acuerdo internacionales en situaciones excepcionales se flexibiliza, puesto que se amplían los supuestos en los que está permitida (por ejemplo, si es necesaria para un interés público importante, aunque no está exigida legalmente) y se elimina la obligación de que el director evalúe previamente el nivel de protección de datos del organismo receptor.

Además, se añade la posibilidad de que el consejo de administración, de acuerdo con

---

118 Ver el dictamen del SEPD de 31 de mayo de 2013 (EDPS Opinion on the Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA, disponible en http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-05-31_Europol_EN.pdf); el dictamen de la ACC de 10 de junio de 2013 (Opinion 13/31 of the Joint Supervisory Board with respect to the proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law enforcement Cooperation and Training (Europol)); y la declaración de la Conferencia de Autoridades Europeas de Protección de Datos Lisboa de 16-17 mayo 2013 "Resolution on ensuring an adequate level of data protection at Europol", disponible en http://www.bfdi.bund.de/EN/PublicRelations/Publications/ResolutionOnEnsuringAnAdequateLevelOfDataProtectionAtEuropol.pdf?__blob=publicationFile, último acceso el 9.06.2013). Ver también el debate de la Comisión LIBE del Parlamento Europeo en la reunión del 7.05.2013, *op.cit.*, con las intervenciones de los directores de Europol y de CEPOL, el consejo de administración de Europol y la ACC, donde prácticamente todos los presentes criticaron la propuesta de fusión de ambas agencias.

119 Ver el dictamen del SEPD de 31 de mayo de 2013, *op. cit.*

el SEPD, autorice una serie de transferencias fuera del marco de los acuerdos en determinados casos excepcionales para un periodo máximo de un año, previa evaluación de las garantías que ofrece el destinatario. No obstante, se mantiene el control a posteriori mediante la obligación de informar al consejo de administración y (ahora) al SEPD.

Por otra parte, el artículo 4(1)(k) menciona, como tarea de Europol, la facilitación de información y la ayuda a las estructuras y misiones de gestión de crisis de la UE. Como critica la ACC, a pesar de que esta función podría implicar el intercambio de datos personales, no está sometida a las condiciones del capítulo VI. Otro aspecto que tampoco queda regulado en la propuesta es la tarea de Europol bajo el acuerdo TFTP.[120]

5.2. La continuidad del acuerdo TFTP en peligro

A menos que una de las partes decida suspender el acuerdo por incumplimiento o denunciarlo, éste estará en vigor hasta el 1 de agosto de 2015. La Comisión y el Consejo se comprometieron a plantearse si renovarían o no el acuerdo si para esa fecha todavía no se había establecido un TFTS europeo.[121] Este parece que será el caso, puesto que la Comisión concluyó en su comunicación del 27 de noviembre de 2013 que la necesidad de un sistema similar al TFTP pero circunscrito al ámbito europeo no estaba claramente demostrada[122].

En el debate de LIBE del 7 de mayo de 2013,[123] algunos diputados europeos denunciaron una clara violación de las disposiciones de protección de datos del acuerdo sobre la base de los informes de la ACC. También criticaron el hecho de que todavía no se hubiera presentado una propuesta legislativa para establecer un TFTS que permita filtrar los datos en la UE antes de enviarlos al UST.

El escándalo sobre las actividades de vigilancia masiva por parte de EEUU y de varios Estados miembros de la UE ha tenido un gran impacto en la posición del Parlamento Europeo. Según las revelaciones de Snowden, la Agencia Nacional de Seguridad Nacional (NSA) puede haber accedido directamente a los datos SWIFT sin cumplir con el acuerdo TFTP[124] y, por tanto, sin consultar a Europol.

---

120 Ver el dictamen de la ACC, *op.cit*,pág. 7-8.

121 Decisión del Consejo 2010/412/UE, 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, 27.07.2010,pág. 3).

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

123 *Op. cit.*

124 Ver por ejemplo, Der Spiegel, "Follow the Money: NSA Spies on International Payments", 15 de septiembre de 2013, disponible en http://www.spiegel.de/international/world/spiegel-exclusive-nsa-

A raíz de estas revelaciones, la Comisión inició el procedimiento de consulta establecido en el artículo 19 del acuerdo TFTP y solicitó explicaciones al UST. El UST respondió en sus cartas de 18 de septiembre y 8 de noviembre de 2013, y en las reuniones de alto nivel de 7 de octubre y 18 de noviembre de 2013, que la aplicación del acuerdo TFTP no revelaba ninguna violación de sus cláusulas[125].

Por su parte, el Parlamento Europeo solicitó en sus resoluciones de octubre de 2013 y de marzo de 2014, una investigación sobre estas acusaciones y la suspensión del acuerdo TFTP.[126] El futuro del acuerdo después más allá de 2015 es por tanto incierto.

6. Conclusiones

La acción exterior de Europol no ha dejado de crecer desde su creación - con la excepción de la internalización producto de las últimas ampliaciones de la UE-, una evolución inevitable visto el incremento de sus competencias y la transnacionalización de los crímenes de los que se ocupa.

A pesar de los numerosos beneficios que aportan las relaciones con terceros países y organizaciones, éstas presentan varios riesgos, especialmente en relación a las transferencias internacionales de datos personales. Sin embargo, es difícil evaluar qué problemas existen realmente, debido a la clasificación de la mayoría de informes de inspección y a las limitaciones inherentes a las inspecciones.

Mención especial merece la aplicación del TFTP, en la cual, sin embargo, Europol no tiene un amplio margen de actuación. El importante escrutinio público y parlamentario del cual ha sido objeto el acuerdo y la mayor disponibilidad de información sobre su inspección, permiten indicar varios problemas en su implementación, a pesar de la existencia de opiniones discrepantes por parte de los diferentes equipos de revisión y evaluación.

La nueva propuesta de Reglamento de Europol, de acuerdo con el TFUE, requiere el consentimiento del Parlamento Europeo para la conclusión de nuevos acuerdos internacionales de intercambio de datos. Si bien esta novedad puede retrasar la conclusión de acuerdos, ya de por sí lenta, constituirá un nuevo elemento de control. Además, en el caso de las transferencias basadas en el nivel adecuado de protección de datos, la evaluación del nivel en cuestión será realizada por la Comisión, mediante una decisión de adecuación, y no por la misma Europol. Sin embargo, se flexibiliza el

---

spies-on-international-bank-transactions-a-922276.html, último acceso el 7.04.2014.

125 Joint Report from the Commission and the U.S. Treasury Department regarding the value of TFTP Provided Data, op.cit., p. 16.

126 Ver la Resolución del Parlamento Europeo, de 23 de octubre de 2013, sobre la suspensión del Acuerdo TFTP a raíz de la vigilancia de la NSA (2013/2831(RSP)) y la Resolución del Parlamento Europeo, de 12 de marzo de 2014, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de justicia y asuntos de interior (2013/2188(INI)).

uso de las excepciones y se omiten cuestiones como las transferencias en el marco de la gestión de crisis y el papel de Europol en el marco del acuerdo TFTP.

Respecto al acuerdo TFTP, si en su momento se puso en duda la necesidad y proporcionalidad de tal medida, después de tres años de funcionamiento se cuestiona también su correcta aplicación. Las evaluaciones de la ACC ponen en duda que la naturaleza misma del programa estadounidense permita realmente respetar las condiciones del acuerdo. A ello se añaden las acusaciones a EEUU de acceso por parte de la NSA a los datos de SWIFT incumpliendo el acuerdo TFTP, que han llevado al Parlamento Europeo a solicitar explícitamente la suspensión del acuerdo.

Tanto la reforma de Europol como el futuro del acuerdo TFTP se decidirán en un momento clave para la protección de la privacidad y los datos personales en la UE. El debate sobre la propuesta de Reglamento de Europol tiene lugar en paralelo con el debate sobre la reforma del marco legal de protección de datos de la UE. Al mismo tiempo, el Consejo de Europa está trabajando sobre la modernización del Convenio 108 y el futuro de la Recomendación 87(15), cuyos principios se aplican actualmente a Europol, y en los cuales se basa el nuevo régimen de protección de datos propuesto por la Comisión para la agencia. Además, si las negociaciones sobre el acuerdo marco entre la UE y los EEUU para el intercambio de datos con fines policiales siguen adelante, éstas podrían coincidir con el momento en que la UE deberá decidir si da continuidad al acuerdo TFTP.

Como el SEPD ha recomendado varias veces, lo más lógico sería primero reformar el marco europeo de protección de datos y, posteriormente, adoptar los instrumentos específicos y los acuerdos necesarios, asegurando que son coherentes con el marco general. En este caso, el orden de los factores sí puede alterar el producto. Sin embargo, la elección de los tiempos responde a muchos factores, incluyendo los intereses y prioridades políticas. En esta situación, conseguir un marco más o menos coherente, operativo y que ofrezca un buen nivel de protección es tarea complicada, pero no imposible. Ello dependerá principalmente de la voluntad política de nuestros gobiernos y parlamentarios, tanto en Bruselas como en las capitales europeas.