COMISIÓN EUROPEA

Bruselas, 20.7.2010

COM(2010)385 final

COMUNICACIÓN DE LA COMISIÓN AL CONSEJO Y AL PARLAMENTO EUROPEO

Panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia

COMUNICACIÓN DE LA COMISIÓN AL CONSEJO Y AL PARLAMENTO EUROPEO

Panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia

1. INTRODUCCIÓN

La Unión Europea ha recorrido un largo camino desde que los dirigentes de cinco países europeos acordaran en 1985 en Schengen suprimir los controles en sus fronteras comunes. Este acuerdo dio origen en 1990 al Convenio de Schengen, que contenía el germen de muchas de las actuales políticas de gestión de la información. La supresión de los controles en las fronteras interiores ha favorecido el desarrollo de una amplia gama de medidas en las fronteras exteriores, referentes, principalmente, a la expedición de visados, la coordinación de las políticas de asilo e inmigración y el fortalecimiento de la cooperación policial, judicial y aduanera en la lucha contra la delincuencia transfronteriza. Ni el espacio de Schengen ni el mercado interior de la UE podrían funcionar hoy día sin el intercambio transfronterizo de datos.

Los ataques terroristas de 2001 en los Estados Unidos, así como los atentados de Madrid y Londres de 2004 y 2005, impulsaron una dinámica diferente en el desarrollo de las políticas europeas de gestión de la información. En 2006, el Consejo y el Parlamento Europeo adoptaron la Directiva sobre conservación de datos, para permitir a las autoridades nacionales combatir las formas graves de delincuencia conservando los datos sobre el tráfico de telecomunicaciones y de localización[1]. El Consejo optó posteriormente por la Iniciativa sueca para simplificar el intercambio transfronterizo de información en investigaciones penales y operaciones de inteligencia. En 2008 aprobó la Decisión Prüm para agilizar el intercambio de perfiles de ADN, impresiones dactilares y datos de los registros de matriculación de vehículos en la lucha contra el terrorismo y otras formas de delincuencia. La cooperación transfronteriza entre unidades de información financiera, organismos de recuperación de activos y plataformas contra la delincuencia informática y el uso por los Estados miembros de Europol y Eurojust, son otras herramientas para combatir las formas graves de delincuencia en el espacio de Schengen.

Inmediatamente después de los ataques terroristas del 11 de septiembre, el Gobierno de los EE.UU. puso en marcha su Programa de seguimiento de la financiación del terrorismo con el objetivo de desbaratar acciones similares mediante el control de transacciones financieras sospechosas. El Parlamento Europeo ha dado su consentimiento para la celebración del

[1] Actualmente no existe en la UE una definición armonizada de «forma grave de delincuencia». Por ejemplo, la Decisión del Consejo que habilita a Europol para consultar el Sistema de Información de Visados (VIS) (Decisión 2008/633/JAI del Consejo, DO L 218 de 13.8.2008, p.129) define «delitos graves» haciendo referencia a lista de delitos establecidos en la orden de detención europea (Decisión 2002/584/JAI, DO L 190 de 18.7.2002, p.1). La Directiva sobre conservación de datos (Directiva 2002/58/CE, DO L 105 de 13.4.2006, p. 54) deja a los Estados miembros definir los «delitos graves». La Decisión Europol (Decisión 2009/371/JAI del Consejo, DO L 121 de 15.5.2009, p. 37) incluye otra lista de delitos definidos como «formas graves de delincuencia» que es muy parecida, pero no idéntica, a la lista de la orden de detención europea.

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 (Acuerdo TFTP UE-EE.UU.)[2]. El intercambio de registros de nombres de pasajeros (*Passenger Name Records* - PNR) con terceros países ha ayudado también a la UE combatir el terrorismo y otras formas graves de delincuencia[3]. Después de celebrar acuerdos PNR con los EE.UU., Australia y Canadá, la Comisión, ha vuelto recientemente al punto de partida para reconsiderar su enfoque en la creación de un sistema PNR en la Unión Europea y compartir esos datos con terceros países.

Las medidas que acabamos de señalar han posibilitado la libre circulación en el espacio de Schengen, han contribuido a la prevención de ataques terroristas y otras formas graves de delincuencia y a combatirlos y han consolidado el desarrollo de una política común de visados y asilo.

Esta comunicación presenta, por primera vez, un panorama completo de las medidas en vigor, en aplicación o en preparación en la UE para regular la recogida, el almacenamiento o el intercambio transfronterizo de información personal con fines represivos o de gestión de la migración. Los ciudadanos tienen derecho a saber qué datos personales suyos se tratan e intercambian, quiénes lo hacen y con qué finalidad. Este documento ofrece una respuesta transparente a todas estas cuestiones. Aclara el objetivo principal de estos instrumentos, su estructura, los tipos de datos personales que cubre, la lista de autoridades que tienen acceso a tales datos y las disposiciones que regulan la protección y la conservación de datos. Además, incluye un número limitado de ejemplos que ilustran cómo funcionan estos instrumentos en la práctica (véase el anexo I). Por último, recoge los principios esenciales en los que debe basarse el diseño y la evaluación de los instrumentos de gestión de la información en el espacio de libertad, seguridad y justicia.

Al ofrecer un panorama general de las medidas que a nivel de la UE regulan la gestión de la información personal y proponer un conjunto de principios para el desarrollo y la evaluación de tales medidas, esta comunicación contribuye un diálogo político informado con todos los interesados. Al mismo tiempo constituye una primera respuesta a las peticiones de los Estados miembros de que se desarrolle un enfoque más «coherente» del intercambio de información personal a efectos represivos, del que se ocupó recientemente la Estrategia de gestión de la información de la UE[4] y para reflexionar sobre la posible necesidad de desarrollar un Modelo europeo para el intercambio de información basado en una evaluación de las actuales medidas de intercambio de la información[5].

---

2 Resolución del Parlamento Europeo, P7_TA-PROV(2010)0279, 8.7.2010

3 En contraposición a los delitos graves, los «delitos de terrorismo» se definen claramente en la Decisión marco del Consejo sobre la lucha contra el terrorismo (Decisión marco 2002/475/JAI del Consejo, DO L 164 de 22.6.2002, p. 3; modificada por la Decisión marco 2008/919/JAI del Consejo, OJ L 330 de 9.12.2008, p. 21).

4 Conclusiones del Consejo sobre una estrategia de gestión de la información en el área de la seguridad interior de la UE, Consejo de Justicia e Interior, 30.11.2009 (Estrategia de gestión de la información de la UE); Libertad, seguridad e intimidad: los asuntos de interior europeos en un mundo abierto, Informe del Grupo consultivo informal de alto nivel sobre el futuro de la política europea de asuntos de interior («el Grupo Futuro»), junio de 2008.

5 Programa de Estocolmo – Una Europa abierta y segura que sirva y proteja al ciudadano, Documento del Consejo 5731/10, 3.3.2010, sección 4.2.2.

La limitación de la finalidad es una consideración clave de la mayoría de los instrumentos que cubre la presente comunicación. Un sistema de información único y general de la UE con múltiples finalidades supondría el grado más elevado de intercambio de información. La creación de un sistema de este tipo, sin embargo, constituiría una restricción grave e ilegítima del derecho de los individuos a su intimidad y a la protección de datos y plantearía enormes desafíos en términos de desarrollo y funcionamiento. En la práctica, las políticas en el espacio de libertad, seguridad y justicia se han ido desarrollando a un ritmo constante, dando origen a varios sistemas e instrumentos de información de diferentes tamaños, alcances y finalidades. La estructura compartimentada de la gestión de la información que ha ido apareciendo en las últimas décadas es más propicia para salvaguardar el derecho de los ciudadanos a la intimidad que cualquier alternativa centralizada.

Esta comunicación no cubre las medidas que incluyen el intercambio de datos no personales con fines estratégicos, tales como los análisis generales de riesgos o evaluaciones de amenazas; tampoco analiza en detalle las disposiciones de protección de datos de los instrumentos sometidos a debate, ya que la Comisión está realizando actualmente, sobre la base del artículo 16 del Tratado de Funcionamiento de la Unión Europea, un ejercicio separado sobre un nuevo marco global para la protección de datos personales en la UE. El Consejo está examinando actualmente el proyecto de directrices de negociación de un acuerdo UE-EE.UU. sobre la protección de datos personales cuando se transfieren y tratan con el fin de prevenir, investigar, detectar o perseguir delitos, incluido el terrorismo, en el marco de la cooperación policial y judicial en materia penal. Como se espera que estas negociaciones establezcan la forma en que ambas partes pueden garantizar un elevado nivel de protección de los derechos y libertades fundamentales al transferir o tratar datos personales antes que el contenido real de tales transferencias o tratamientos de datos, la presente comunicación no cubre esta iniciativa[6].

2. INSTRUMENTOS DE LA UE QUE REGULAN LA RECOGIDA, EL ALMACENAMIENTO O EL INTERCAMBIO TRANSFRONTERIZO DE DATOS PERSONALES PARA FINES REPRESIVOS O DE GESTIÓN DE LA MIGRACIÓN

Esta sección ofrece un panorama general de los instrumentos de la Unión Europea que regulan la recogida, el almacenamiento o el intercambio transfronterizo de datos personales con fines represivos o de gestión de la migración. La sección 2.1 se centra en las medidas en vigor, en ejecución o en consideración; la sección 2.2 se refiere a las iniciativas establecidas en el Plan de Acción del Programa de Estocolmo[7]. Informa sobre los siguientes aspectos de cada instrumento:

– Antecedentes (indica si la medida la propusieron los Estados miembros o la Comisión);[8]

---

6 COM(2010)252 de 26.5.2010.

7 COM(2010)171, 20.4.2010 (Plan de Acción del Programa de Estocolmo).

8 En el antiguo tercer pilar de la Unión Europea relativo a la cooperación policial y judicial en materia penal, los Estados miembros y la Comisión compartían el derecho de iniciativa. El Tratado de Amsterdam integró los ámbitos del control de las fronteras exteriores, los visados, el asilo y la inmigración en el (primer) pilar comunitario, en el que la Comisión disfrutaba del derecho exclusivo de iniciativa. El Tratado de Lisboa ha elimienado la estructura de pilares de la Unión, reafirmando el derecho de iniciativa de la Comisión. En los ámbitos de la cooperación policial y judicial en materia penal (incluida la cooperación administrativa), sin embargo, todavía se puede proponer legislación a iniciativa de una cuarta parte de los Estados miembros.

– Finalidad o finalidades para las que se recogen, almacenan o intercambian los datos;

– Estructura (sistema de información centralizado o intercambio descentralizado de datos);

– Cobertura de datos personales;

– Autoridades con acceso a los datos;

– Disposiciones de protección de datos;

– Normas de conservación de datos;

– Estado de ejecución;

– Mecanismo de revisión.

2.1. Instrumentos en aplicación, en ejecución o en consideración

Instrumentos de la UE para mejorar el funcionamiento del espacio de Schengen y de la unión aduanera

El **Sistema de Información de Schengen** (SIS) surgió del deseo de los Estados miembros de crear un espacio sin controles en las fronteras interiores facilitando la circulación de personas a través de sus fronteras exteriores[9]. En funcionamiento desde 1995, su objetivo es mantener la seguridad pública, incluida la seguridad nacional, dentro del espacio de Schengen y facilitar la circulación de personas utilizando la información comunicada a través de este sistema. El SIS es un sistema de información centralizado que comprende una parte nacional en cada Estado participante y una unidad de apoyo técnico en Francia. Los Estados miembros pueden introducir descripciones de las personas buscadas para su detención a efectos de entrega o extradición; nacionales de terceros países a los que se deniega la entrada; personas desaparecidas; testigos o personas objeto de una citación judicial; personas y vehículos sujetos a vigilancia especial debido a la amenaza que pueden suponer para la seguridad pública o nacional; vehículos, documentos y armas de fuego perdidos o robados; y billetes de banco sospechosos. Los datos introducidos en el SIS incluyen nombres y apodos, características físicas, lugar y fecha de nacimiento, nacionalidad y si el individuo va armado y es violento. La policía, los controles fronterizos, las aduanas y las autoridades judiciales de procesos penales pueden acceder a dichos datos de acuerdo con sus respectivas competencias legales. Las autoridades de inmigración y las oficinas consulares tienen acceso a los datos relativos a nacionales de terceros países incluidos en la lista de prohibición de entrada y a las descripciones de documentos perdidos y robados. Europol puede acceder a algunas categorías de datos del SIS, incluidas las descripciones de personas buscadas para su detención a efectos de entrega o extradición y las de personas sujetas a vigilancia especial debido a la amenaza que pueden suponer para la seguridad pública o nacional. Eurojust puede acceder a las descripciones de personas buscadas para su detención a efectos de entrega o extradición y las de testigos o personas objeto de citaciones judiciales. Los datos personales sólo pueden utilizarse para los fines específicos para los que se solicitaron. Los datos personales

[9] Convenio de aplicación del Acuerdo de Schengen, de 14 de junio de 1985, entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa relativo a la supresión gradual de los controles en las fronteras comunes, DO L 239 de 22.9.2000, p. 19.

introducidos en el SIS a efectos de la búsqueda de personas sólo podrán conservarse el tiempo necesario para cumplir los fines para los que se suministraron y no más de tres años tras la fecha de su introducción. Los datos sobre personas sujetas a vigilancia especial debido a la amenaza que pueden suponer para la seguridad pública o nacional deberán borrarse al cabo de un año. Los Estados miembros deberán adoptar normativas nacionales que fijen un nivel de protección de datos como mínimo equivalente al resultante del Convenio del Consejo de Europa de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y la Recomendación del Comité de Ministros del Consejo de Europa de 1987 por la que se regula el uso de datos personales en el ámbito policial[10]. Aunque el Convenio de Schengen no incluye un mecanismo de revisión, los signatarios pueden proponer modificaciones al mismo y una vez introducidas el texto modificado debe ser aprobado por unanimidad y ratificado por los parlamentos nacionales. El SIS es plenamente aplicable en 22 Estados miembros, así como en Suiza, Noruega e Islandia. El Reino Unido e Irlanda participan en los aspectos de la cooperación policial del Convenio de Schengen y del SIS, con excepción de las descripciones relacionadas con los nacionales de terceros países incluidos en la lista de prohibición de entrada. Chipre ha suscrito el Convenio de Schengen, pero todavía no lo aplica. Está previsto que Liechtenstein empiece a aplicarlo en 2010; se espera que Bulgaria y Rumanía lo hagan en 2011. Las búsquedas en el SIS generan respuestas positivas si los detalles de la persona o el objeto buscado coinciden con los de una descripción existente. Tras obtener una respuesta positiva, las autoridades encargadas de aplicar la ley pueden, a través de su red de servicios SIRENE, solicitar información suplementaria sobre las personas objeto de la descripción[11].

A medida que nuevos Estados miembros se han ido sumando al espacio Schengen, el volumen de la base de datos SIS ha aumentado en consecuencia: entre enero de 2008 y 2010, el número total de descripciones SIS pasó de 22,9 a 31,6 millones[12]. Anticipándose a este incremento de los volúmenes de datos y cambios en las necesidades de los usuarios, los Estados miembros decidieron en 2001 desarrollar un **Sistema de Información de Schengen de segunda generación** (SIS II), encargando de ello a la Comisión[13]. Actualmente en fase de desarrollo, la finalidad del SIS II es garantizar un elevado nivel de seguridad en el espacio de libertad, seguridad y justicia mejorando las funciones del sistema de primera generación y facilitar la circulación de personas utilizando la información comunicada a través de este sistema. Además de las categorías de datos originales que cubría el sistema de primera generación, SIS II podrá tratar impresiones dactilares, fotografías, copias de la orden de detención europea, disposiciones para proteger los intereses de personas cuya identidad ha sido usurpada y enlaces entre las diferentes descripciones. Por ejemplo, el SIS II permitirá vincular descripciones relativas a las personas buscadas por sustracción, el individuo sustraído y el vehículo utilizado para el delito. Los derechos de acceso y las normas para la conservación de datos son idénticos a los del sistema de la primera generación. Los datos personales sólo pueden utilizarse para los fines específicos para los que se solicitaron. Los datos personales de SIS II deberán tratarse de conformidad con las disposiciones específicas

---

10 Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE nº 108), Consejo de Europa, 28.1.1981 (Convenio del Consejo de Europa 108); Recomendación nº R (87) 15 del Comité de Ministros por la que se regula el uso de datos personales en el ámbito policial, Consejo de Europa, 17.9.1987 (Recomendación policial).

11 SIRENE corresponde a *Supplementary Information Request at National Entry* (Solicitud de información adicional al puesto fronterizo de entrada).

12 Documento 5441/08 del Consejo de 30.1.2008; Documento 6162/10 del Consejo de 5.2.2010.

13 Reglamento (CE) nº 1986/2006, DO L 381 de 28.12.2006, p. 1; Reglamento (CE) nº 1987/2006, DO L 381 de 28.12.2006, p. 4; Decisión 2007/533/JAI, DO L 205 de 7.8.2007, p. 63.

los actos jurídicos de base que rigen este sistema (Reglamento (CE) nº 1987/2006 y Decisión 2007/533/JAI del Consejo), que aclaran los principios de la Directiva 95/46/CE y de conformidad con el Reglamento (CE) nº 45/2001, el Convenio 108 del Consejo de Europa y la Recomendación policial[14]. El SIS II utilizará s-TESTA, la red de comunicación de datos segura de la Comisión[15]. Una vez sea operativo, el sistema se aplicará en todos los Estados miembros, Suiza, Liechtenstein, Noruega e Islandia[16]. La Comisión deberá remitir al Parlamento Europeo y al Consejo un informe de situación bianual sobre el desarrollo de SIS II y la potencial migración al mismo del sistema de primera generación[17].

El desarrollo de **EURODAC** se remonta a la supresión de las fronteras interiores, lo que hizo necesario establecer unas normas claras sobre el tratamientos de las solicitudes de asilo. EURODAC es un sistema informatizado de identificación de impresiones dactilares centralizado que contiene las impresiones dactilares de determinados nacionales de terceros países. Entró en funcionamiento en enero de 2003 y su finalidad es ayudar a establecer qué Estado miembro debe ser responsable, de acuerdo con el Reglamento de Dublín, de examinar una solicitud de asilo particular[18]. A los individuos que tengan al menos 14 años de edad que soliciten asilo en un Estado miembro se les tomarán automáticamente las impresiones dactilares, como se hace con los nacionales de terceros países interceptados con ocasión del cruce irregular de una frontera exterior. Comparando las impresiones dactilares de estos individuos con los registros EURODAC, las autoridades nacionales buscarán establecer dónde podría haber presentado esa persona una solicitud de asilo o por dónde podría haber entrado en la Unión Europea por primera vez. Las autoridades también pueden comparar con los registros EURODAC las impresiones dactilares de los nacionales de terceros países presentes ilegalmente en su territorio. Los Estados miembros deberán especificar la lista de autoridades con acceso a esta base de datos, que normalmente incluye a las autoridades de asilo y migración, guardias de fronteras y policía. Los Estados miembros cargarán los datos relevantes en la base de datos central a través de sus puntos nacionales de acceso. Los datos personales de EURODAC sólo pueden utilizarse para facilitar la aplicación del Reglamento de Dublín; cualquier otro uso será objeto de sanciones. Las impresiones dactilares de los solicitantes de asilo se conservarán durante diez años; las de los migrantes en situación irregular, durante dos años. Los registros de los solicitantes de asilo se eliminarán una vez hayan adquirido la nacionalidad de un Estado miembro; las de los migrantes en situación irregular se eliminarán una vez hayan obtenido un permiso de residencia o la ciudadanía, o

---

14 Reglamento (CE) nº 1987/2006, DO L 381 de 28.12.2006, p. 4; Decisión 2007/533/JAI, DO L 205 de 7.8.2007, p. 63. Directiva 95/46/CE, DO L 281 de 23.11.1995, p. 31; Reglamento (CE) nº 45/2001, DO L 8 de 12.1.2001, p. 1. Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE nº 108), Consejo de Europa, 28.1.1981 (Convenio del Consejo de Europa 108); Recomendación nº R (87) 15 del Comité de Ministros por la que se regula el uso de datos personales en el ámbito policial, Consejo de Europa, 17.9.1987 (Recomendación policial).

15 S-TESTA, que corresponde a *Secure Trans-European Services for Telematics between Administrations* (Servicios transeuropeos seguros de telemática entre las administraciones), es una red de comunicación de datos financiada por la Comisión que permite el intercambio de datos seguro y codificado entre adminsitraciones nacionales e instituciones, agencias y organismos de la UE.

16 El Reino Unido e Irlanda participarán en SIS II con excepción de las descripciones relativas a nacionales de terceros países incluidos en la lista de prohibición de entrada.

17 Reglamento (CE) nº 1104/2008 del Consejo, DO L 299 de 8.11.2008, p. 1; Decisión 2008/839/JAI del Consejo, DO L 299 de 08/11/2008, p. 43.

18 Reglamento (CE) nº 343/2003 del Consejo, DO L 50 de 25.2.2003, p. 1 (Reglamento de Dublín), Reglamento (CE) nº 2725/2000 del Consejo, DO L 316 de 15.12.2000, p. 1 (Reglamento EURODAC). Estos instrumentos se basan en el Convenio de Dublín de 1990 (DO C 254 de 19.8.1997, p.1) cuya finalidad es tratar de determinar qué Estado miembro debería examinar las solicitudes de asilo. El sistema para evaluar las solicitudes de asilo se conoce como «sistema de Dublín».

hayan salido del territorio de los Estados miembros. La Directiva 95/46/CE se aplica al tratamiento de datos personales con arreglo a este instrumento[19]. EURODAC funciona sobre la base de la red s-TESTA de la Comisión y es aplicable en todos los Estados miembros, así como en Noruega, Islandia y Suiza. El acuerdo que permitirá la conexión de Liechtenstein está pendiente de su celebración. La Comisión deberá presentar al Parlamento Europeo y al Consejo informes anuales sobre el funcionamiento de la unidad central de EURODAC.

A raíz de los ataques del 11 de septiembre de 2001, los Estados miembros acordaron impulsar la adopción de una política común de visados creando una forma de intercambio de información sobre visados de corta duración[20]. La supresión de las fronteras interiores ha hecho también que sea más sencillo utilizar abusivamente los regímenes de visados de los Estados miembros. El **sistema de información de visados** (*Visa Information System* - VIS) trata de resolver ambas cuestiones: su objetivo es ayudar a aplicar una política de visados común facilitando el examen de las solicitudes de visado y los controles de las fronteras exteriores contribuyendo al mismo tiempo a prevenir las amenazas a la seguridad interior de los Estados miembros[21]. El VIS será un sistema de información centralizado que comprende una parte nacional en cada Estado participante y una unidad de apoyo técnico en Francia. El VIS usará un sistema de correspondencias biométricas (*Biometric Matching System* - BMS) para garantizar unas comparaciones fidedignas de las impresiones dactilares y verificar la identidad de los titulares de los visados en las fronteras exteriores. En él se incluirán datos sobre las solicitudes de visados, fotografías, impresiones dactilares, decisiones relacionadas de las autoridades responsables de los visados y enlaces entre aplicaciones relacionadas. Las autoridades encargadas de los visados, el asilo, la inmigración y el control fronterizo tendrán acceso a esta base de datos para identificar la identidad de los titulares de los visados y la autenticidad de los mismos; la policía y Europol podrán consultarlo para prevenir y combatir el terrorismo y otras formas graves de delincuencia[22]. Los expedientes de solicitud podrán conservarse cinco años. Los datos personales del VIS deberán tratarse de conformidad con las disposiciones específicas incluidas en los actos jurídicos de base que rigen este sistema (Reglamento (CE) nº 767/2008 y Decisión 2008/633/JAI del Consejo), que complementan las disposiciones de la Directiva 95/46/CE, el Reglamento (CE) nº 45/2001, la Decisión marco 2009/977/JAI del Consejo, el Convenio 108 del Consejo de Europa, su protocolo adicional 181 y la Recomendación policial[23]. El VIS se aplicará en todos los Estados miembros (excepto en el Reino Unido e Irlanda), así como en Suiza, Noruega e Islandia. Funcionará sobre la base de la red s-TESTA de la Comisión. La Comisión evaluará este sistema a los tres años de su puesta en marcha y posteriormente cada cuatro años.

---

19 Directiva 95/46/CE, DO L 281 de 23.11.1995, p. 31.

20 Consejo Extraordinario de Justicia e Interior de 20 de septiembre de 2001.

21 Decisión 2004/512/CE del Consejo, DO L 213 de 15.6.2004, p. 5; Reglamento (CE) nº 767/2008, DO L 218 de 13.8.2008, p. 60; Decisión 2008/633/JAI del Consejo, DO L 218 de 13.8.2008, p. 129. Véase también la Declaración sobre la lucha contra el terrorismo, Consejo Europeo, 25.3.2004.

22 Decisión 2008/633/JAI del Consejo, DO L 218 de 13.8.2008, p. 129.

23 Reglamento (CE) nº 767/2008, DO L 218 de 13.8.2008, p. 60; Decisión 2008/633/JAI del Consejo, DO L 218 de 13.8.2008, p. 129; Directiva 95/46/CE, DO L 281 de 23.11.1995, p. 31; Reglamento (CE) nº 45/2001, DO L 8 de 12.1.2001, p. 1; Decisión marco 2008/977/JAI del Consejo, DO L 350 de 30.12.2008, p. 60; Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE nº 108), Consejo de Europa, 28.1.1981 (Convenio del Consejo de Europa 108); Protocolo adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal relativo a las autoridades de control y a la transferencia de datos (ETS nº 181), Consejo de Europa, 8.11.2001 (Protocolo adicional 181). Recomendación nº R (87) 15 del Comité de Ministros por la que se regula el uso de datos personales en el ámbito policial, Consejo de Europa, 17.9.1987 (Recomendación policial).

A iniciativa española, el Consejo adoptó en 2004 una directiva que regula la transmisión de la **información previa sobre pasajeros** (*Advance Passenger Information* – API) por parte de los transportistas aéreos a las autoridades de control fronterizo.[24]. La finalidad de este instrumento es mejorar el control fronterizo y combatir la migración irregular. Si se les solicita, los transportistas deben comunicar a las autoridades de control fronterizo el nombre, la fecha de nacimiento, la nacionalidad, el punto de embarque y el paso fronterizo de entrada de los pasajeros que viajan a la UE desde terceros países. Estos datos personales se toman habitualmente de la parte legible mecánicamente de los pasaportes de los pasajeros y se remiten a las autoridades una vez se ha completado la facturación. Tras la llegada del vuelo, las autoridades y los transportistas pueden conservar 24 horas los datos de la API. El sistema API funciona de forma descentralizada a través del intercambio de información entre operadores privados y autoridades públicas. Este instrumento no permite el intercambio de API entre Estados miembros; sin embargo, los servicios represivos, distintos de los guardias de fronteras, pueden solicitar acceso a esta información a efectos represivos. Las autoridades públicas sólo pueden usar los datos personales con objeto del control fronterizo y combatir la migración irregular y sólo pueden tratarse de acuerdo con la Directiva 95/46/CE[25]. De aplicación en toda la UE, este instrumento sólo se utiliza en un pequeño número de Estados miembros. La Comisión revisará esta Directiva en 2011.

Una parte importante del Programa de 1992 de la Comisión, por el que se establecía el mercado interior, se refería a la supresión de todos los controles y formalidades respecto a las mercancías que circularan en la Comunidad[26]. La supresión de tales procedimientos en las fronteras interiores elevaba el riesgo de fraude, lo que hizo necesario que los Estados miembros establecieran, por una parte, un mecanismo de asistencia mutua administrativa que ayudara a prevenir, investigar y perseguir operaciones que infringieran la legislación comunitaria de aduanas y agricultura y, por otra parte, la cooperación aduanera para permitir detectar y perseguir las infracciones a las disposiciones aduaneras nacionales, en particular mejorando el intercambio transfronterizo de información. Sin perjuicio de la competencia de la UE en la unión aduanera[27], el **Convenio de Nápoles II** relativo a la asistencia mutua y la cooperación entre las administraciones aduaneras tiene por finalidad permitir a las administraciones aduaneras nacionales prevenir y detectar las infracciones de las disposiciones aduaneras nacionales y ayudarles a perseguir y castigar las infracciones a las disposiciones aduaneras comunitarias y nacionales[28]. De acuerdo con este instrumento, un grupo de unidades centrales de coordinación solicitan asistencia por escrito a sus homólogos de otros Estados miembros para las investigaciones penales referentes a infracciones de las normas aduaneras nacionales y comunitarias. Estas unidades sólo pueden tratar datos personales para los fines del Convenio de Nápoles II. Pueden transmitir esta información a las autoridades aduaneras nacionales, autoridades encargadas de las investigaciones y organismos judiciales y, previo consentimiento del Estado miembro que haya suministrado los datos, a otras autoridades. Los datos pueden conservarse por un periodo no superior al necesario para

---

24 Directiva 2004/82/CE del Consejo, DO L 261 de 6.8.2004, p. 24.

25 Directiva 95/46/CE, DO L 281 de 23.11.1995, p. 31.

26 Reglamento (CEE) 2913/92 del Consejo, DO L 302 de 19.10.1992.

27 Reglamento (CE) n° 515/97 del Consejo, de 13 marzo 1997, relativo a la asistencia mutua entre las autoridades administrativas de los Estados miembros y la colaboración entre éstas y la Comisión con objeto de asegurar la correcta aplicación de las regulaciones aduanera o agrícola, DO L 82 de 22.3.1997, p. 1, modificado por el Reglamento (CE) nº 766/2008, DO L 218, 13.8.2008, p. 48.

28 Convenio celebrado sobre la base del artículo K.3 del Tratado de la Unión Europea, relativo a la asistencia mutua y la cooperación entre las administraciones aduaneras, DO C 24 de 23.1.1998, p. 2 (Convenio de Nápoles II).

los fines para los que se entregaron. Los datos personales disfrutarán en el Estado miembro que los haya recibido como mínimo del mismo nivel de protección que en el Estado miembro que los haya suministrado y su tratamiento deberá cumplir lo dispuesto en la Directiva 95/46/CE y el Convenio 108 del Consejo de Europa[29]. Todos los Estados miembros han ratificado el Convenio de Nápoles II. Pueden proponer su modificación y una vez efectuada, el texto modificado debe ser adoptado por el Consejo de Ministros y ratificado por los Estados miembros.

Como complemento al Convenio de Nápoles II, el Convenio SIA despliega el **Sistema de Información Aduanero** (SIA) para ayudar a prevenir, investigar y perseguir infracciones graves de las legislaciones nacionales incrementando, a través de la difusión rápida de información, la efectividad de la cooperación entra las administraciones aduaneras de los Estados miembros[30]. El SIA, gestionado por la Comisión, es un sistema de información centralizado accesible a través de terminales situadas en cada Estado miembro y en la Comisión, Europol y Eurojust. Incluye datos personales con referencia a mercancías, medios de transporte, empresas, personas y bienes y dinero en efectivo retenidos, intervenidos o confiscados. Los datos personales son nombres y apodos, fecha y lugar de nacimiento, nacionalidad, sexo, características físicas, documentos de identidad, dirección, antecedentes de violencia, razón para introducir los datos en el SIA, actuación sugerida y registros de matriculación de los medios de transporte. En el caso de los bienes y el dinero en efectivo retenidos, intervenidos o confiscados, sólo se introducirán en el SIA los datos biográficos y una dirección. Esta información sólo se podrá utilizar para observaciones, informes o llevar a cabo inspecciones particulares o controles específicos, o para análisis estratégicos u operativos respecto a personas sospechosas de haber infringido o de infringir las disposiciones aduaneras nacionales. Las autoridades nacionales de aduanas, fiscales, agrícolas, de salud pública y policía, Europol y Eurojust podrán acceder a los datos del SIA[31]. El tratamiento de los datos personales deberán atenerse a las normas específicas que establece el Convenio SIA y lo dispuesto en la Directiva 95/46/CE, el Reglamento (CE) nº 45/2001, el Convenio 108 del Consejo de Europa y la Recomendación policial[32]. Los datos personales sólo se podrán copiar del SIA a otros sistemas de tratamiento de datos para análisis de gestión de riesgos u operativos, a los que sólo podrán acceder los analistas designados por los Estados miembros. Los datos personales copiados del SIA sólo se podrán conservar el tiempo necesario para lograr el fin para el que se copiaron y no más de diez años. El SIA establece también una **base de datos de identificación de los expedientes aduaneros** (FIDE) para ayudar a prevenir,

---

29 Directiva 95/46/CE, DO L 281 de 23.11.1995, p. 31; Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE nº 108), Consejo de Europa, 28.1.1981 (Convenio del Consejo de Europa 108).

30 Convenio establecido sobre la base del artículo K.3 del Tratado de la Unión Europea, relativo a la utilización de la tecnología de la información a efectos aduaneros, DO C 316 de 27.11.1995, p. 34, modificado por la Decisión 2009/917/JAI del Consejo, DO L 323 de 10.12.2009, p. 20.

31 A partir de mayo de 2011, Europol y Eurojust tendrán acceso de lectura al SIA sobre la base de la Decisión 2009/917/JAI del Consejo, DO L 323 de 10.12.2009, p. 20.

32 Convenio establecido sobre la base del artículo K.3 del Tratado de la Unión Europea, relativo a la utilización de la tecnología de la información a efectos aduaneros, DO C 316 de 27.11.1995, p. 34, modificado por la Decisión 2009/917/JAI del Consejo, DO L 323 de 10.12.2009, p. 20; Directiva 95/46/CE, DO L 281 de 23.11.1995, p. 31; Reglamento (CE) nº 45/2001, DO L 8 de 12.1.2001, p. 1; Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE nº 108), Consejo de Europa, 28.1.1981 (Convenio del Consejo de Europa 108); Recomendación nº R (87) 15 del Comité de Ministros por la que se regula el uso de datos personales en el ámbito policial, Consejo de Europa, 17.9.1987 (Recomendación policial).

investigar y perseguir infracciones graves de las leyes nacionales[33]. FIDE permite a las autoridades nacionales responsables de efectuar investigaciones aduaneras, al abrir un fichero de investigación, identificar a otras autoridades que hayan podido investigar a personas o empresas concretas. Estas autoridades pueden introducir en la FIDE datos procedentes de sus ficheros de investigación, incluidos los datos biográficos de las personas investigadas y el nombre de la empresa, el nombre comercial, numero de IVA y dirección de las empresas investigadas. Los datos procedentes de los ficheros de investigación en los que no se haya detectado fraude aduanero podrán almacenarse un máximo de tres años; los procedentes de los ficheros de investigación en los que se haya detectado un caso de fraude aduanero podrán almacenarse un máximo de seis años; y los de los ficheros en los se haya dictado condena o sanción podrán conservarse un máximo de diez años. El SIA y la FIDE utilizan la red de comunicación común, la red de sistema interfaz común o un acceso a la red seguro suministrado por la Comisión. El SIA está vigente en todos los Estados miembros. La Comisión, en cooperación con los Estados miembros, informa anualmente al Parlamento Europeo y al Consejo sobre el funcionamiento del SIA.

Instrumentos de la UE para prevenir y combatir el terrorismo y otras formas graves de delincuencia transfronteriza

Los ataques terroristas de marzo de 2004 en Madrid impulsaron varias iniciativas nuevas a nivel de la UE. A solicitud del Consejo Europeo, la Comisión presentó en 2005 una propuesta de instrumento que regulara el intercambio de información en virtud del principio de disponibilidad[34]. En lugar de aprobar esta propuesta, el Consejo adoptó en 2006 la **Iniciativa sueca**, que racionaliza los intercambios entre Estados miembros de cualquier información o inteligencia sobre actividades delictivas existente que pueda ser necesaria para una investigación o una operación de inteligencia penales[35]. Esta instrumento se asienta en el principio político de «acceso equivalente», según el cual las condiciones aplicables a los intercambios de datos transfronterizos no deben ser más estrictas que las que regulan el acceso en el propio país. La Iniciativa sueca funciona de forma descentralizada y permite a la policía, las aduanas y cualquier otra autoridad con competencias para investigar delitos (con excepción de los servicios de inteligencia, que habitualmente se ocupan de la información relacionada con la seguridad nacional o la del Estado) compartir información o inteligencia sobre actividades delictivas con sus homólogos del resto de la UE. Los Estados miembros deben designar puntos de contacto nacionales para tratar las solicitudes urgentes de información. Esta medida establece claros límites temporales para el intercambio de información y exige a los Estados miembros que rellenen un formulario al solicitar datos. Los Estados miembros tienen que responder a las solicitudes de información y datos en un plazo de ocho horas en los casos urgentes, de una semana en casos no urgentes y de dos semanas en todos los demás casos. El uso de información y datos obtenidos a través de este instrumento está sujeto a las legislaciones nacionales de protección de datos, según las cuales los Estados miembros no pueden aplicar un trato diferente a la información de fuentes nacionales y a la procedente de otros Estados miembros. El Estado miembro que entrega información o

---

33 FIDE, que corresponde a *Fichier d'Identification des Dossiers d'Enquêtes douanières*, se basa en el Reglamento (CE) nº 766/2008 y el Protocolo aprobado con arreglo al artículo 34 del Tratado de la Unión Europea, que modifica, en lo relativo a la creación de un fichero europeo de identificación de los expedientes de investigación aduanera, el Convenio relativo a la utilización de la tecnología de la información a efectos aduaneros, DO C 139 de 13.6.2003, p. 1.

34 COM(2005) 490 de 12.10.2005; Conclusiones de la Presidencia – Programa de La Haya, 4/5.11.2004. Véase también la Declaración sobre la lucha contra el terrorismo, Consejo Europeo, 25.3.2004.

35 Decisión marco 2006/960/JAI del Consejo, DO L 386 de 29.12.2006, p. 89.

inteligencia puede, sin embargo, fijar condiciones para su uso en otro Estado miembro. Los datos personales deben tratarse de acuerdo con la legislación nacional de protección de datos, con el Convenio 108 del Consejo de Europa, su protocolo adicional 181 y la Recomendación policial[36]. Doce de los 31 signatarios de esta medida (incluidos los Estados miembros de la UE, así como Noruega, Islandia, Suiza y Liechtenstein) han adoptado legislación nacional para su aplicación; cinco Estados rellenan habitualmente el formulario para solicitar información; pero sólo dos Estados lo usan con frecuencia para intercambiar información[37]. La Comisión debe presentar su informe de evaluación al Consejo antes de finales de 2010.

La **Decisión Prüm** se basa en un acuerdo celebrado en 2005 por Alemania, Francia, España, los Estados del Benelux y Austria para impulsar la cooperación en la lucha contra el terrorismo, la delincuencia transfronteriza y la migración irregular. En respuesta al interés expresado por varios Estados miembros para adherirse a este Tratado, Alemania propuso en su presidencia del Consejo de 2007 transformarlo en un instrumento de la UE. La Decisión Prüm de 2008, que se aplicará a partir de agosto de 2011, establece las normas para el intercambio transfronterizo de perfiles de ADN, impresiones dactilares, datos de los registros de matriculación de vehículos e información sobre individuos sospechosos de preparar ataques terroristas[38]. Su objetivo es mejorar la prevención de delitos, especialmente de terrorismo y transfronterizos, y mantener el orden público en relación con acontecimientos destacados. El sistema funcionará de forma descentralizada mediante la interconexión, a través de puntos de contacto nacionales, de las bases de datos de ADN, impresiones dactilares y registros de vehículos de los Estados participantes. Mediante la red s-Testa de la Comisión, los puntos de contacto tratarán las solicitudes entrantes y salientes de comparaciones transfronterizas de perfiles de ADN, impresiones dactilares y datos de los registros de matriculación de vehículos. Sus atribuciones para transmitir dichos datos a los usuarios finales se rigen por la legislación nacional. A partir de agosto de 2001, la comparación de datos se habrá informatizado completamente. Sin embargo, los Estados miembros deben pasar un riguroso proceso de evaluación (en el que se evalúa, en particular, que cumplen los requisitos de protección de datos y técnicos) para recibir la autorización y poder empezar a compartir datos de forma informatizada. Los datos personales no pueden intercambiarse con este instrumento hasta que los Estados miembros no garanticen un nivel de protección de datos como mínimo equivalente al resultante del Convenio 108 del Consejo de Europa, su protocolo adicional 181 y la Recomendación policial[39]. El Consejo decidirá por unanimidad si

---

36 Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE nº 108), Consejo de Europa, 28.1.1981 (Convenio del Consejo de Europa 108); Protocolo adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal relativo a las autoridades de control y a la transferencia de datos (ETS nº 108), Consejo de Europa, 8.11.2001 (Protocolo adicional 181). Recomendación nº R (87) 15 del Comité de Ministros por la que se regula el uso de datos personales en el ámbito policial, Consejo de Europa, 17.9.1987 (Recomendación policial).

37 Esta información se basa en las respuestas a un cuestionario, cuyos resultados presentó la presidencia española del Consejo en una reunión del grupo de trabajo ad hoc del Consejo sobre intercambio de información de 22 de junio de 2010.

38 Decisión 2008/615/JAI del Consejo, DO L 210 de 6.8.2008, p. 1; Decisión 2008/616/JAI del Consejo, DO L 210 de 06/08/2008, p. 12.

39 Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE nº 108), Consejo de Europa, 28.1.1981 (Convenio del Consejo de Europa 108); Protocolo adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal relativo a las autoridades de control y a la transferencia de datos (ETS nº 108), Consejo de Europa, 8.11.2001 (Protocolo adicional 181). Recomendación nº R (87) 15 del Comité de Ministros por la que se regula el uso de datos personales en el ámbito policial, Consejo de Europa, 17.9.1987 (Recomendación policial).

se ha cumplido o no esta condición. La información personal sólo podrá usarse para los fines para los que se entrega, salvo que el Estado miembro que la haya suministrado consienta su uso para otros fines. Las personas podrán también dirigirse a sus responsables de la protección de datos nacionales, designados por la Directiva 95/46/CE, para que se respeten sus derechos respecto al tratamiento de los datos personales en el marco de este instrumento. La comparación de los perfiles de ADN y las impresiones dactilares se efectuará sobre una base de respuestas positivas o negativas (anónimas) y las autoridades nacionales sólo podrán solicitar información personal sobre el interesado si la respuesta a su búsqueda original ha sido positiva. Las peticiones de información adicional se canalizarán habitualmente a través de la Iniciativa sueca. La Decisión Prüm se está aplicando en la UE-27, mientras que Noruega e Islandia están en proceso de adhesión a la misma[40]. La Comisión debe presentar su informe de evaluación al Consejo en 2012.

En respuesta a los atentados con bombas de julio de 2005 en Londres, el Reino Unido, Irlanda, Suecia y Francia propusieron la adopción de un instrumento de la UE que armonizara las normas nacionales aplicables a la conservación de datos. La **Directiva sobre conservación de datos** de 2006 obliga a los proveedores de servicios de telefonía e internet a conservar, con el fin de investigar, detectar y perseguir formas graves de delincuencia, los datos del tráfico de comunicaciones electrónicas y de localización, así como la información sobre los abonados (incluido su número de teléfono, dirección IP e identificador del equipo móvil)[41]. La Directiva sobre conservación de datos no regula el acceso a los datos conservados por las autoridades nacionales ni su uso. Su alcance excluye explícitamente el contenido de las comunicaciones electrónicas; en otros términos, no pueden realizarse escuchas telefónicas al amparo del este instrumento. Esta medida deja a los Estados miembros la tarea definir las «formas graves de delincuencia». Los Estados miembros también determinan qué autoridades nacionales pueden tener acceso a dichos datos caso por caso y los procedimientos para conceder el acceso a la información. Los periodos de conservación de datos varían de 6 a 24 meses. Las Directivas 95/46/CE y 2002/58/CE regulan la protección de los datos personales en este instrumento[42]. Seis Estados miembros todavía no han incorporado esta medida en su totalidad y los tribunales constitucionales de Alemania y Rumanía han declarado inconstitucional su legislación de aplicación nacional. El Tribunal Constitucional alemán consideró que las normas que regulan el acceso a los datos y su uso, tal como las establece la legislación nacional, eran inconstitucionales[43]. El Tribunal Constitucional rumano consideró que la conservación de datos *per se* infringía el artículo 8 del Convenio para la protección de los derechos humanos y de las libertades fundamentales (Convenio Europeo de Derechos Humanos) y que por consiguiente era inconstitucional[44]. La Comisión está evaluando actualmente este instrumento y va a presentar su informe de evaluación al Parlamento Europeo y al Consejo a finales de 2010.

La creación en curso de un **sistema de información europeo de antecedentes penales** (*European Criminal Records Information System* - ECRIS) se remonta a una iniciativa belga

---

40 Hasta la fecha diez Estados miembros han recibido autorización para iniciar el intercambio informatizado de perfiles de ADN; cinco están autorizados para las impresiones dactilares y siete para los datos de los registros de matriculación de vehículos. Alemania, Austria, España y los Países Bajos han entregado a la Comisión estadísticas parciales de su utilización de este instrumento.

41 Directiva 2006/24/CE, DO L 105 de 13.4.2006, p. 54.

42 Directiva 95/46/CE, DO L 281 de 23.11.1995, p. 31; Directiva 2002/58/CE, DO L 201 de 31.7.2002, p. 37 (Directiva relativa a la intimidad en las comunicaciones electrónicas).

43 Sentencia del Tribunal Constitucional alemán, Bundesverfassunggericht 1 BvR 256/08, 11.3.2008.

44 Decisión nº 1258 del tribunal Constitucional rumano, 8.10.2009.

de 2004 que perseguía inhabilitar a los delincuentes condenados por delitos sexuales para trabajar con niños en otros Estados miembros. Los Estados miembros se basaban anteriormente en el Convenio del Consejo de Europa sobre ayuda mutua en materia penal para intercambiar información sobre las resoluciones condenatorias a sus nacionales, pero este sistema se reveló ineficiente[45]. El Consejo dio un primer paso hacia su reforma adoptando la Decisión 2005/876/JAI del Consejo, por la cual los Estados miembros debían crear una autoridad central que enviaría, a intervalos regulares, las condenas de no nacionales al Estado o Estados miembros de nacionalidad[46]. Esta instrumento permitía también a los Estados miembros obtener, por primera vez y de conformidad con la legislación nacional, las condenas anteriores pronunciadas contra sus propios nacionales en otros Estados miembros. Podían solicitar tal información rellenando un formulario normalizado en vez de a través de los procedimientos de asistencia jurídica recíproca. En 2006 y 2007, la Comisión presentó un amplio paquete legislativo compuesto por tres instrumentos: Decisión marco 2008/675/JAI del Consejo por la que se obliga a los Estados miembros a tener en cuenta condenas anteriores con motivo de nuevos procesos penales; Decisión marco 2008/315/JAI del Consejo relativa a la organización y al contenido del intercambio de información de los registros de antecedentes penales; y Decisión 2009/316/JAI del Consejo por la que se crea el ECRIS como medio técnico para intercambiar información extraída de los registros de antecedentes penales[47]. Previstas para su aplicación a partir de abril de 2012, las Decisiones marco 2009/315/JAI y 2009/316/JAI del Consejo pretenden definir las formas en que un Estado miembro de condena debe transmitir la información relativa a una nueva condena al Estado o Estados miembros de la nacionalidad de la persona condenada, las obligaciones de almacenamiento y un marco para un sistema informatizado de intercambio de información. El ECRIS será un sistema de información descentralizado que interconectará las bases de datos de los registros de antecedentes penales de los Estados miembros a través de la red s-TESTA de la Comisión. Un equipo de autoridades centrales intercambiará los datos sobre las nuevas condenas de sus ciudadanos y los registros de antecedentes. Los datos estarán cifrados, estructurados según un formato predeterminado e incluirán lo siguiente: detalles biográficos; la condena, la sentencia y el delito subyacente, e información adicional (incluidas las impresiones dactilares, si se dispone de ellas). A partir de abril de 2012, deberán suministrarse extractos de los registros de antecedentes penales para los procesos penales en curso y remitirlos a las autoridades judiciales o administrativas competentes tales como los organismos autorizados para investigar personas para empleos sensibles o tenencia de armas. Los datos personales suministrados para procesos penales sólo pueden usarse para ese fin; su utilización para cualquier otra finalidad requiere el consentimiento del Estado miembro que la haya facilitado. El tratamiento de los datos personales debe atenerse a las disposiciones específicas establecidas en la Decisión marco 2009/315/JHA del Consejo, que incorpora las normas de la Decisión 2005/876/JAI del Consejo, así como la Decisión 2009/977/JAI del Consejo y el Convenio 108 del Consejo de Europa[48]. Para los tratamientos de datos personales que

---

45 Convenio europeo de asistencia judicial en materia penal (STE nº 30), Consejo de Europa, 20.4.1959. Véase también COM(2005)10 de 25.1.2005.

46 Decisión 2005/876/JAI del Consejo, DO L 322 de 9.12.2005, p. 33.

47 Decisión marco 2008/675/JAI del Consejo, DO L 220 de 15.8.2008, p. 32; Decisión marco 2009/315/JAI del Consejo, DO L 93 de 7.4.2009, p. 23; Decisión 2009/316/JAI del Consejo, DO L 93 de 7.4.2009, p. 33. Véase también COM(2005)10 de 25.1.2005.

48 Decisión marco 2009/315/JAI del Consejo, DO L 93 de 7.4.2009, p. 23; Decisión 2005/876/JAI del Consejo, DO L 322 de 9.12.2005, p. 33; Decisión marco 2008/977/JAI del Consejo, DO L 350 de 30.12.2008, p. 60; Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE nº 108), Consejo de Europa, 28.1.1981 (Convenio del Consejo de Europa 108).

efectúen las instituciones de la UE usando el ECRIS, por ejemplo para garantizar la seguridad de datos, se aplicará el Reglamento (CE) 45/2001[49]. Este paquete legislativo no incluye normas sobre la conservación de datos, ya que el almacenamiento de información relacionada con condenas penales está regulado por las legislaciones nacionales. Quince Estados miembros están participando actualmente en un proyecto piloto y nueve de ellos han iniciado el intercambio electrónico de información extraída de los registros de antecedentes penales. La Comisión deberá presentar al Parlamento Europeo y al Consejo dos informes de evaluación relativos al funcionamiento de este paquete legislativo: la Decisión marco 2006/675/JAI del Consejo se revisará en 2011; la Decisión marco 2009/315/JAI del Consejo se revisará en 2015. A partir de 2016, la Comisión deberá publicar también informes regulares sobre el funcionamiento del ECRIS.

A iniciativa finlandesa, el Consejo adoptó en 2000 un instrumento por el que se organiza el intercambio de información entre las **unidades de información financiera** (UIF, *Financial Intelligence Units* - FIU) para combatir el blanqueo de capitales y, posteriormente, la financiación del terrorismo[50]. Las UIF las crean habitualmente los organismos encargados de los servicios represivos, autoridades judiciales u órganos administrativos que informan a las autoridades financieras. Estos cuerpos deben compartir los datos financieros o policiales que sean necesarios, incluidos los detalles de las transacciones financieras, con sus homólogos de la UE, excepto en los casos en los que esta divulgación fuera desproporcionada respecto a los intereses de personas físicas o jurídicas. La información proporcionada para analizar o investigar el blanqueo de capitales o la financiación del terrorismo puede utilizarse también para investigaciones o acciones penales salvo que el Estado miembro que la entregue prohíba tal uso. El tratamiento de los datos personales debe respetar lo dispuesto en la Decisión marco 2009/977/JAI del Consejo, el Convenio del Consejo de Europa de 108 y su Recomendación policial[51]. En 2002, varios Estados miembros crearon FIU.net, una aplicación para una red descentralizada que trata el intercambio de datos entre las UIF y que usa la red s-TESTA de la Comisión[52]. Esta iniciativa tiene veinte UIF como miembros. Se está debatiendo actualmente si utilizar la aplicación segura SIENA de Europol para el funcionamiento de FIU.net[53]. Tras haber evaluado si los Estados miembros cumplían los requisitos de este instrumento, el Consejo facultó a las UIF, mediante la tercera Directiva contra el blanqueo de capitales, para recibir, analizar y difundir informes sobre transacciones sospechosas relacionadas con el blanqueo de capitales *y* la financiación del terrorismo[54]. Como parte de su Plan de acción sobre servicios financieros, la Comisión ha estado revisando la aplicación de la tercera Directiva contra el blanqueo de capitales desde 2009[55].

---

49 Reglamento (CE) nº 45/2001, DO L 8 de 12.1.2001, p. 1.

50 Decisión 2000/642/JAI del Consejo, DO L 271 de 24.10.2000, p. 4.

51 Decisión marco 2008/977/JAI del Consejo, DO L 350 de 30.12.2008, p. 60; Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE nº 108), Consejo de Europa, 28.1.1981 (Convenio del Consejo de Europa 108); Recomendación nº R (87) 15 del Comité de Ministros por la que se regula el uso de datos personales en el ámbito policial, Consejo de Europa, 17.9.1987 (Recomendación policial).

52 http://www.fiu.net/

53 SIENA corresponde a *Secure Information Exchange Network Application* (Red de Intercambio Seguro de Información).

54 Directiva 2005/60/CE, DO L 309 de 25.11.2005, p 15 (tercera Directiva contra el blanqueo de capitales).

55 Véase, por ejemplo, *Evaluation of the economic impacts of the Financial Services Action Plan – Final report* (para la Comisión Europea, DG MARKT), CRA International, 3.2009.

Suscribiendo una iniciativa propuesta por Austria, Bélgica y Finlandia, el Consejo adoptó en 2007 un instrumento destinado a mejorar la cooperación entre **organismos de recuperación de activos** (ORA, *Asset Recovery Offices* - ARO) para rastrear e identificar los productos del delito[56]. Igual que las UIF, los ORA cooperan sobre una base descentralizada, pero sin ayuda de una plataforma en línea. Deben usar la Iniciativa sueca para intercambiar información, especificando los detalles de los bienes buscados, tales como cuentas bancarias, bienes inmobiliarios y vehículos, así como los detalles de las personas físicas o jurídicas buscadas, con nombre y apellidos, dirección, fecha de nacimiento e información sobre el accionista o la empresa. El uso de información intercambiada a través de este instrumento está sujeto a las legislaciones nacionales de protección de datos, según las cuales los Estados miembros no pueden aplicar un trato diferente a la información de fuentes nacionales y a la procedente de otros Estados miembros. El tratamiento de los datos personales debe cumplir lo dispuesto en el Convenio 108 del Consejo de Europa, su protocolo adicional 181 y la Recomendación policial[57]. Hasta la fecha, más de veinte Estados miembros han creado sus ORA. Dado el carácter sensible de la información intercambiada, se está debatiendo actualmente si utilizar la aplicación segura SIENA de Europol para intercambiar datos entre los ORA. En un proyecto piloto iniciado en mayo de 2010, doce ORA empezaron a utilizar SIENA para compartir información de interés para el seguimiento de activos. La Comisión debe presentar un informe de evaluación al Consejo en 2010.

En 2008, la presidencia francesa del Consejo invitó a los Estados miembros a crear **plataformas de alerta contra la delincuencia informática** nacionales, y a Europol una plataforma europea de alerta contra la delincuencia informática, para recoger, analizar e intercambiar información sobre delitos cometidos en internet[58]. Los ciudadanos pueden informar a sus plataformas nacionales de los casos de contenido o comportamiento ilegales detectados en internet. La plataforma europea contra la delincuencia informática (*European Cybercrime Platform* - ECCP), gestionada por Europol, funcionará como centro de información que analizará e intercambiará con las autoridades nacionales encargadas de los servicios represivos aplicación de la ley información relacionada con los delitos informáticos que entren en el mandato de Europol[59]. Hasta la fecha, casi todos los Estados miembros han creado plataformas nacionales de alerta contra la delincuencia informática. Europol está trabajando en la ejecución técnica de la ECCP y pronto desplegará su aplicación SIENA con el fin de mejorar el intercambio de datos con las plataformas nacionales. En la medida en que esa intercambio de información afecte al tratamiento de los datos personales por parte de Europol, serán de aplicación las correspondientes disposiciones de protección de datos

---

56 Decisión 2007/845/JAI del Consejo, DO L 332 de 18.12.2007, p. 103.

57 Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE nº 108), Consejo de Europa, 28.1.1981 (Convenio del Consejo de Europa 108); Protocolo adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal relativo a las autoridades de control y a la transferencia de datos (ETS nº 181), Consejo de Europa, 8.11.2001 (Protocolo adicional 181). Recomendación nº R (87) 15 del Comité de Ministros por la que se regula el uso de datos personales en el ámbito policial, Consejo de Europa, 17.9.1987 (Recomendación policial).

58 Conclusiones del Consejo sobre la creación de plataformas nacionales de aviso y una plataforma europea de aviso para informar sobre infracciones observadas en internet, Consejo de Justicia y Asuntos de Interior, 24.10.2008; Conclusiones del Consejo relativas a un Plan de acción para aplicar la estrategia concertada para combatir la delincuencia, Consejo de Asuntos Generales, 26.4.2010. Europol ha rebautizado su proyecto como «*European Cybercrime Platform*» (ECCP).

59 El objetivo de Europol es prevenir y combatir la delincuencia organizada, el terrorismo y otras formas de delincuencia grave que afecten a dos o más Estados miembros. Véase la Decisión marco 2009/371/JAI del Consejo, DO L 121 de 15.5.2009, p. 37.

incluidas en la Decisión Europol (Decisión 2008/839/JAI del Consejo), así como el Reglamento (CE) 45/2001, el Convenio de 108 del Consejo de Europa, su protocolo adicional 181 y la Recomendación policial[60]. Lo dispuesto en la Decisión marco 2009/977/JAI del Consejo regulan el intercambio de datos personales entre los Estados miembros y Europol[61]. A falta de instrumento jurídico, no existe un mecanismo oficial de revisión de las plataformas de alerta contra la delincuencia informática. Sin embargo, Europol ya cubre esta importante área y, en el futuro, informará de las actividades de la ECCP en su Informe anual presentado al Consejo para su aprobación y al Parlamento Europeo para información.

Agencias y organismos de la UE encargados de ayudar a los Estados miembros a prevenir y combatir las formas graves de delincuencia transfronteriza

Creada en 1995, la **Oficina Europea de Policía** (Europol) empezó a funcionar en 1999 y en enero de 2010 se convirtió en una agencia de la UE[62]. Su objetivo es ayudar a los Estados miembros a prevenir y combatir la delincuencia organizada, el terrorismo y otras formas de delincuencia grave que afecten a dos o más Estados miembros. Sus tareas principales consisten en recoger, almacenar, tratar, analizar e intercambiar información y datos; prestar asistencia para las investigaciones; y proporcionar apoyo en materia de análisis e información a los Estados miembros. El principal órgano de enlace entre Europol y los Estados miembros son las unidades nacionales de Europol (UNE), que envían funcionarios de enlace a Europol. Los jefes de las UNE se reúnen con regularidad para ayudar a Europol en materias operativas, mientras que el funcionamiento de la agencia está supervisado por un consejo de administración y el director. Las herramientas de gestión de la información de Europol incluyen el sistema de información de Europol (*Europol Information System* - EIS), los ficheros de trabajo de análisis (*Analysis Work Files* - AWF) y la aplicación SIENA. El EIS contiene los datos personales, incluidos, entre otros, los identificadores biométricos, las condenas penales y las relaciones con la delincuencia organizada, de las personas sospechosas de cometer delitos que entran en el mandato de Europol. El acceso se limita a las UNE, funcionarios de enlace, personal de Europol autorizado y el director. Los AWF, abiertos para ayudar a las investigaciones penales, incluyen datos sobre individuos y cualquier otra información que las UNE puedan decidir añadir. Los funcionarios de enlace tienen acceso, pero sólo los analistas pueden introducir datos en estos ficheros. Un sistema de índice permite a las UNE y a los funcionarios de enlace verificar si un AWF contiene información de interés para su Estado miembro. La aplicación SIENA de Europol es utilizada cada vez más por los Estados miembros para compartir datos sensibles a efectos represivos. Europol puede tratar información y datos, incluidos los datos personales, para llevar a cabo sus tareas; los Estados miembros sólo pueden usar la información obtenida de los ficheros de datos de Europol con el fin de prevenir y combatir las formas graves de delincuencia de carácter transfronterizo. Cualquier restricción que imponga el Estado miembro que suministre la información a su

---

60 Decisión 2009/371/JAI del Consejo, DO L 121 de 15.5.2009, p. 37; Reglamento (CE) nº 45/2001, DO L 8 de 12.1.2001, p. 1. Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE nº 108), Consejo de Europa, 28.1.1981 (Convenio del Consejo de Europa 108); Protocolo adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal relativo a las autoridades de control y a la transferencia de datos (ETS nº 181), Consejo de Europa, 8.11.2001 (Protocolo adicional 181). Recomendación nº R (87) 15 del Comité de Ministros por la que se regula el uso de datos personales en el ámbito policial, Consejo de Europa, 17.9.1987 (Recomendación policial).

61 Decisión marco 2008/977/JAI del Consejo, DO L 350 de 29.12..2006, p. 60.

62 Decisión 2009/371/JAI, DO L 121 de 15.5.2009, p. 37, que sustituye al Convenio, 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, p. 2.

utilización se aplicará también a los demás usuarios que extraigan esos datos de los ficheros de Europol. Europol también puede intercambiar información personal con terceros países que hayan suscrito acuerdos operativos con Europol y que garanticen un nivel adecuado de protección de los datos. Podrá conservar los datos sólo el tiempo necesario para efectuar sus tareas. Los AWF podrán conservarse un plazo máximo de tres años, con la posibilidad de ampliarlo otros tres años El tratamiento de datos personales por parte de Europol debe atenerse a lo establecido en las normas específicas sobre protección de datos incluidas en su propio instrumento regulador (Decisión 2009/371/JAI del Consejo), así como el Reglamento (CE) 45/2001, el Convenio 108 del Consejo de Europa, su protocolo adicional 181 y la Recomendación policial[63]. Lo dispuesto en la Decisión marco 2009/977/JAI del Consejo se aplica al intercambio de datos personales entre los Estados miembros y Europol[64]. Una autoridad común de control, compuesta por miembros de las autoridades nacionales de control, supervisa el tratamiento de los datos personales por parte de Europol, así como la transmisión por Europol de datos personales a otras partes. Presenta informes regulares al Parlamento Europeo y al Consejo. Europol presenta un informe anual sobre sus actividades al Consejo para su aprobación y al Parlamento Europeo para información.

Además de su impacto sobre distintos instrumentos ya descritos, los ataques terroristas de 11 de septiembre de 2001 contribuyeron a la creación, en 2002, de la **Unidad Europea de Cooperación Judicial** (Eurojust)[65]. Eurojust es un organismo de la UE cuyo objetivo es mejorar la coordinación de investigaciones y acciones penales en los Estados miembros y la coordinación entre las autoridades nacionales competentes. Cubre los mismos tipos de delincuencia y delitos que Europol. Con este mandato y para la ejecución de sus tareas, los 27 miembros nacionales de Eurojust, que forman su Colegio, tienen acceso a los datos personales de los sospechosos y delincuentes. Estos datos incluyen, entre otras cosas, lo siguiente: información biográfica, datos de contacto, datos de los registros de matriculación de vehículos, perfiles de ADN, fotografías, impresiones dactilares, así como datos sobre el tráfico, la localización y el abonado suministrados por los proveedores de servicios de telecomunicaciones. Los Estados miembros deberán intercambiar esa información con Eurojust para que pueda realizar sus tareas. Todos los datos personales relacionados con los casos deberán introducirse en el sistema automático de gestión de asuntos de Eurojust, que funciona sobre la base de la red s-TESTA de la Comisión. Un sistema de índice almacena los datos personales y no personales relevantes para las investigaciones en curso. Eurojust puede tratar datos personales para ejecutar sus tareas, pero estas operaciones deben cumplir las normas específicas incluidas en el propio instrumento regulador de Eurojust (Decisión 2009/426/JAI del Consejo), así como el Convenio 108 del Consejo de Europa, su protocolo adicional 181 y la Recomendación policial. Lo dispuesto en la Decisión marco 2009/977/JAI del Consejo se aplica al intercambio de datos personales entre los Estados miembros y

---

63 Decisión 2009/371/JAI del Consejo, DO L 121 de 15.5.2009, p. 37; Reglamento (CE) nº 45/2001, DO L 8 de 12.1.2001, p. 1. Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE nº 108), Consejo de Europa, 28.1.1981 (Convenio del Consejo de Europa 108); Protocolo adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal relativo a las autoridades de control y a la transferencia de datos (ETS nº 181), Consejo de Europa, 8.11.2001 (Protocolo adicional 181). Recomendación nº R (87) 15 del Comité de Ministros por la que se regula el uso de datos personales en el ámbito policial, Consejo de Europa, 17.9.1987 (Recomendación policial).

64 Decisión marco 2008/977/JAI del Consejo, DO L 350 de 29.12..2006, p. 60.

65 Decisión 2002/187/JAI del Consejo, DO L 63 de 6.3.2002, p. 1, modificada por la Decisón 2009/426/JAI del Consejo, DO L 138 de 4.6.2009, p. 14. Véase también el Consejo Extraordinario de Justicia e Interior de 20 de septiembre de 2001.

Eurojust[66]. Eurojust puede intercambiar datos con las autoridades nacionales y terceros países con los que haya celebrado acuerdos, siempre que el miembro nacional que haya suministrado los datos haya autorizado dicha transferencia y el tercer país garantice un nivel adecuado de protección de los datos personales. Los datos personales pueden conservarse el tiempo necesario para que Eurojust pueda alcanzar sus objetivos, pero deberán eliminarse una vez se haya cerrado el caso. Los Estados miembros deberán aplicar el fundamento jurídico modificado de Eurojust a más tardar en junio de 2011. Antes de junio de 2014, la Comisión tendrá que revisar, y podrá proponer los cambios que considere apropiados, el intercambio de información entre los miembros nacionales de Eurojust. Antes de junio de 2013, Eurojust tendrá que informar al Consejo y a la Comisión sobre la experiencia de conceder acceso a nivel nacional a su sistema de gestión de asuntos. Los Estados miembros podrán revisar los derechos nacionales de acceso sobre esta base. Una autoridad común de control, compuesta por jueces nombrados por los Estados miembros, supervisa el tratamiento de datos personales por parte de Eurojust e informa anualmente al Consejo. El Presidente del Colegio presenta al Consejo un informe anual sobre las actividades de Eurojust, que el Consejo transmite al Parlamento Europeo.

Acuerdos internacionales para prevenir y combatir el terrorismo y otras formas graves de delincuencia transnacional

Como consecuencia de los ataques terroristas del 11 de septiembre de 2001, los EE.UU. aprobaron una legislación que exigía a las compañías aéreas que efectúan vuelos hacia, desde o a través de su territorio que suministraran a las autoridades estadounidenses los datos del **registro de nombres de pasajeros** (*Passenger Name Record* - PNR) almacenados en sus sistemas informatizados de reserva. Pronto Canadá y Australia decidieron hacer lo mismo. Dado que la legislación de la UE aplicable exige que se evalúe previamente el nivel de protección de datos que garantizan los terceros países, la Comisión intervino para cumplir esta función y negoció acuerdos PNR con estos países[67]. Firmó el acuerdo con los EE.UU. en julio de 2007, con Australia en junio de 2008 y un acuerdo API/PNR con Canadá en octubre de 2005[68]. Los acuerdos con los EE.UU. y Canadá se aplican provisionalmente mientras que el canadiense sigue en vigor a pesar de que en septiembre de 2009 expiró la decisión de la Comisión sobre el carácter adecuado de las normas canadienses de protección de datos[69]. Crítico con su contenido, el Parlamento Europeo ha pedido a la Comisión que renegocie los tres acuerdos sobre la base de un claro conjunto de principios[70]. Enviados bastante antes de la salida del vuelo, los datos PNR ayudan a las autoridades policiales a controlar a los pasajeros sobre sus posibles vínculos con actividades terroristas u otras formas graves de delincuencia. Por consiguiente, el objetivo de cada acuerdo es prevenir y combatir el terrorismo y otras formas graves de delincuencia transnacional. A cambio de los datos PNR de la UE, el Departamento de seguridad interna (*Department of Homeland Security* - DHS) de los EE.UU.

---

66 Decisión marco 2008/977/JAI del Consejo, DO L 350 de 30.12..2006, p. 60.

67 Directiva 95/46/CE (Directiva sobre protección de datos), DO L 281 de 23.11.1995, p. 31.

68 El paquete canadiense consiste en un compromiso por parte de Canadá relativo al tratamiento de los datos API/PNR, la decisión sobre el carácter adecuado de las normas canadienses de protección de datos y un acuerdo internacional (véanse los DO L 91 de 29.3.2006, p. 4, y DO L 82 de 21.3.2006, p. 14). El acuerdo con los EE.UU. se encuentra en el DO L 204 de 4.8.2007, p. 16, y el australiano en el DO L 213 de 8.8.2008, p.47.

69 En 2009 Canadá se comprometió con la Comisión, la Presidencia del Consejo y los Estados miembros de la UE a que seguiría aplicando su compromiso anterior, de 2005, relativo al uso de los datos PNR de la UE. La decisión de la Comisión sobre el carácter adecuado se basaba en este compromiso anterior.

70 Resolución del Parlamento Europeo, P7_TA(2010)0144, 5.5.2010.

comparte la «información sobre pistas», resultante de su análisis de los PNR, con los servicios represivos, Europol y Eurojust; y tanto Canadá como los EE.UU. se han comprometido en sus respectivos acuerdos a cooperar con la UE para crear su propio sistema PNR. Los acuerdos estadounidense y australiano contienen 19 categorías de datos, incluidos los biográficos, de reservas, de pago e información suplementaria; el acuerdo canadiense incluye 25 tipos de datos similares. La información suplementaria incluye datos sobre billetes de ida sólo, situación de *stand by* y situación «no presentado». El acuerdo con los EE.UU. permite también, en condiciones especiales, utilizar información sensible. El DHS puede tratar dicha información si está en peligro la vida de la persona de cuyos datos se trata o la de otras personas, pero debe borrarla en el plazo de 30 días. Los PNR se envían a un conjunto de unidades centrales del DHS, a la Agencia de servicios fronterizos de Canadá (*Canada Border Services Agency*) y al servicio de aduanas australiano, que sólo pueden compartirlos con otras autoridades nacionales responsables de los servicios represivos o de la lucha antiterrorista. En el acuerdo con los EE.UU., el DHS espera que el nivel de protección de datos que tiene que aplicar al tratamiento de los datos PNR originarios de la UE «no sea más estricto» que el que aplican las autoridades de la UE en sus sistemas PNR nacionales. Si no se cumple este requisito, puede suspender determinadas partes del acuerdo. La UE considera que Canadá y Australia disponen de un nivel «adecuado» de protección de los datos PNR originarios de la UE si cumplen los términos de sus respectivos acuerdos. En los EE.UU. los PNR originarios de la UE se conservan siete años en una base de datos activa y ocho años más en una inactiva. En Australia se conservan en una base de datos activa durante 3,5 años y posteriormente en una base de datos inactiva durante dos años. En ambos países, sólo se puede acceder a la base de datos inactiva con autorización especial. En Canadá, los datos se conservan durante 3,5 años, pasando la información al anonimato al cabo de 72 horas. Todos los acuerdos fijan unas revisiones periódicas, mientras que los acuerdos canadiense y australiano incluyen también una cláusula de denuncia. En la UE, sólo el Reino Unido tiene un sistema PNR. Francia, Dinamarca, Bélgica, Suecia y los Países Bajos han promulgado la correspondiente legislación o están ensayando actualmente el uso de los datos PNR como preparación para crear sistemas PNR. Otros Estados miembros están considerando la creación de sistemas PNR y todos los Estados miembros usan, sobre una base de caso por caso, datos PNR para fines represivos.

Tras los ataques del 11 de septiembre de 2001, el Departamento del Tesoro de los EE.UU. desarrolló un **Programa de seguimiento de la financiación del terrorismo** (*Terrorist Finance Tracking Program* - TFTP) para identificar, rastrear y perseguir a los terroristas y a sus fuentes de financiación. Con arreglo al TFTP, el Tesoro de los EE.UU. solicitó mediante requerimientos administrativos a la filial estadounidense de una empresa belga que transfiriera al Tesoro series limitadas de datos de mensajería financiera que habían transitado por su red. En enero de 2010 esta empresa cambió la arquitectura de su sistema, lo que redujo en más de la mitad el volumen de datos bajo jurisdicción de los EE.UU que normalmente pueden ser objeto de requerimientos por Parte del Tesoro. En noviembre de 2009, la Presidencia del Consejo de la Unión Europea y el Gobierno de los Estados Unidos firmaron un acuerdo interino relativo al tratamiento y transferencia entre la UE y los EE.UU. de datos de mensajería financiera con fines TFTP, que no aprobó el Parlamento Europeo[71]. Sobre la base de un nuevo mandato, la Comisión Europea negoció un nuevo proyecto de acuerdo con los EE.UU., presentando al Consejo el 18 de junio de 2010 una propuesta de decisión del Consejo relativa a la celebración del Acuerdo entre la Unión Europea y los Estados Unidos de América relativo al tratamiento y la transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos, a efectos del Programa de Seguimiento de la Financiación del

[71] Resolución del Parlamento Europeo, P7_TA(2010)0029, 11.2.2010.

Terrorismo (Acuerdo TFTP UE-EE.UU.)[72]. El Parlamento Europeo dio su consentimiento a la celebración de este acuerdo el 8 de julio de 2010[73]. Se espera ahora que el Consejo adopte una Decisión del Consejo por la que se celebre este acuerdo, tras lo cual el acuerdo entrará en vigor mediante un Canje de Notas entre las dos partes. La finalidad del Acuerdo TFTP UE-EE.UU. es prevenir, detectar, investigar o perseguir el terrorismo o su financiación. Obliga a los proveedores de servicios de mensajería financiera a transferir al Tesoro de los EE.UU., sobre la base de evaluaciones de amenazas geográficas específicas y solicitudes individualizadas, conjuntos de datos de mensajería financiera que incluyeran, entre otros, el nombre, el número de cuenta, dirección y número de identificación del ordenante y el receptor o receptores de las transacciones financieras. El Tesoro sólo puede buscar estos datos para los fines del TFTP y sólo si tiene razones para creer que una persona identificada tiene conexión con el terrorismo o su financiación. Está prohibida la extracción de datos y la transferencia de datos relacionados con transacciones en la Zona Única de Pagos en Euros. Los EE.UU. entregará a los Estados miembros de la UE, a Europol y a Eurojust cualquier «información sobre pistas» relativa a posibles tramas terroristas en la UE y ayudará a la UE a crear su propio sistema equivalente al TFTP. Si la UE creara este programa, ambas partes podrían reajustar los términos de este acuerdo. Antes de poder transferir los datos, todas las solicitudes de información de los EE.UU. podrán ser investigadas por Europol para garantizar que cumplen las condiciones de este acuerdo. La información extraída de los mensajes financieros podrá conservarse sólo el tiempo necesario para las investigaciones o acciones penales específicas; los datos no extraídos podrán conservarse hasta cinco años. Cuando sea necesario para investigar, prevenir o perseguir el terrorismo o su financiación, el Tesoro puede transferir a las autoridades encargadas de los servicios represivos, de seguridad pública o lucha antiterrorista, a los Estados miembros de la UE, a Europol o a Eurojust los datos personales extraídos de los mensajes FIN. También pueden compartir con terceros países toda información sobre pistas relativa a nacionales de la UE y de residentes en ella, siempre que el Estado miembro afectado dé su consentimiento. El cumplimiento por las partes de la estricta limitación de la finalidad a la lucha antiterrorista del acuerdo y otras salvaguardias estará sujeto a seguimiento por supervisores independientes, incluida una persona nombrada por la Comisión. Tendrá una duración de cinco años y podrá darse por concluido o suspendido por cualquiera de las partes. Un equipo de revisión dirigido por la Comisión y del que formarán parte representantes de dos organismos de protección de datos y una persona con experiencia judicial revisará el acuerdo a los seis meses de su entrada en vigor, evaluando en particular la aplicación por las partes de las disposiciones sobre la limitación de su finalidad y proporcionalidad y el cumplimiento de sus obligaciones de protección de datos. El informe de la Comisión se presentará al Parlamento Europeo y al Consejo.

2.2. Iniciativas con arreglo al Plan de Acción del Programa de Estocolmo

Propuestas legislativas que va a presentar la Comisión

En el Programa de Estocolmo, el Consejo Europeo solicitó a la Comisión que presentara tres propuestas relacionadas directamente con la presente comunicación: un sistema PNR de la UE para prevenir, detectar y perseguir el terrorismo y las formas graves de delincuencia; un sistema de entrada y salida y un programa de viajeros registrados. El Consejo Europeo insistió en que estas dos últimas se presentaran «lo antes posible». La Comisión ha incorporado estas

[72] COM(2010)316 de 15.6.2010.

[73] Resolución del Parlamento Europeo, P7_TA-PROV(2010)0279, 8.7.2010.

tres peticiones a su Plan de Acción del Programa de Estocolmo[74]. Ahora realizará estas peticiones y, en el futuro, evaluará estos instrumentos basándose en los principios de desarrollo de las políticas que se contemplan en la sección 4.

En noviembre de 2007, la Comisión presentó una propuesta de decisión marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros (*Passenger Name Record* - PNR) con fines represivos[75]. Esta iniciativa recibió apoyo en el Consejo y posteriormente fue modificada para tener en cuenta las modificaciones propuestas por el Parlamento Europeo y la opinión del Supervisor Europeo de Protección de Datos. Con la entrada en vigor del Tratado de Lisboa quedó sin objeto. Como se señaló en el Plan de Acción del Programa de Estocolmo, la Comisión se encuentra actualmente trabajando para presentar, a principios de 2011, un paquete de **Registro de nombres de pasajeros** (*Passenger Name Record* - PNR) que consiste en lo siguiente: una comunicación sobre una estrategia externa PNR de la UE que subraye los principios esenciales que rigen la negociación de acuerdos con terceros países; las directrices de negociación para la renegociación de acuerdos PNR con los EE.UU. y Australia; y directrices de negociación para un nuevo acuerdo con Canadá. La Comisión se encuentra también en proceso de preparación de una nueva propuesta de PNR de la UE.

En 2008, la Comisión presentó una serie de sugerencias para desarrollar un sistema de gestión integrada de fronteras en la UE que facilite los desplazamientos de los nacionales de terceros países y refuerce la seguridad interior[76]. Constatando que las personas que rebasan la duración de estancia autorizada constituía el mayor grupo de migrantes irregulares de la UE, sugirió la posible introducción de un **sistema de entrada y salida** (*Entry/Exit System* – EES) para los nacionales de terceros países que entren en la UE para estancias breves de hasta tres meses. Este sistema registraría el momento y lugar de entrada y el tiempo de la estancia autorizada y transmitiría automáticamente alertas a las autoridades competentes para identificar a las personas que rebasaran la duración de la estancia autorizada. Basado en la verificación biométrica de datos, desplegaría el mismo sistema de correspondencias biométricas y equipo operativo que los que utilizan el SIS II y el VIS. La Comisión está llevando a cabo actualmente una evaluación de impacto y, tal como se señala en el Plan de Acción del Programa de Estocolmo, tratará de presentar una propuesta legislativa en 2011.

La tercera propuesta que debía tenerse en cuenta era la de un **programa de viajeros registrados** (*Registered Travellers Programme* - RTP)[77]. Este programa permitiría a determinados grupos de viajeros frecuentes de terceros países entrar en la UE, sujetos a un examen previo apropiado, usando controles fronterizos simplificados en barreras automáticas. El RTP se basaría también en la verificación de la identidad utilizando datos biométricos y permitiría irse desplazando gradualmente del actual enfoque de un control genérico de fronteras hacia otro basado en el riesgo individual. La Comisión ha realizado una evaluación de impacto y, de acuerdo con el Plan de Acción del Programa de Estocolmo, espera presentar una propuesta legislativa en 2011.

Iniciativas que debe estudiar la Comisión

---

74 Programa de Estocolmo – Una Europa abierta y segura que sirva y proteja al ciudadano, Documento 5731/10 del Consejo de 3.3.2010; COM(2010)171 de 20.4.2010 (Plan de Acción del Programa de Estocolmo).

75 COM(2007)654 de 6.11.2007.

76 COM(2008)69 de 13.2.2008.

77 COM(2008)69 de 13.2.2008.

En el Programa de Estocolmo, el Consejo Europeo solicitó a la Comisión que estudiara tres iniciativas relacionadas directamente con la presente Comunicación: las posibilidades de rastrear la financiación del terrorismo en la UE; la posibilidad y utilidad de desarrollar un sistema europeo de autorización de viaje; y la necesidad de crear un Sistema Europeo de Fichero Policial y su valor añadido. La Comisión ha incorporado estas iniciativas a su Plan de Acción del Programa de Estocolmo. Ahora evaluará su viabilidad y decidirá si se sigue adelante con ellos y de qué forma sobre la base de los principios de desarrollo de las políticas que se contemplan en la sección 4.

El Acuerdo TFTP UE-EE.UU. insta a la Comisión Europea a estudiar la posible introducción de un **programa de seguimiento de la financiación del terrorismo de la UE** equivalente al TFTP de los EE.UU., que permita una transferencia de datos «más específica» de la UE a los EE.UU. El proyecto de Decisión de Consejo sobre la celebración de este acuerdo invita también a la Comisión a presentar al Parlamento Europeo y al Consejo, a más tardar un año después de la entrada en vigor del Acuerdo TFTP UE-EE.UU., un marco jurídico y técnico para la extracción de datos en territorio de la UE[78]. En el plazo de tres años desde la entrada en vigor de este acuerdo, la Comisión deberá presentar un informe de situación sobre la evolución de un sistema equivalente en la UE. Si no se ha creado este sistema dentro de los cinco años siguientes a la entrada en vigor del acuerdo, la UE podrá decidir poner término a dicho acuerdo. El Acuerdo TFTP UE-EE.UU. obliga también a los EE.UU. a cooperar con la UE y prestarle asistencia y asesoría si la UE decidiera crear este sistema. Sin perjuicio de cualquier eventual decisión, la Comisión ha empezado a considerar la protección de datos, recursos e implicaciones prácticas de este empeño. Tal como se indicaba en el Plan de Acción del Programa de Estocolmo, la Comisión presentará en 2011 una comunicación sobre la viabilidad de la creación de un Programa de Seguimiento de la Financiación del Terrorismo de la UE (UE TFTP).

En su comunicación de 2008 sobre la gestión integrada de fronteras, la Comisión sugería la posible creación de un **sistema electrónico de autorización de viaje** (ESTA) para nacionales de terceros países no sujetos a la obligación del visado[79]. De acuerdo con este programa, se pediría a los nacionales seleccionables de terceros países que hicieran una solicitud electrónica en la que presentaran, antes de viajar, detalles biográficos, de pasaporte y de viaje. En comparación con el procedimiento del visado, el ESTA ofrecería un método más rápido y simple para verificar si una persona cumple las condiciones necesarias para la entrada. La Comisión está realizando actualmente un estudio sobre las ventajas, inconvenientes e implicaciones prácticas de introducir el ESTA. Tal como se indicaba en el Plan de Acción del Programa de Estocolmo, su objetivo es presentar en 2011 una comunicación sobre la viabilidad de crear dicho programa.

En su presidencia del Consejo de 2007, Alemania inició un debate sobre la posible creación de un **Sistema Europeo de Fichero Policial** (*European Police Records Index System* - EPRIS)[80]. El EPRIS ayudaría a los funcionarios de los servicios represivos a localizar información en la UE, en particular sobre las conexiones entre individuos sospechosos de delincuencia organizada. La Comisión presentará al Consejo en 2010 su proyecto de condiciones para su estudio de viabilidad del EPRIS. Tal como se establecía en el Plan de

---

78 Documento 11222/1/10 REV 1 del Consejo de 24.6.2010; Documento 11222/1/10 REV1 COR1 del Consejo de 24.6.2010.

79 COM(2008)69 de 13.2.2008.

80 Véase el Documento 15526/1/09 del Consejo de 2.12.2009.

Acción del Programa de Estocolmo, tratará de presentar en 2012 una comunicación sobre la viabilidad de crear dicho sistema.

3. ANÁLISIS DE LOS INSTRUMENTOS EN APLICACIÓN, EN EJECUCIÓN O EN CONSIDERACIÓN

El anterior panorama general sugiere las siguientes observaciones preliminares:

Estructura descentralizada

De los distintos instrumentos actualmente en aplicación, en ejecución o en consideración, sólo seis implican la recogida o almacenamiento de datos personales a nivel de la UE, a saber, SIS (y SIS II), VIS, EURODAC, SIA, Europol y Eurojust. Las demás medidas regulan el intercambio o transferencia transfronterizos y descentralizados a terceros países de información personal recogida a nivel nacional por las autoridades públicas o empresas privadas. La mayoría de los datos personales se recoge y almacena a nivel nacional; la UE trata de añadirle valor permitiendo, en ciertas condiciones, el intercambio de esta información con socios de la UE y terceros países. La Comisión ha presentado recientemente al Parlamento Europeo y al Consejo, una propuesta modificada de Reglamento por el que se establece una Agencia para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia[81]. La tarea de la futura Agencia de sistemas informáticos será ocuparse de la gestión operativa del SIS II, el VIS y EURODAC, y cualquier otro sistema informático del futuro del espacio de libertad, seguridad y justicia, para mantener estos sistemas en funcionamiento sobre una base permanente, garantizando así el flujo ininterrumpido de información.

Finalidad limitada

La mayoría de los instrumentos analizados tienen una finalidad unitaria: EURODAC pretende mejorar el funcionamiento del sistema de Dublín; la API, mejorar el control fronterizo; la Iniciativa sueca mejorar las investigaciones penales y las operaciones de inteligencia; el Convenio de Nápoles II ayudar a prevenir, detectar, perseguir y castigar el fraude aduanero; el SIA para ayudar a prevenir, investigar y perseguir infracciones graves de las legislaciones nacionales incrementando la efectividad de la cooperación entre las administraciones aduaneras de los Estados miembros; ECRIS, UIF y ORA racionalizar el intercambio transfronterizo de datos en ámbitos concretos; y la Decisión Prüm, la Directiva sobre conservación de datos, el TFTP y el PNR combatir el terrorismo y las formas graves de delincuencia. SIS, SIS II y VIS son las principales excepciones de este modelo: el objetivo original del VIS era facilitar el intercambio transfronterizo de datos sobre visados, pero posteriormente se amplió para prevenir y combatir el terrorismo y las formas graves de delincuencia. SIS y SIS II tienen por finalidad garantizar un elevado nivel de seguridad en el espacio de libertad, seguridad y justicia y facilitar la circulación de personas utilizando la información comunicada a través de este sistema. Con excepción de estos sistemas de información centralizados, la finalidad limitada es un factor central a la hora de diseñar las medidas de gestión de la información a nivel de la UE.

Posibles solapamientos de funciones

[81] COM(2010)93 de 19.3.2010.

La misma información personal puede recogerse a través de diferentes instrumentos, pero sólo puede usarse para una finalidad limitada con arreglo a cada instrumento concreto (con excepción del VIS, SIS y SIS II). Por ejemplo, los datos biográficos de una persona, incluidos su nombre, fecha y lugar de nacimiento y nacionalidad, pueden tratarse a través de SIS, SIS II, VIS, API, SIA, la Iniciativa sueca, la Decisión Prüm, ECRIS, UIF, ORA, Europol, Eurojust y los acuerdos PNR y TFTP. Sin embargo, estos datos sólo pueden tratarse para el control fronterizo en el caso de la API; para la prevención, investigación y persecución del fraude aduanero en el caso del SIA; para investigaciones penales y operaciones de inteligencia en el caso de la Iniciativa sueca; para la prevención del terrorismo y la delincuencia transfronteriza en el caso de la Decisión Prüm; para examinar los antecedentes penales de una persona en el caso del ECRIS; para investigar las relaciones de una persona con la delincuencia organizada y las redes terroristas en el caso de las UIF; para el seguimiento de activos en el caso de los ORA; para investigar y ayudar a perseguir delitos transfronterizos graves en el caso de Europol y Eurojust; prevenir y combatir el terrorismo y otras formas graves de delincuencia transnacional en el caso de los PNR; e identificar y perseguir a terroristas y a sus financiadores en el caso del TFTP. Los datos biométricos, tales como las impresiones dactilares y fotografías, pueden tratarse con arreglo a SIS II, VIS, EURODAC, la Iniciativa sueca, la Decisión Prüm, ECRIS, Europol y Eurojust, de nuevo para la finalidad limitada de cada medida. La Decisión Prüm es el único instrumento que permite el intercambio transfronterizo de perfiles de ADN anónimos (si bien estos datos pueden transmitirse también a Europol y Eurojust). Otras medidas tratan información personal muy especializada relevante sólo para sus objetivos: los sistemas PNR tratan los detalles de las reservas de vuelos de los pasajeros; FIDE, datos relevantes para la investigación del fraude aduanero; la Directiva sobre conservación de datos, direcciones IP e identificadores de equipos móviles; ECRIS, antecedentes penales; ORA, activos privados y detalles de empresas; las plataformas contra la delincuencia informática, delitos de internet; Europol, vínculos con redes de delincuencia; y el TFTP, datos de mensajería financiera. El intercambio transfronterizo de información y datos para investigaciones penales constituye el único ejemplo de solapamiento importante de funciones. Desde un punto de vista jurídico, la Iniciativa sueca sería suficiente para intercambiar *cualquier* tipo de información relevante para tales investigaciones (siempre que las legislaciones nacionales permitan el intercambio de esos datos personales). Desde un punto de vista operativo, sin embargo, la Decisión Prüm puede ser preferible para compartir los datos de los perfiles de ADN y de las impresiones dactilares, ya que su sistema de respuestas positivas o negativas garantiza respuestas instantáneas y su método de intercambio automatizado de datos garantiza un elevado nivel de seguridad de los datos[82]. De igual forma, puede ser más eficiente para las UIF, las ORA y las plataformas contra la delincuencia informática ponerse en contacto directamente con sus homólogos de la UE sin rellenar los formularios que exige la Iniciativa sueca para pedir información.

Derechos de acceso controlado

Los derechos de acceso a los instrumentos impulsados por la lógica de la lucha antiterrorista y la delincuencia grave tienden a limitarse a una definición más restringida de la comunidad

[82] La Decisión Prüm (Decisión 2008/615/JAI del Consejo, DO L 210 de 6.8.2008, p. 1) tiene la correspondiente decisión de aplicación (Decisión 2008/616/JAI del Consejo, DO L 210 de 6.8.2008, p. 12) pensada para garantizar medidas técnicas avanzadas que garanticen la protección y la seguridad de los datos, en particular su confidencialidad y su integridad, así como procedimientos de cifrado y autorización para acceder a los datos e incluye normas específicas que regulan la admisibilidad de las consultas.

encargada de ejercer la represión, a saber, policía, control fronterizo y autoridades aduaneras. Los derechos de acceso a las medidas a las que se aplica la lógica de Schengen se conceden por lo general a las autoridades de inmigración y, en determinadas condiciones, a la policía, el control fronterizo y las autoridades aduaneras. El flujo de información está controlado por interfaces nacionales en el caso de los SIS y VIS centralizados y a través de puntos de contacto nacionales o unidades centrales de coordinación en el caso de los instrumentos descentralizados, como la Decisión Prüm, la Iniciativa sueca, el Convenio de Nápoles II, ECRIS, TFTP, los acuerdos PNR, UIF, ORA y las plataformas contra la delincuencia informática.

Normas variables de conservación de datos

Los periodos de conservación de datos varían ampliamente según los objetivos de los distintos instrumentos. El acuerdo PNR con los EE.UU. tiene el plazo de conservación más largo, quince años, mientras que la API tiene el más breve, veinticuatro horas. Los acuerdos PNR introducen una distinción interesante entre datos en uso activo y pasivo: tras un cierto plazo, la información debe archivarse y sólo puede «desbloquearse» mediante una autorización especial. El uso canadiense de los datos PNR de la UE ofrece un buen ejemplo: la información se debe convertir en anónima al cabo de 72 horas, pero sigue estando disponible para los funcionarios autorizados 3,5 años.

Gestión efectiva de la identidad

Varias de las medidas antes analizadas, incluidos los futuros SIS II y VIS, tienen por finalidad permitir la verificación de la identidad usando datos biométricos. Se espera que la aplicación del SIS II mejore la seguridad en el espacio de libertad, seguridad y justicia ayudando, por ejemplo, a identificar aquellos individuos para los que se han emitido órdenes de detención europeas, aquellos a los que se ha denegado la entrada en el espacio de Schengen y aquellos a los que se busca por otras razones específicas de investigación (como las personas desaparecidas o los testigos en asuntos judiciales) independientemente de que dispongan de documentos de identificación o de su autenticidad. La aplicación del VIS deberá facilitar la expedición de visados y el proceso de gestión.

Seguridad de los datos a través de las soluciones de la UE

Para intercambiar información sensible a través de las fronteras europeas, los Estados miembros prefieren soluciones de la UE. Varios instrumentos de tamaño, estructura y finalidades diferentes se basan en la red de comunicación de datos s-TESTA, financiada por la Comisión, para compartir información sensible. En ellos se incluyen los sistemas centralizados SIS II, VIS y EURODAC, los instrumentos descentralizados Prüm, ECRIS y las UIF, así como Europol y Eurojust. El SIA y la FIDE utilizan la red de comunicación común, la red de sistema interfaz común o un acceso a la red seguro suministrado por la Comisión. Mientras tanto, la aplicación de la red de intercambio de información de Europol parece haberse convertido en la aplicación elegida para algunas iniciativas recientes que se basan en la transferencia segura de datos: se está debatiendo actualmente si FIU.net, las ORA y las plataformas de alerta contra la delincuencia informática deberían funcionar sobre la base de esta aplicación.

Mecanismos de revisión divergentes

Los instrumentos antes analizados incluyen toda una gama de diferentes mecanismos de revisión. En el caso de sistemas de información complejos, como SIS II, VIS y EURODAC, la Comisión debe presentar al Parlamento Europeo y al Consejo informes anuales o bianuales sobre el funcionamiento o el estado de aplicación de estos sistemas. En relación con los instrumentos de intercambio de información descentralizados, la Comisión tiene que presentar a las demás instituciones un único informe de evaluación a los pocos años de su aplicación: la Directiva sobre conservación de datos, la Iniciativa sueca y las medidas ORA deberán evaluarse en 2010; la Decisión Prüm, en 2012; y ECRIS, en 2016. Los tres acuerdos PNR establecen revisiones periódicas y *ad hoc*, y dos de ellos incluyen también cláusulas de extinción. Europol y Eurojust presentan informes anuales al Consejo, que los transmite para información al Parlamento Europeo. Estas consideraciones sugieren que la actual estructura de gestión de la información de la UE no conduce a la adopción de un mecanismo de evaluación único para todos los instrumentos. A la vista de esta diversidad, es esencial que las futuras modificaciones de los instrumentos del ámbito de gestión de la información tengan en cuenta su posible efecto sobre las demás medidas que regulan la recogida, almacenamiento o intercambio de datos personales en el espacio de libertad, seguridad y justicia.

4. PRINCIPIOS DE DESARROLLO DE LAS POLÍTICAS

La sección 2 describía varias iniciativas que la Comisión Europea ha aplicado, presentado o considerado en los últimos años. El gran número de ideas nuevas y el creciente cuerpo legislativo en el ámbito de la seguridad interior y la gestión de la inmigración hacen necesario definir un núcleo de principios que servirán como referencia para iniciar y evaluar las propuestas políticas de los próximos años. Estos principios se fundamentan en los principios generales que se establecen en los Tratados de la UE, la jurisprudencia del Tribunal de Justicia de la Unión Europea y el Tribunal Europeo de Derechos Humanos y los acuerdos interinstitucionales pertinentes entre el Parlamento Europeo, el Consejo y la Comisión Europea, y tratan de complementarlos. La Comisión propone desarrollar y aplicar nuevas iniciativas y evaluar los actuales instrumentos sobre la base de estos dos grupos de principios:

Principios sustantivos

Salvaguardar los derechos fundamentales, en particular el derecho a la intimidad y a la protección de datos

Salvaguardar los derechos fundamentales de las personas, tal como se consagra en la Carta de los Derechos Fundamentales de la Unión Europea, en particular su derecho a la intimidad y a la protección de los datos personales, será una de las principales preocupaciones de la Comisión cuando desarrolle nuevas propuestas que incluyan el tratamiento de datos personales en el ámbito de la seguridad interior o la gestión de la migración. Los artículo 7 y 8 de la Carta proclaman el derecho de toda persona al «respeto de su vida privada y familiar» y a «la protección de los datos de carácter personal que la conciernan»[83]. El artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE), que es vinculante para las actividades de los Estados miembros, las instituciones, agencias y organismos de la Unión, reafirma el derecho de toda persona a «la protección de los datos de carácter personal que le conciernan»[84]. Al desarrollar nuevos instrumentos basados en el uso de tecnología de la

[83] Carta de los derechos fundamentales de la Unión Europea, DO C 83 de 30.3.2010, p. 389.

[84] Versiones consolidadas del Tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea, DO C 83 de 30.3.2010, p. 1.

información, la Comisión tratará de seguir el enfoque conocido como «intimidad mediante el diseño». Esto supone integrar la protección de datos personales en la base tecnológica del instrumento propuesto, limitando el tratamiento de datos a lo que sea necesario para el objetivo propuesto y conceder el acceso a los datos sólo a las entidades que «necesitan saber»[85].

Necesidad

La interferencia entre una autoridad pública y el derecho a la intimidad puede ser necesaria en interés de la seguridad nacional, la seguridad pública o la prevención de delitos[86]. La jurisprudencia del Tribunal Europeo de Derechos Humanos establece tres condiciones con las cuales pueden justificarse estas restricciones: si son lícitas, si persiguen una finalidad legítima y si son necesarias en una sociedad democrática. La interferencia con el derecho a la intimidad se considera necesaria si responde a una necesidad social acuciante, si guarda proporción con el objetivo perseguido y si las razones expuestas por la autoridad pública para justificarla son pertinentes y suficientes[87]. En todas las propuestas políticas futuras, la Comisión evaluará el impacto que se espera pueda producir la iniciativa sobre el derecho de las personas a la intimidad y a la protección de los datos personales y expondrá por qué ese impacto es necesario y por qué la solución propuesta guarda proporción con el fin legítimo de mantener la seguridad interior de la Unión Europea, prevenir los delitos o gestionar la migración. Una autoridad independiente a nivel nacional o de la UE controlará en todos los casos que se cumplen las normas sobre protección de datos personales.

Subsidiariedad

La Comisión tratará de justificar sus nuevas propuestas teniendo en cuenta los principios de subsidiariedad y proporcionalidad, de acuerdo con el artículo 5 del Protocolo nº 2 anejo al Tratado de la Unión Europea. Las nuevas propuestas legislativas incluirán una declaración que haga posible evaluar el cumplimiento del principio de subsidiariedad, tal como se establece en el artículo 5 del Tratado de la Unión Europea. Esta declaración incluirá una evaluación del impacto financiero, económico y social de la propuesta y, en el caso de una directiva, de sus implicaciones para las normas que deberán establecer los Estados miembros[88]. Las razones por las que se llega a la conclusión de que un objetivo de la UE puede alcanzarse mejor a nivel de la UE se sustentarán mediante indicadores cualitativos. Las propuestas legislativas tendrán debidamente en cuenta la necesidad de que cualquier carga, que recaiga sobre la UE, los Gobiernos nacionales, las autoridades regionales, los agentes económicos y los ciudadanos sea lo más reducida posible y proporcional al objetivo que se desea alcanzar. En el caso de propuestas que requieran nuevos acuerdos internacionales, esta declaración considerará el impacto que se espera pueda producir la propuesta sobre las relaciones con los terceros países de que se trate.

---

85 Para una amplia descripción de la «intimidad mediante el diseño» véase *Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy*, Supervisor Europeo de Protección de Datos, 18.3.2010.

86 Véase el artículo 8 del Convenio para la protección de los derechos humanos y de las libertades fundamentales (STE nº 5), Consejo de Europa, 4.11.1950.

87 Véase *Marper / Reino Unido*, sentencia del Tribunal de Justicia de la Unión Europea, Estrasburgo, 4.12.2008.

88 Los principios básicos de las evaluaciones de impacto se establecen en las Directrices para la evaluación de impacto de la Comisión Europea (SEC(2009)92, 15.1.2009).

Gestión precisa del riesgo

La información en el espacio de libertad, seguridad y justicia se intercambia habitualmente para analizar las amenazas a la seguridad, determinar la evolución de la actividad delictiva o evaluar riesgos en los ámbitos políticos relacionados[89]. El riesgo está vinculado a menudo, pero no siempre, a individuos cuyo anterior comportamiento o pautas de comportamiento indican que ese riesgo puede seguir existiendo en el futuro. Sin embargo, el riesgo debe basarse en pruebas y no en hipótesis. Las pruebas de necesidad y la limitación de las finalidades son esenciales en cualquier medida de gestión de la información. Es pertinente desarrollar perfiles de riesgo, que no deben confundirse con perfiles raciales u otros perfiles discriminatorios, que son incompatibles con los derechos fundamentales. Estos perfiles pueden ayudar a centrar los recursos en individuos concretos para identificar las amenazas a la seguridad y proteger a las víctimas de los delitos.

Principios orientados hacia el proceso[90]

Rentabilidad

Los servicios públicos basados en la tecnología de la información deberían permitir que se prestaran mejores servicios y de un mayor valor para los contribuyentes. Teniendo en cuenta el actual clima económico, todas las nuevas propuestas, en especial cuando se refieren a la creación o actualización de sistemas de información, deberá tender a ser lo más rentable posible. Este tipo de planteamiento tendrá en cuenta las soluciones ya existentes para minimizar el solapamiento y aprovechar al máximo las posibles sinergias. La Comisión evaluará si puede ser posible cumplir los objetivos de la propuesta utilizando mejor los instrumentos existentes. También tendrá en cuenta la posibilidad de añadir funciones auxiliares a los sistemas de información existentes antes de proponer nuevos sistemas.

Diseño de la política desde la base

El desarrollo de nuevas iniciativas debe basarse, lo más temprano posible, en las aportaciones de todos los interesados de relevancia, incluidas las autoridades nacionales responsables de la aplicación, los agentes económicos y la sociedad civil. Diseñar unas políticas que tengan en cuenta los intereses de los usuarios finales exige unos enfoques horizontales y amplias consultas[91]. Por esta razón, la Comisión tratará de establecer enlaces permanentes con funcionarios y profesionales nacionales a través de las estructuras del Consejo, comités de gestión y formaciones *ad hoc*.

Asignación clara de responsabilidades

A la vista de la complejidad técnica de los proyectos de recogida e intercambio de información en el espacio de libertad, seguridad y justicia, debe prestarse especial atención al diseño inicial de las estructuras de gobernanza. La experiencia del proyecto SIS II demuestra

---

89 Ejemplos prácticos de riesgos gestionados con éxito incluyen impedir a una persona expulsada que había cometido un delito grave en un Estado miembro volver a entrar en el espacio de Schengen a través de otro Estado miembro (SIS) o impedir que una persona solicitara asilo en varios Estados miembros (EURODAC).

90 Estos principios se inspiran en las Conclusiones del Consejo sobre una estrategia de gestión de la información en el área de la seguridad interior de la UE, Consejo de de Justicia e Interior, 30.11.2009.

91 Los principios generales y las normas mínimas de las consultas públicas se fijan en COM(2002)704, 11.12.2002.

que si no se definen unos objetivos, papeles y responsabilidades generales claros y estables en una fase temprana, pueden producirse importantes rebasamientos de costes y retrasos en la aplicación. Una evaluación temprana de la experiencia en la aplicación de la Decisión Prüm sugiere que una estructura de gobernanza descentralizada no tiene por qué ser una panacea, ya que los Estados miembros no disponen de jefe de proyecto a que dirigirse para que asesore sobre los aspectos financieros o técnicos de la ejecución. La futura Agencia de sistemas informáticos podría prestar esta asesoría técnica a los custodios de los sistemas de información en el espacio de libertad, seguridad y justicia. También puede ofrecer una plataforma para una amplia participación de los interesados en la gestión y el desarrollo operativos de sistemas informáticos. Como posible salvaguardia frente a los rebasamientos de costes y plazos resultado de los cambios en los requisitos, no se desarrollará ningún sistema nuevo de información en el espacio de libertad, seguridad y justicia, especialmente si incluye algún sistema informático de gran volumen, antes de que se hayan adoptado definitivamente los instrumentos jurídicos de base que establezcan sus finalidades, alcance, funciones y detalles técnicos.

Cláusulas de revisión y extinción

La Comisión evaluará todos los instrumentos incluidos en esta comunicación. Ello se hará en relación con la amplia gama de instrumentos que existen en el ámbito de la gestión de la información. Se debería obtener así una imagen fiable de cómo encaja cada uno de los instrumentos en el amplio panorama de la gestión de la seguridad interior y de la migración. Las futuras propuestas incluirán, cuando proceda, la obligación de elaborar un informe al año, revisiones periódicas y *ad hoc*, así como una cláusula de extinción. Los instrumentos existentes sólo se mantendrán si continúan sirviendo para el propósito legítimo que se les designó. El anexo II fija las fechas y mecanismos de revisión de todos los instrumentos contemplados en esta comunicación.

5. EL CAMINO A SEGUIR

Esta comunicación ofrece, por primera vez, un resumen claro y amplio de las medidas en vigor, en aplicación o en preparación en la UE para regular la recogida, el almacenamiento o el intercambio transfronterizo de información personal con fines de aplicación de la ley o de gestión de la migración.

Da a los ciudadanos un panorama general de la información que se recoge, almacena o intercambia sobre ellos, para qué y por quién. Es una herramienta de referencia transparente para los interesados que deseen debatir sobre la futura dirección de la política de la UE en este ámbito. Al mismo tiempo da una primera respuesta a la petición del Consejo Europeo de desarrollar unos instrumentos de gestión de la información a nivel de la UE de acuerdo con la Estrategia de gestión de la información de la UE[92] y para reflexionar sobre la necesidad de un Modelo europeo para el intercambio de información[93].

---

92 Conclusiones del Consejo sobre una estrategia de gestión de la información en el área de la seguridad interior de la UE, Consejo de Justicia e Interior, 30.11.2009 (Estrategia de gestión de la información de la UE).

93 Programa de Estocolmo – Una Europa abierta y segura que sirva y proteja al ciudadano, Documento del Consejo 5731/10, 3.3.2010, sección 4.2.2.

la Comisión desea dar continuidad a esta comunicación presentando una comunicación sobre el Modelo europeo para el intercambio de información en 2012[94]. Para ello, la Comisión inició un ejercicio de «cartografía de la información» en enero de 2010 sobre las bases jurídicas y el funcionamiento práctico del intercambio entre Estados miembros de datos e información penales, cuyos resultados tiene previsto presentar la Comisión al Consejo y al Parlamento Europeo en 2011[95].

Por último, esta comunicación presenta, por primera vez, la visión que tiene la Comisión de los amplios principios que pretende seguir en el desarrollo futuro de instrumentos para la recogida, el almacenamiento o el intercambio de datos. Estos principios se usarán también al evaluar los instrumentos existentes. Al adoptar este enfoque del desarrollo y evaluación de las políticas basado en una serie de principios, se espera mejorar la coherencia y eficacia de los instrumentos actuales y futuros de forma que se respeten completamente los derechos fundamentales de los ciudadanos.

94 Así se indica en el Plan de Acción del Programa de Estocolmo de la Comisión (COM(2010)171, 20.4.2010).

95 Este ejercicio de cartografía de la información se está realizando en estrecha cooperación con un Equipo para el proyecto de cartografía de la información compuesto por representantes de los Estados miembros de la UE y la AELC, Europol, Eurojust, Frontex y el Supervisor Europeo de Protección de Datos.

ANEXO I

Los siguientes datos y ejemplos sirven para ilustrar el funcionamiento en la práctica de las medidas de gestión de la información actualmente aplicadas

Sistema de Información de Schengen (SIS)

Número total de descripciones SIS introducidas en la base de datos central SIS (C.SIS)[96]			
Categorías de descripciones	**2007**	**2008**	**2009**
Billetes de banco	177 327	168 982	134 255
Documentos vírgenes	390 306	360 349	341 675
Armas de fuego	314 897	332 028	348 353
Documentos emitidos	17 876 227	22 216 158	25 685 572
Vehículos	3 012 856	3 618 199	3 889 098
Personas buscadas (apodos)	299 473	296 815	290 452
Personas buscadas (nombre principal)	859 300	927 318	929 546
De las cuales:			
Personas buscadas para su detención a efectos de entrega o extradición	19 119	24 560	28 666
Nacionales de terceros países en la lista de prohibición de entrada	696 419	746 994	736 868
Personas adultas desaparecidas	24 594	23 931	26 707
Menores desaparecidos	22 907	24 628	25 612
Testigos o personas sujetas a citación judicial	64 684	72 958	78 869
Personas sujetas a control excepcional para prevenir amenazas a la seguridad pública	31 568	34 149	32 571
Personas sujetas a control excepcional para prevenir amenazas a la seguridad nacional	9	98	253
Total	**22 933 370**	**27 919 849**	**31 618 951**

[96] Documento 6162/10 del Consejo de 5.2.2010; Documento del Consejo 5764/09 de 28.1.2009; Documento 5441/08 del Consejo de 30.1.2008.

EURODAC – Circulación de solicitantes de asilo que presentaron nuevas solicitudes en el mismo o en otro Estado miembro (2008)

Estados miembros que han enviado impresiones dactilares para su comparación y que han obtenido respuestas positivas de Estados miembros (columnas) en los que la persona había solicitado asilo previamente	Estado miembro en el que se presentó la primera solicitud de asilo[97]																													Total de 2ª solicitud	
	AT	BE	BG	CH	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IS	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	UK	Respuestas positivas locales	Total de respuestas positivas
AT	1 725	74	2	0	1	87	274	5	2	31	12	25	115	212	5	0	134	3	14	0	9	52	49	1 371	1	42	111	17	260	61	**1 725**	**4 694**
BE	180	5 450	4	0	3	38	408	17	0	41	17	28	378	67	28	0	69	3	37	0	2	180	73	625	6	3	192	17	58	205	**5 450**	**8 129**
BG	5	2	116	0	1	1	5	1	0	7	0	0	0	1	0	0	1	0	2	0	0	1	3	0	0	6	8	0	0	4	**116**	**164**
CH	32	52	1	4	3	5	35	0	0	17	17	8	39	19	1	0	355	0	1	0	13	15	37	3	1	0	41	4	4	25	**4**	**732**
CY	1	0	0	0	68	0	1	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	**68**	**73**
CZ	55	12	0	0	0	637	48	4	0	0	3	4	13	0	1	0	8	2	1	0	0	7	6	17	1	0	13	0	1	6	**637**	**839**
DE	260	268	12	0	4	79	1 852	42	0	174	39	56	256	106	9	2	200	5	26	2	5	174	137	149	4	43	567	30	89	128	**1 852**	**4 718**
DK	44	43	3	0	0	13	126	119	0	27	13	44	36	13	4	0	47	0	7	0	0	30	225	55	2	4	436	2	7	41	**119**	**1 341**
EE	0	0	0	0	0	0	1	1	0	0	0	8	0	0	0	0	0	0	0	0	0	0	1	0	0	0	3	0	0	9	**0**	**23**
EL	66	88	27	0	12	9	131	10	0	766	8	8	35	3	9	0	48	0	1	0	0	33	24	3	0	13	141	0	8	316	**766**	**1 759**
ES	16	18	2	0	1	3	37	1	0	11	108	0	29	4	5	0	35	0	0	0	0	9	9	4	6	0	21	5	1	16	**108**	**341**
FI	37	44	1	0	1	10	115	25	0	48	5	229	14	30	10	1	194	0	3	0	90	49	107	44	2	4	362	3	3	81	**229**	**1 512**
FR	365	339	0	0	8	97	502	29	0	92	78	31	860	161	8	0	336	11	26	1	29	106	74	1 739	8	9	286	37	75	190	**860**	**5 497**
HU	297	53	4	0	1	3	169	4	0	2	3	19	70	791	1	0	27	1	10	0	0	28	32	0	0	76	79	19	14	14	**791**	**1 717**
IE	20	21	0	0	4	2	24	1	0	9	8	0	23	4	309	0	35	0	4	0	4	16	7	0	0	0	22	2	2	187	**309**	**704**
IS	4	3	0	0	0	0	3	0	0	3	1	1	6	2	1	0	3	0	1	0	1	3	10	1	0	0	11	1	0	3	**0**	**58**
IT	390	111	5	0	6	33	349	11	0	270	47	27	192	60	23	5	3 290	0	11	0	58	78	116	9	2	6	201	59	224	680	**3 290**	**6 263**
LT	3	1	0	0	1	3	0	0	0	0	1	0	1	0	0	0	0	5	0	0	0	0	4	14	0	0	5	0	2	0	**5**	**40**
LU	7	21	4	0	0	0	12	2	0	0	0	1	9	6	0	1	8	0	2	0	1	6	4	0	0	0	10	3	1	3	**2**	**101**
LV	3	1	0	0	0	0	1	0	1	0	0	0	1	0	0	0	0	5	0	0	0	0	0	0	0	0	1	0	2	0	**0**	**15**
MT	1	0	0	0	0	0	0	0	0	0	0	5	1	0	0	0	6	0	0	0	16	0	1	0	0	0	1	1	0	0	**16**	**32**
NL	109	223	16	0	1	27	198	21	0	113	16	29	109	33	7	1	226	0	14	0	58	1 240	95	16	8	9	289	8	22	129	**1 240**	**3 017**
NO	84	103	6	0	2	13	256	76	0	199	55	57	78	23	8	0	524	8	13	1	83	86	276	164	1	9	826	10	21	96	**276**	**3 078**
PL	188	65	0	0	0	30	68	15	0	0	2	4	75	1	1	0	0	3	3	0	0	7	27	1,208	1	1	43	1	13	4	**1 208**	**1 760**
PT	1	10	0	0	0	0	4	1	0	0	11	0	9	0	0	0	2	0	2	0	0	2	2	0	3	0	2	0	1	2	**3**	**52**
RO	43	2	5	0	1	9	33	0	0	3	0	5	14	11	0	0	0	0	1	0	0	9	1	1	0	64	17	0	4	4	**64**	**227**
SE	243	133	30	0	4	36	516	173	0	143	29	143	145	80	16	3	276	0	16	0	130	98	430	147	5	13	1,914	11	26	122	**1 914**	**4 882**
SI	14	4	0	0	0	1	10	1	0	1	1	2	15	6	0	0	5	0	1	0	0	2	3	0	0	0	5	45	3	2	**45**	**121**
SK	105	4	0	0	0	7	33	0	1	0	0	1	2	12	0	0	3	0	0	1	0	4	4	4	0	0	9	2	195	6	**195**	**393**
UK	109	153	7	0	3	12	276	30	0	108	6	38	209	25	217	2	768	0	8	0	43	128	76	7	4	11	174	6	46	3 141	**3 141**	**5 607**
Total de 1ª solicitud	**4 407**	**7 298**	**245**	**4**	**125**	**1 155**	**5 487**	**589**	**4**	**2 067**	**480**	**773**	**2 734**	**1 670**	**663**	**15**	**6 600**	**46**	**204**	**5**	**542**	**2 363**	**1 833**	**5 581**	**55**	**313**	**5 791**	**283**	**1 082**	**5 475**	**24 433**	**57 889**

97 COM(2009)494 de 25.9.2009. Las «respuestas positivas locales» se refieren a la presentación de una nueva solicitud de asilo en el Estado miembro en el que se presentó la anterior.

Sistema de información previa sobre pasajeros (*Advance Passenger Information* - API)

Utilización por parte del Reino Unido de la información previa sobre pasajeros para mejorar el control fronterizo y combatir la migración irregular[98]	
Número de acciones emprendidas en 2009	
Historial negativo previo (persona a la que se denegó la entrada)	379
Pasaportes perdidos, robados o cancelados (documento incautado)	56

[98] La Agencia de fronteras del Reino Unido suministró esta información a la Comisión a efectos de esta comunicación.

Sistema de Información Aduanero (SIA)

Número total de casos introducidos en la base de datos SIA (2009)[99]	
Acción	**SIA (basado en el Convenio SIA)**
Casos creados	2 007
Casos activos	274
Casos consultados	11 920
Casos suprimidos	1 355

[99] Información proporcionada por la Comisión.

Iniciativa sueca

Ejemplos del uso de la Iniciativa sueca para investigar delitos[100]	
Homicidio	En 2009 hubo un intento de homicidio en la capital de un Estado miembro. La policía recogió una muestra biológica de un vaso del que había bebido el sospechoso. Tras extraer ADN de esta muestra, los expertos forenses generaron un perfil ADN. La comparación de este perfil con otros perfiles de referencia de la base nacional de datos ADN no dio resultados positivos. Por ello, la fuerza policial que investigaba el caso envió, a través de su punto de contacto Prüm, una solicitud para compararlo con perfiles ADN de referencia de otros Estados miembros a los que se había autorizado a intercambiar esos datos sobre la base de la Decisión Prüm o el Acuerdo Prüm. Esta comparación transfronteriza dio una respuesta positiva. Sobre la base de la Iniciativa sueca, la fuerza policial que investigaba el caso solicitó más datos del sospechoso. Su punto de contacto nacional recibió respuestas de otros Estados miembros en 36 horas, lo que permitió a la policía identificar al sospechoso.
Violación	En 2003 una persona sin identificar violó a una mujer. La policía recogió muestras de la víctima, pero el perfil ADN generado a partir de la muestra no coincidía con ninguno de los perfiles de referencia de la base nacional de datos ADN. Una solicitud de comparación de ADN, enviada por el punto de contacto Prüm a otros Estados miembros a los que se había autorizado a intercambiar perfiles ADN de referencia sobre la base de la Decisión Prüm o el Acuerdo Prüm, tuvo una respuesta positiva. La fuerza policial que investigaba el caso solicitó entonces más información sobre el sospechoso con arreglo a la Iniciativa sueca. Su punto de contacto nacional recibió una respuesta en 8 horas, lo que permitió a la policía identificar al sospechoso.

[100] Las fuerzas de policía de un Estado miembro proporcionaron estos ejemplos a la Comisión a efectos de esta comunicación.

Respuestas positivas obtenidas por Alemania en la comparación transfronteriza de perfiles DNA, según el tipo de delito (2009)[101]

Respuestas positivas por tipo de delito	**Austria**	**España**	**Luxemburgo**	**Países Bajos**	**Eslovenia**
Delitos contra intereses públicos	32	4	0	5	2
Delitos contra la libertad de las personas	9	3	5	2	0
Delitos sexuales	40	22	0	31	4
Delitos contra las personas	49	24	0	15	2
Otros delitos	3 005	712	18	1 105	71

[101] Respuesta del Gobierno alemán a una pregunta parlamentaria de Ulla Jelpke, Inge Höger y Jan Korte (nº de referencia 16/14120), *Bundestag*, nº de referencia 16/14150, 22.10.2009. Estas cifras se refieren al periodo que empieza con la fecha en que un Estado miembro inició el intercambio de datos con Alemania y finaliza el 30 de septiembre de 2009.

Ejemplos en los que los Estados miembros han detectado casos de delitos graves a través de la conservación de datos[102]	
Asesinato	La policía de un Estado miembro logró seguir la pista a un grupo de asesinos responsable de la muerte de seis personas por motivos raciales. Los autores trataron de escapar a su captura cambiando sus tarjetas SIM, pero las listas de llamadas y los identificadores de los equipos móviles los delataron.
Homicidio	Una autoridad policial pudo probar la participación de dos sospechosos en un caso de homicidio analizando los datos de tráfico del teléfono móvil de la víctima. Esto permitió a los detectives reconstruir la ruta por la que la víctima y los dos sospechosos habían viajado juntos.
Robo	Las autoridades rastrearon a un delincuente responsable de diecisiete robos estudiando los datos del tráfico de su tarjeta SIM prepago anónima. Al identificar a su novia, pudieron localizar también al delincuente.
Fraude	Los investigadores desenredaron una trama en la que una banda anunciaba la venta de coches de lujo en internet mediante pago en metálico y robaban sistemáticamente a los que se presentaban para hacerse cargo de sus vehículos. Una dirección IP permitió a la policía seguir la pista al abonado y detener a los delincuentes.

[102] Estos ejemplos anónimos se basan en las respuestas de los Estados miembros a un cuestionario de la Comisión de 2009 respecto a la incorporación de la Directiva 2006/24/CE (Directiva sobre conservación de datos).

Cooperación Unidad de Información Financiera (UIF, *Financial Intelligence Unit* - FIU)

Número total de solicitudes de información efectuadas por las UIF nacionales a través de FIU.net[103]

Año	Solicitudes de información	Usuarios activos
2007	3 133	12 Estados miembros
2008	3 084	13 Estados miembros
2009	3 520	18 Estados miembros

[103] La oficina FIU.net suministró esta información a la Comisión a efectos de esta comunicación.

Cooperación Organismo de recuperación de activos (ORA, *Asset Recovery Office* - ARO)

Solicitudes de seguimiento de activos presentadas por los Estados miembros y tramitadas por Europol[104]

Año	**2004**	**2005**	**2006**	**2007**
Solicitudes	5	57	53	133
De las cuales:				
Asuntos relacionados con fraude				29
Asuntos relacionados con blanqueo de capitales				26
Asuntos relacionados con drogas				25
Asuntos relacionados con otros delitos				18
Asuntos relacionados con drogas y blanqueo de capitales				19
Asuntos relacionados con fraude y blanqueo de capitales				7
Asuntos relacionados con combinaciones de delitos				9

[104] Evaluación de la eficacia de las prácticas de los Estados miembros de la UE en la identificación, seguimiento, embargo y decomiso de bienes de origen delictivo - Informe final (para la Comisión Europea, DG JLS), Matrix Insight, 6.2009.

Asuntos de decomiso de bienes tramitados por Eurojust (2006-2007)[105]			
Tipos de asuntos		**Asuntos iniciados por**	
Asuntos relacionados con delitos medioambientales	1	Alemania	27%
Asuntos relacionados con la participación en una organización delictiva	5	Países Bajos	21%
Asuntos relacionados con el tráfico de drogas	15	Reino Unido	15%
Asuntos relacionados con fraude fiscal	8	Finlandia	13%
Asuntos relacionados con fraude	8	Francia	8%
Asuntos relacionados con fraude en el IVA	1	España	6%
Asuntos relacionados con blanqueo de capitales	9	Portugal	4%
Asuntos relacionados con corrupción	1	Suecia	2%
Asuntos relacionados con delitos contra la propiedad	2	Dinamarca	2%
Asuntos relacionados con tráfico de armas	1	Letonia	2%
Asuntos relacionados con la falsificación y la piratería de productos	2		
Asuntos relacionados con fraude en pagos anticipados	2		
Asuntos relacionados con falsificaciones de documentos administrativos	1		
Asuntos relacionados con delitos de tráfico de vehículos	1		
Asuntos relacionados con terrorismo	1		
Asuntos relacionados con imitaciones y falsificaciones	2		
Asuntos relacionados con el tráfico de seres humanos	1		

[105] Ibídem.

Plataformas de alerta contra la delincuencia informática

Ejemplos de la Plataforma francesa de alerta contra la delincuencia informática, Pharos, en la investigación de asuntos de delincuencia informática[106]	
Pornografía infantil	Un usuario de internet alertó a Pharos de la existencia de un blog que contenía fotos e imágenes tipo dibujos animados de abusos sexuales con niños. El editor del blog, que aparecía desnudo en una foto, también lo usaba para entablar amistad con niños con fines deshonestos. Los investigadores identificaron como principal sospechoso a un profesor particular de matemáticas. Un registro en su domicilio descubrió 49 videos con imágenes de pornografía infantil. La investigación reveló también que había hecho los preparativos para poner en marcha un curso de clases particulares. El acusado fue declarado culpable y sentenciado a pena de cárcel con suspensión de condena.
Abuso sexual infantil	La policía francesa recibió informaciones sobre un individuo que ofrecía dinero por internet a cambio de relaciones sexuales con niños. Un detective de Pharos, haciéndose pasar por un menor, estableció contacto con el sospechoso, que le ofreció dinero a cambio de relaciones sexuales. El posterior chat en internet permitió a Pharos identificar la dirección Protocolo de Internet del sospechoso y seguir su pista hasta una población conocida por su elevado número de casos de abuso sexual infantil. El acusado fue declarado culpable y sentenciado a pena de reclusión con suspensión de condena.

[106] Pharos corresponde a *plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements*.

Europol

Ejemplos de la contribución de Europol a la lucha contra las formas graves de delincuencia transfronteriza[107]	
Operación Andromeda	En diciembre de 2009, Europol ayudó a ejecutar una amplia operación policial transfronteriza contra una red de tráfico de drogas con contactos en 42 países. Esta red tenía sus bases en Bélgica y Noruega y traía la droga desde Perú, a través de los Países Bajos, a Bélgica, el Reino Unido, Italia y otros Estados miembros. La cooperación policial estuvo coordinada por Europol; la judicial, por Eurojust. Las autoridades participantes instalaron una oficina móvil en Pisa; Europol, una sala de operaciones en La Haya. Europol elaboró las referencias cruzadas de la información entre sospechosos y redactó un informe que describía la red criminal.
Participantes	Italia, Países Bajos, Alemania, Bélgica, Reino Unido, Lituania, Noruega y Eurojust.
Resultados	Las fuerzas de policía participantes intervinieron 49 kg de cocaína, 10 kg de heroína, 6 000 pastillas de éxtasis, dos armas de fuego, cinco documentos de identidad falsos y 43 000 euros en metálico, y detuvieron a 15 personas.
Operación Typhon	Entre abril de 2008 y febrero de 2010, Europol prestó apoyo analítico a las fuerzas policiales de 20 países que participaban en el Operativo Typhon. En esta amplia operación contra una red de pedofilia que distribuía imágenes de pornografía infantil a través de un sitio web austríaco, Europol elaboró un análisis de apoyo técnico e inteligencia penal sobre la base de las imágenes recibidas de Austria. A continuación evaluó la fiabilidad de los datos y los reestructuró antes de preparar su propio material de inteligencia. Cruzando los datos con la información contenida en su fichero de trabajo de análisis, elaboró 30 informes de inteligencia que impulsaron investigaciones en varios países.
Participantes	Alemania, Austria, Bélgica, Bulgaria, Canadá, Dinamarca, Eslovaquia, Eslovenia, España, Francia, Hungría, Italia, Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Reino Unido, Rumanía y Suiza.
Resultados	Las fuerzas participantes identificaron a 286 sospechosos, detuvieron a 118 sospechosos y rescataron a cinco víctimas que habían sufrido abusos en este caso en cuatro países.

[107] Europol suministró esta información a la Comisión a efectos de esta comunicación. Se puede obtener más información sobre la Operación Andrómeda en http://www.eurojust.europa.eu/.

Eurojust

Ejemplos de Eurojust como coordinador de amplias operaciones judiciales transfronterizas contra las formas graves de delincuencia[108]	
Trata de seres humanos y financiación del terrorismo	En mayo de 2010, Eurojust coordinó una operación transfronteriza que tuvo como resultado la detención de cinco miembros de una red de delincuencia organizada activa en Afganistán, Pakistán, Rumanía, Albania e Italia. El grupo dotaba a nacionales afganos y pakistaníes de documentación falsa y los llevaba a Italia a través de Irán, Turquía y Grecia. Una vez en Italia, se despachaba a los migrantes a Alemania, Suecia, Bélgica, Reino Unido y Noruega. Las ganancias generadas por este tráfico se destinaban a financiar el terrorismo.
Fraude con tarjetas bancarias	Coordinando la cooperación policial y judicial transfronterizas, Europol y Eurojust ayudaron a desarticular una red de fraude con tarjetas bancarias activa en Irlanda, Italia, Países Bajos, Bélgica y Rumanía. Esta red robó los datos de identificación de unas 15 000 tarjetas de pago, provocando una pérdida de 6,5 millones de euros. Antes de esta operación, que provocó 24 detenciones en julio de 2009, magistrados belgas, irlandeses, italianos, holandeses y rumanos facilitaron la emisión de órdenes de detención europeas y peticiones para practicar escuchas telefónicas a los sospechosos.
Trata de seres humanos y tráfico de drogas	Tras una reunión de coordinación organizada por Eurojust en marzo de 2009, las autoridades italianas, holandesas y colombianas detuvieron a 62 individuos sospechosos de trata de seres humanos y tráfico de drogas. Esta red traficaba con mujeres vulnerables trayéndolas de Nigeria a los Países Bajos, forzándolas a prostituirse en Italia, Francia y España. Las ganancias de la prostitución financiaban la compra por parte de la red de cocaína en Colombia y su envío a la UE para el consumo.

[108] Estos ejemplos proceden de http://www.eurojust.europa.eu/.

Ejemplos de análisis de los PNR para obtener información que permita investigar formas graves de delincuencia transfronteriza[109]	
Tráfico de menores	El análisis de los PNR reveló que tres niños viajaban solos de un Estado miembro de la UE a un tercer país, sin indicaciones de las persona que debía recogerlos a su llegada. Alertadas por la policía del Estado miembro tras su partida, las autoridades del tercer país detuvieron a la persona que iba a recibir a los niños: un delincuente sexual fichado en el Estado miembro.
Trata de seres humanos	El análisis de los PNR puso de manifiesto la existencia de un grupo de traficantes de seres humanos que hacía siempre la misma ruta. Utilizaban documentos falsos para facturar en un vuelo interior de la UE y al mismo tiempo usaban los documentos auténticos para facturar en otro vuelo destinado a un tercer país. Una vez en la sala de espera del aeropuerto, embarcarían en el vuelo interior .
Fraude con tarjetas de crédito	Varias familias viajaron a un Estado miembro con billetes comprados mediante tarjetas de crédito robadas. Las investigaciones mostraron que un grupo de delincuentes utilizaba estas tarjetas para comprar los billetes, vendiéndolos de mano a mano en centros de llamadas a larga distancia. Los datos PNR vincularon a los viajeros con las tarjetas de crédito y los vendedores.
Tráfico de drogas	La autoridad policial de un Estado miembro disponía de información que sugería que un hombre estaba implicado en tráfico de drogas desde un tercer país, pero los guardias fronterizos nunca le hallaron nada a su llegada a la UE. El análisis de los PNR reveló que siempre viajaba acompañado. Una inspección de la persona que viajaba con él permitió descubrir grandes cantidades de droga.

[109] Estos ejemplos son anónimos para proteger las fuentes de información.

Programa de seguimiento de la financiación del terrorismo (*Terrorist Finance Tracking Program* - TFTP)

Ejemplos en los que el TFTP obtiene información para investigar tramas terroristas[110]	
Trama terrorista de Barcelona 2008	En enero de 2008, se detuvo a diez sospechosos en Barcelona en conexión con un intento frustrado de llevar a cabo un ataque en el sistema de transporte público de la ciudad. Los datos TFTP se usaron para identificar los vínculos de los sospechosos con Asia, África y Norteamérica.
Trama de la bomba líquida transatlántica de 2006	La información del TFTP se utilizó para investigar y condenar a una serie de individuos en relación con un intento frustrado de hacer explotar en agosto de 2006 diez vuelos transatlánticos con destino a los EE.UU. y Canadá procedentes del Reino Unido.
Bombas de Londres 2005	Los datos del TFTP se utilizaron para que los investigadores dispusieran de nuevas pistas, corroborar las identidades de los sospechosos y revelar las relaciones entre los individuos responsables de este ataque.
Bombas de Madrid 2004	Los datos TFTP se entregaron a varios Estado miembros para ayudarles en las investigaciones que iniciaron a raíz de este ataque.

110 Segundo informe sobre el 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, Juez Jean-Louis Bruguière, enero de 2010.

ANEXO II

Panorama general en forma de cuadro de los instrumentos en aplicación, en ejecución o en consideración

Instrumento	Antecedentes	Finalidad(es)	Estructura	Cobertura de datos personales	Acceso a los datos	Protección de datos	Conservación de datos	Estado de ejecución	Revisión
Sistema de Información de Schengen (SIS)	Iniciado por los Estados miembros	Mantener la seguridad pública, incluida la seguridad nacional, dentro del espacio de Schengen y facilitar la circulación de personas utilizando la información comunicada a través de este sistema.	Centralizada: N.SIS (partes nacionales) conectadas por interfaz a C.SIS (parte central).	Nombres y apodos, características físicas, lugar y fecha de nacimiento, nacionalidad y si la persona va armada y es violenta. Las descripciones SIS se refieren a varios grupos diferentes de personas.	La policía, la policía fronteriza, las aduanas y las autoridades judiciales tienen acceso a todos los datos; las autoridades de inmigración y consulares a la lista de prohibición de entrada y a los documentos perdidos y robados. Europol y Eurojust pueden acceder a algunos datos.	Convenio 108 del Consejo de Europa (CdE) y Recomendación policial R (87) 15 CdE.	Los datos personales introducidos en el SIS a efectos de la búsqueda de personas sólo podrán conservarse el tiempo necesario para cumplir los fines para los que se suministraron y no más de tres años. Los datos sobre personas sujetas a vigilancia especial debido a la amenaza que pueden suponer para la seguridad pública o nacional deberán borrarse al cabo de un año.	El SIS es plenamente aplicable en 22 Estados miembros, así como en Suiza, Noruega e Islandia. El Reino Unido e Irlanda participan en SIS II con excepción de las descripciones relativas a nacionales de terceros países incluidos en la lista de prohibición de entrada. Se espera que Bulgaria, Rumanía y Liechtenstein apliquen esta medida pronto.	Los signatarios pueden proponer modificaciones al Convenio de Schengen. El texto modificado deberá ser adoptado por unanimidad y ratificado por los parlamentos.

Panorama general en forma de cuadro de los instrumentos en aplicación, en ejecución o en consideración

Instrumento	Antecedentes	Finalidad(es)	Estructura	Cobertura de datos personales	Acceso a los datos	Protección de datos	Conservación de datos	Estado de ejecución	Revisión
Sistema de Información de Schengen (II) (SIS II)	Iniciado por la Comisión.	Garantizar un elevado nivel de seguridad en el espacio de libertad, seguridad y justicia y facilitar la circulación de personas utilizando la información comunicada a través de este sistema.	Centralizada: N.SIS II (partes nacionales) conectadas por interfaz a CS-SIS (parte central). SIS II funcionará con la red segura s-TESTA.	Las categorías de datos de SIS más impresiones dactilares y fotografías, copias de la orden de detención europea, descripciones de identidades usurpadas y vínculos entre descripciones. Las descripciones SIS II se refieren a varios grupos diferentes de personas.	La policía, la policía fronteriza, las aduanas y las autoridades judiciales tendrán acceso a todos los datos; las autoridades de inmigración y consulares a la lista de prohibición de entrada y a los documentos perdidos y robados. Europol y Eurojust podrán acceder a algunos datos.	Normas específicas establecidas con arreglo a los actos jurídicos de base que rigen SIS II y la Directiva 95/46/CE, el Reglamento (CE) 45/2001, la Decisión marco 2009/977/JAI del Consejo, el Reglamento (CE) 45/2011, el Convenio 108 CdE y la Recomendación policial R (87) 15 CdE	Los datos personales introducidos en el SIS a efectos de la búsqueda de personas sólo podrán conservarse el tiempo necesario para cumplir los fines para los que se suministraron y no más de tres años. Los datos sobre personas sujetas a vigilancia especial debido a la amenaza que pueden suponer para la seguridad pública o nacional deberán borrarse al cabo de un año.	El SIS II se encuentra en fase de ejecución. Una vez sea operativo, el sistema se aplicará a la UE-27, Suiza, Liechtenstein, Noruega e Islandia. El Reino Unido e Irlanda participarán en SIS II con excepción de las descripciones relativas a nacionales de terceros países incluidos en la lista de prohibición de entrada.	La Comisión debe enviar informes de situación bianuales al Parlamento Europeo (PE) y al Consejo sobre la evolución de SIS II y la potencial migración desde SIS.

Panorama general en forma de cuadro de los instrumentos en aplicación, en ejecución o en consideración

Instrumento	Antecedentes	Finalidad(es)	Estructura	Cobertura de datos personales	Acceso a los datos	Protección de datos	Conservación de datos	Estado de ejecución	Revisión
EURODAC	Iniciado por la Comisión.	Ayudar a establecer qué Estado miembro debe evaluar una solicitud de asilo.	Centralizada, consiste en puntos nacionales de acceso conectados por un interfaz a la unidad central de EURODAC. Funciona a través de la red s-TESTA.	Datos de las impresiones dactilares, sexo, lugar y fecha de la solicitud de asilo, número de referencia usado por el Estado miembro de origen y fecha en que se tomaron, transmitieron e introdujeron en el sistema las impresiones dactilares.	Los Estados miembros deberán especificar la lista de autoridades con acceso a los datos, que normalmente incluye a las autoridades de asilo y migración, guardias de fronteras y policía.	Directiva 95/46/CE.	10 años las impresiones dactilares de los solicitantes de asilo; 2 años las de los nacionales de terceros países interceptados con ocasión del cruce irregular de una frontera exterior.	El Reglamento EURODAC está en vigor en todos los Estados miembros, Noruega, Islandia y Suiza. El acuerdo que permitirá la conexión de Liechtenstein está esperando su celebración.	La Comisión debe enviar un informe anual al PE y al Consejo sobre el funcionamiento de la unidad central de EURODAC.
Sistema de información de visados (*Visa Information System* - VIS)	Iniciado por la Comisión.	Ayudar a aplicar una política de visados común y prevenir amenazas a la seguridad interior.	Centralizada, compuesta por partes nacionales que estarán conectadas por una interfaz a la parte central. VIS funcionará a través de la red s-TESTA.	Solicitudes de visado, impresiones dactilares, fotografías, decisiones de visado relacionadas y enlaces entre solicitudes relacionadas.	Las autoridades de visado, asilo y control fronterizo tendrán acceso a todos los datos. La policía y Europol podrán consultar VIS para prevenir, detectar e investigar delitos graves.	Normas específicas establecidas por los actos jurídicos de base que rigen VIS y la Directiva 95/46/CE, el Reglamento (CE) 45/2001, la Decisión marco 2009/977/JAI del Consejo, el Convenio 108 CdE, el Protocolo adicional 181 CdE y la Recomendación policial R (87) 15 CdE.	Cinco años.	El VIS está en fase de ejecución y se aplicará en todos los Estados miembros (excepto en el Reino Unido e Irlanda), y en Noruega, Islandia y Suiza.	La Comisión deberá informar al PE y al Consejo sobre el funcionamiento del VIS a los tres años de su puesta en marcha y posteriormente cada cuatro años.

Panorama general en forma de cuadro de los instrumentos en aplicación, en ejecución o en consideración

Instrumento	Antecedentes	Finalidad(es)	Estructura	Cobertura de datos personales	Acceso a los datos	Protección de datos	Conservación de datos	Estado de ejecución	Revisión
Sistema de información previa sobre pasajeros (*Advance Passenger Information* - API)	Iniciado por España.	Mejorar el control fronterizo y combatir la migración irregular.	Descentralizada.	Datos personales de pasaportes, punto de embarque y punto de entrada en la UE.	Autoridades de control fronterizo y, a petición, autoridades de los servicios represivos.	Directiva 95/46/CE.	Los datos deben borrarse a las 24 horas de la llegada del vuelo a la UE.	API está en vigor en todos los Estados miembros, pero pocos lo usan.	La Comisión evaluará el sistema API en 2011.
Convenio de Nápoles II	Iniciado por los Estados miembros	Ayudar a las aduanas nacionales a prevenir y detectar las infracciones de las disposiciones aduaneras nacionales y ayudarles a perseguir y castigar las infracciones de las disposiciones aduaneras comunitarias y nacionales.	Descentralizada, funciona a través de un conjunto de unidades centrales de coordinación.	Toda la información relacionada con una persona identificada o identificable.	Las unidades centrales de coordinación transmiten los datos a las autoridades aduaneras nacionales, autoridades encargadas de las investigaciones y organismos judiciales y, previo consentimiento del Estado miembro que haya suministrado los datos, a otras autoridades.	Directiva 95/46/CE y Convenio 108 CdE. Los datos disfrutarán en el Estado miembro que los haya recibido de un nivel de protección como mínimo equivalente al del Estado miembro que los haya suministrado.	Los datos pueden conservarse por un periodo no superior al necesario para los fines para los que se entregaron.	Todos los Estados miembros han ratificado este Convenio.	Los signatarios pueden proponer modificaciones al Convenio de Nápoles II. El texto modificado deberá ser adoptado por el Consejo y ratificado por los Estados miembros.

Panorama general en forma de cuadro de los instrumentos en aplicación, en ejecución o en consideración

Instrumento	Antecedentes	Finalidad(es)	Estructura	Cobertura de datos personales	Acceso a los datos	Protección de datos	Conservación de datos	Estado de ejecución	Revisión
Sistema de Información Aduanero (SIA)	Iniciado por los Estados miembros	Ayudar a las autoridades competentes a prevenir, investigar y perseguir infracciones graves de las leyes aduaneras nacionales.	Centralizada, accesible a través de terminales en los Estados miembros y en la Comisión. El SIA y la FIDE funcionan sobre la base de AFIS, que utiliza la red de comunicación común, la red de sistema interfaz común o un acceso a la red seguro suministrado por la Comisión.	Nombres y apodos, fecha y lugar de nacimiento, nacionalidad, sexo, características físicas, documentos de identidad, dirección, antecedentes de violencia, razón para introducir los datos en el SIA, actuación sugerida y registros de matriculación de los medios de transporte.	Pueden acceder a los datos del SIA las autoridades aduaneras nacionales, Europol y Eurojust.	Normas específicas establecidas por el Convenio SIA y la Directiva 95/46/CE, el Reglamento (CE) 45/2001, el Convenio 108 CdE y la Recomendación policial R (87) 15 CdE.	Los datos personales copiados del SIA a otros sistemas para gestión de riesgo o análisis operativos sólo se podrán conservar el tiempo necesario para lograr el fin para el que se copiaron y no más de diez años.	En vigor en todos los Estados miembros.	La Comisión, en cooperación con los Estados miembros, informa anualmente al PE y al Consejo sobre el funcionamiento del SIA.
Iniciativa sueca	Iniciada por Suecia.	Racionalizar el intercambio de información para investigaciones y operaciones de inteligencia penales.	Descentralizada, los Estados miembros deben designar puntos de contacto nacionales que traten las solicitudes urgentes de información.	Toda la información o inteligencia penal existente de que dispongan las autoridades de los servicios represivos.	Policía, aduanas y cualquier otra autoridad con atribuciones para investigar delitos (con excepción de los servicios de inteligencia).	Normas nacionales de protección de datos así como el Convenio 108 CdE, el Protocolo adicional 181 CdE y la Recomendación policial R (87) 15 CdE.	La información y los datos suministrados a través de este instrumento sólo pueden utilizarse para los fines para los que se solicitaron y con arreglo a las condiciones específicas fijadas por el Estado miembro que los haya facilitado.	12 de los 31 signatarios (Estados de la UE y la AELC) han aprobado leyes nacionales para la aplicación de este instrumento; cinco rellenan el formulario para solicitar datos; y dos lo usan con frecuencia para intercambiar información.	La Comisión debe presentar su informe de evaluación al Consejo en 2010.

Panorama general en forma de cuadro de los instrumentos en aplicación, en ejecución o en consideración

Instrumento	Antecedentes	Finalidad(es)	Estructura	Cobertura de datos personales	Acceso a los datos	Protección de datos	Conservación de datos	Estado de ejecución	Revisión
Decisión Prüm	Iniciada por los Estados miembros	Mejorar la prevención de los delitos, en particular el terrorismo, y mantener el orden público.	Descentralizada, interconectada a través de la red s-TESTA. Los puntos de contacto nacionales tratan las solicitudes para comparar datos que salen y entran.	Perfiles anónimos de ADN e impresiones dactilares, datos de los registros de matriculación de vehículos e información sobre individuos sospechosos de vínculos con el terrorismo.	Los puntos de contacto transmiten las solicitudes; el acceso está regulado por las legislaciones nacionales.	Normas específicas establecidas en la Decisión Prüm y en el Convenio 108 CdE, el Protocolo adicional 181 CdE y la Recomendación policial R (87) 15 CdE. Las personas pueden dirigirse a su supervisor nacional de protección de datos para que se respeten sus derechos respecto al tratamiento de los datos personales.	Los datos personales deben borrarse una vez que ya no sean necesarios para la finalidad para la que se suministraron. El periodo máximo de conservación de los datos nacionales del Estado que los haya suministrado es vinculante para el Estado que los reciba.	La Decisión Prüm está en fase de ejecución. Diez Estados miembros han sido autorizados a intercambiar ADN, cinco a intercambiar impresiones dactilares y siete a intercambiar datos de los registros de matriculación de vehículos. Noruega e Islandia están a punto de acceder a este instrumento.	La Comisión debe presentar su informe de evaluación al Consejo en 2012.
Directiva sobre conservación de datos	Iniciada por los Estados miembros	Mejorar la investigación, la detección y la persecución de delitos graves conservando los datos sobre el tráfico de telecomunicaciones y de localización.	Descentralizada, este instrumento impone obligaciones a los proveedores de servicios de telecomunicaciones para conservar datos.	Número de teléfono, dirección IP e identificador del equipo móvil.	Las autoridades con derechos de acceso se definen a nivel nacional.	Directivas 95/46/CE y 2002/58/CE.	De 6 a 24 meses,	Seis Estados miembros todavía no han incorporado esta directiva y los tribunales constitucionales alemán y rumano dictaminaron que las leyes de aplicación no eran constitucionales.	La Comisión debe presentar su informe de evaluación al PE y al Consejo en 2010.

Panorama general en forma de cuadro de los instrumentos en aplicación, en ejecución o en consideración

Instrumento	Antecedentes	Finalidad(es)	Estructura	Cobertura de datos personales	Acceso a los datos	Protección de datos	Conservación de datos	Estado de ejecución	Revisión
Sistema de información europeo de antecedentes penales (ECRIS)	Iniciado por Bélgica y propuesto por la Comisión.	Mejorar el intercambio transfronterizo de datos relativos a los antecedentes penales de ciudadanos de la UE.	Descentralizada, interconectada a través de un conjunto de autoridades centrales que intercambiarán información extraída de los registros de antecedentes penales utilizando la red s-TESTA.	Datos biográficos; la condena, la sentencia y el delito; datos adicionales, incluidas las impresiones dactilares (si se dispone de ellas).	Autoridades judiciales y autoridades administrativas competentes.	Normas específicas establecidas por la Decisión marco 2009/315/JAI, que incorpora las normas de la Decisión 2005/876 JAI del Consejo, así como la Decisión marco 2009/977/JAI del Consejo, el Convenio 108 CdE y el Reglamento (CE) nº 45/2001.	Se aplican las normas nacionales de conservación de datos, ya que este instrumento sólo regula los intercambios de datos.	ECRIS II se encuentra en fase de ejecución. Nueve Estados miembros han empezado a intercambiar información electrónicamente.	La Comisión debe presentar dos informes de evaluación al PE y al Consejo: sobre la Decisión marco 2008/675/JAI, en 2011; sobre la Decisión marco 2009/315/JAI, en 2015. A partir de 2016, la Comisión deberá publicar informes regulares sobre el funcionamiento de la Decisión marco 2009/316/JAI (ECRIS).
Cooperación Unidad de Información Financiera (FIU.net)	Iniciada por los Países Bajos.	Intercambiar la información necesaria para analizar e investigar el blanqueo de capitales y la financiación del terrorismo.	Descentralizada, las UIF intercambian datos a través de FIU.net que funciona por la red s-TESTA. La aplicación de Europol SIENA podrá respaldar pronto FIU.net.	Todos los datos pertinentes para analizar o investigar el blanqueo de capitales y la financiación del terrorismo.	Unidades de información financiera (dentro de las fuerzas de policía, autoridades judiciales o administrativas que informen a las autoridades financieras).	Decisión marco 2008/315/JAI del Consejo, Convenio 108 del CdE y Recomendación policial R (87) 15 CdE.	Se aplican las normas nacionales de conservación de datos, ya que este instrumento sólo regula los intercambios de datos.	Veinte Estados miembros participan en FIU.net, una aplicación para compartir datos en línea que funciona por s-TESTA.	Como parte de su Plan de acción sobre servicios financieros, la Comisión ha estado revisando la aplicación de la Directiva 2005/60/CE desde 2009.

Panorama general en forma de cuadro de los instrumentos en aplicación, en ejecución o en consideración

Instrumento	Antecedentes	Finalidad(es)	Estructura	Cobertura de datos personales	Acceso a los datos	Protección de datos	Conservación de datos	Estado de ejecución	Revisión
Cooperación Organismos de recuperación de activos (ORA, *Asset Recovery Office* - ARO)	Iniciada por los Estados miembros	Intercambiar la información necesaria para rastrear e identificar los productos del delito.	Descentralizada, los ORA son necesarios para intercambiar información a través de la Iniciativa sueca. La aplicación de Europol SIENA podrá respaldar pronto la cooperación ORA.	Detalles de la propiedad buscada, tales como cuentas bancarias, bienes inmobiliarios y vehículos, así como los detalles de las personas buscadas, nombre, dirección, información sobre el accionista y la empresa.	Organismos de recuperación de activos.	Convenio 108 CdE, Protocolo adicional 181 CdE y Recomendación policial R (87) 15 CdE.	Se aplican las normas nacionales de conservación de datos, ya que este instrumento sólo regula los intercambios de datos.	Más de veinte Estados miembros han creado ORA; doce participan en un proyecto piloto que ha desplegado la aplicación SIENA de Europol para intercambiar datos pertinentes para el seguimiento de activos.	La Comisión debe presentar su informe de evaluación al Consejo en 2010.
Plataformas contra la delincuencia informática nacionales y de la UE	Iniciada por Francia.	Recoger, intercambiar y analizar información sobre delitos cometidos en internet.	Descentralizada, reúne plataformas nacionales de aviso y la plataforma de la UE contra delincuencia informática de Europol. La aplicación SIENA de Europol podrá respaldar pronto los intercambios de datos entre plataformas de aviso.	Contenido o comportamiento ilícitos detectados en internet.	Las plataformas nacionales reciben informes de los ciudadanos; la plataforma de la UE contra delincuencia informática de Europol recibe informes de las autoridades de los servicios represivos sobre formas graves de delincuencia informática transfronteriza.	Normas específicas establecidas en la Decisión Europol y en la Decisión marco 2009/977/JAI del Consejo, el Convenio 108 CdE, el Protocolo adicional 181 CdE, la Recomendación policial R (87) 15 CdE y el Reglamento (CE) 45/2001.	Se aplican las normas nacionales de conservación de datos, ya que esta medida sólo regula los intercambios de información.	Casi todos los Estados miembros han creado plataformas nacionales de aviso; Europol está trabajando en su Plataforma contra la delincuencia informática de la UE.	Europol cubre la delincuencia informática y, en el futuro, informará de las actividades de la Plataforma contra la delincuencia informática de la UE en su Informe anual presentado al Consejo para su aprobación y al Parlamento Europeo para información.

Panorama general en forma de cuadro de los instrumentos en aplicación, en ejecución o en consideración

Instrumento	Antecedentes	Finalidad(es)	Estructura	Cobertura de datos personales	Acceso a los datos	Protección de datos	Conservación de datos	Estado de ejecución	Revisión
Europol	Iniciado por los Estados miembros	Ayudar a los Estados miembros a prevenir y combatir la delincuencia organizada, el terrorismo y otras formas de delincuencia grave que afecten a dos o más Estados miembros.	Europol es una agencia de la UE con sede en La Haya. Está desarrollando SIENA, su propia red de intercambio seguro de información.	El sistema de información de Europol (*Europol Information System* - EIS) contiene los datos personales, incluidos, entre otros, los identificadores biométricos, las condenas y las relaciones con la delincuencia organizada, de las personas sospechosas de cometer delitos que entran en el mandato de Europol. Los ficheros de trabajo de análisis (*Analysis Work Files* - AWF) contienen todos los datos personales pertinentes.	Pueden acceder al EIS las unidades nacionales de Europol, los funcionarios de enlace, el personal de Europol y el director. Los funcionarios de enlace tienen autorizado el acceso a los AWF. Los datos personales pueden intercambiarse con terceros países que tengan acuerdos con Europol.	Normas específicas establecidas en Decisión Europol y en la Decisión marco 2009/977/JAI del Consejo, el Convenio 108 CdE, el Protocolo adicional 181 CdE, la Recomendación policial R (87) 15 CdE y el Reglamento (CE) 45/2001.	Los ficheros AWF podrán conservarse un plazo máximo de tres años, con la posibilidad de ampliarlo otros tres años.	Todos los Estados miembros usan activamente Europol así como los terceros países con los que tiene acuerdos operativos. Todos los Estados miembros aplican el nuevo fundamento jurídico de Europol.	Una autoridad común de control supervisa el tratamiento por parte de Europol de los datos personales y la transmisión de esos datos a otras partes. Presenta informes periódicos al PE y al Consejo. Europol presenta también un informe anual sobre sus actividades al Consejo para su aprobación y al PE para información.

Panorama general en forma de cuadro de los instrumentos en aplicación, en ejecución o en consideración

Instrumento	Antecedentes	Finalidad(es)	Estructura	Cobertura de datos personales	Acceso a los datos	Protección de datos	Conservación de datos	Estado de ejecución	Revisión
Eurojust	Iniciado por los Estados miembros	Mejorar la coordinación de las investigaciones y las acciones penales en los Estados miembros e impulsar la cooperación entre las autoridades competentes.	Eurojust es un organismo de la UE con sede en La Haya que utiliza s-TESTA para el intercambio de datos.	Datos personales de sospechosos y delincuentes en casos de delitos graves que afecten a dos o más Estados miembros, incluidos los datos biográficos, datos de contacto, perfiles de ADN, impresiones dactilares, fotografías y datos sobre el tráfico de telecomunicaciones y de localización.	Los 27 miembros nacionales de Europol que pueden compartir datos con las autoridades nacionales y terceros países si la fuente de información está de acuerdo.	Normas específicas establecidas en la Decisión Eurojust y en la Decisión marco 2009/977/JAI del Consejo, el Convenio 108 CdE, el Protocolo adicional 181 CdE y la Recomendación policial R (87) 15 CdE.	La información debe borrarse una vez se haya alcanzado el objetivo para el que se suministró y una vez se haya cerrado el caso.	El fundamento jurídico modificado de Eurojust está siendo ejecutado actualmente por los Estados miembros.	La Comisión debe revisar, antes de junio de 2014, el intercambio de datos entre los miembros nacionales de Eurojust. Antes de junio de 2013, Eurojust tendrá que informar al Consejo y a la Comisión sobre la concesión de acceso nacional a su sistema de gestión de asuntos. Una autoridad común de control supervisa el tratamiento por parte de Eurojust de los datos personales e informa anualmente al Consejo. El Presidente del Colegio de Eurojust presenta al Consejo un informe anual sobre las actividades de Eurojust, que el Consejo transmite al PE.

Panorama general en forma de cuadro de los instrumentos en aplicación, en ejecución o en consideración

Instrumento	Antecedentes	Finalidad(es)	Estructura	Cobertura de datos personales	Acceso a los datos	Protección de datos	Conservación de datos	Estado de ejecución	Revisión
Acuerdos PNR con EE.UU. y Australia; Acuerdo API/PNR con Canadá	Iniciados por la Comisión.	Prevenir y combatir el terrorismo y otras formas graves de delincuencia transnacional.	Acuerdos internacionales	Los acuerdos estadounidense y australiano contienen 19 categorías de datos PNR, incluidos los biográficos, de reservas, de pago e información suplementaria; el acuerdo canadiense incluye 25 tipos de datos similares.	El Departamento de seguridad interna de los EE.UU, la Agencia de servicios fronterizos de Canadá y el servicio de aduanas australiano, que pueden compartir datos con los servicios interiores represivos y antiterroristas.	Las normas de protección de los datos se fijan en los acuerdos internacionales específicos.	EE.UU.: siete años de uso activo y ocho años de pasivo; Australia: 3,5 años de uso activo y dos años de pasivo; Canadá: 72 horas de uso activo y 3,5 años de pasivo.	Los acuerdos con los EE.UU. y Australia se aplican provisionalmente; el de Canadá está en vigor. La Comisión renegociará estos acuerdos. Seis estados miembros de la UE han promulgado leyes que permiten el uso de datos PNR con efectos represivos.	Todos los acuerdos fijan revisiones periódicas, mientras que los acuerdos canadiense y australiano incluyen también cláusulas de denuncia.

Panorama general en forma de cuadro de los instrumentos en aplicación, en ejecución o en consideración

Instrumento	Antecedentes	Finalidad(es)	Estructura	Cobertura de datos personales	Acceso a los datos	Protección de datos	Conservación de datos	Estado de ejecución	Revisión
Acuerdo TFTP UE-EE.UU.	Iniciado por la Comisión.	Prevenir, detectar, investigar o perseguir el terrorismo o la financiación del terrorismo.	Acuerdo internacional.	Datos de mensajería financiera que incluyan, entre otros, el nombre, el número de cuenta, dirección y número de identificación del ordenante y receptores de las transacciones financieras.	El Tesoro de los EE.UU. puede compartir los datos personales extraídos de los mensajes financieros con las autoridades de los servicios represivos, de seguridad pública o antiterroristas de los EE.UU., los Estados miembros, Europol o Eurojust. La transferencia a terceros países está sujeta al consentimiento de los Estados miembros.	El acuerdo incluye cláusulas estrictas de finalidad limitada y proporcionalidad.	Los datos personales extraídos de los mensajes financieros podrán conservarse sólo el tiempo necesario para las investigaciones o acciones penales individuales; los datos no extraídos podrán conservarse sólo cinco años.	El PE dio su consentimiento a la celebración del Acuerdo TFTP UE-EE.UU. el 8 de julio de 2010. Se espera ahora que el Consejo adopte una Decisión del Consejo por la que se celebre este acuerdo, tras lo cual el acuerdo entrará en vigor mediante un Canje de Notas entre las partes.	La Comisión deberá revisar los acuerdos a los seis meses de su entrada en vigor. Su informe de evaluación se deberá remitir al PE y al Consejo.