I

(Resoluciones, recomendaciones y dictámenes)

DICTÁMENES

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Dictamen del Supervisor Europeo de Protección de Datos acerca del informe final del Grupo de Contacto de Alto Nivel entre la UE y Estados Unidos sobre el intercambio de información y la protección de la vida privada y los datos personales

(2009/C 128/01)

EL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS,

Visto el Tratado constitutivo de la Comunidad Europea, en particular su artículo 286,

Vista la Carta de los Derechos Fundamentales de la Unión Europea, en particular su artículo 8,

Vista la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos,

Visto el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, y en particular su artículo 41,

HA ADOPTADO EL SIGUIENTE DICTAMEN:

I. **INTRODUCCIÓN — ANTECEDENTES DEL PRESENTE DICTAMEN**

1. El 28 de mayo de 2008, la Presidencia del Consejo de la Unión Europea anunció al Coreper que el Grupo de Contacto de Alto Nivel entre la UE y Estados Unidos sobre el intercambio de información y la protección de la vida privada y los datos personales (en lo sucesivo, «el Grupo de Contacto») había ultimado su informe con vistas a la Cumbre que la UE celebraría el 12 de junio de 2008. El informe se hizo público el 26 de junio de 2008 [1]

2. Como primer paso para intercambiar información con Estados Unidos con el objetivo de combatir el terrorismo y las formas graves de delincuencia internacional, el Grupo de Contacto se inclina en el informe por determinar unos principios comunes de protección de la vida privada y los datos personales.

3. La Presidencia del Consejo indicó al anunciar el informe que cualquier propuesta relativa a la actuación consecutiva a éste sería bienvenida, y que agradecería en particular que se expusieran las reacciones a las recomendaciones del informe en cuanto a la forma de continuar los trabajos. El Supervisor Europeo de Protección de Datos (SEPD) responde a esta invitación con el presente dictamen, basado en la información que se ha hecho pública sobre la situación de los trabajos, sin perjuicio de la posición que pueda tomar en el futuro a la luz de la evolución de este expediente.

4. El SEPD observa que los trabajos del Grupo de Contacto se han realizado, en especial desde el 11 de septiembre de 2001, en el contexto de una intensificación del intercambio de datos entre Estados Unidos y la UE, que se ha llevado a cabo merced a acuerdos internacionales u otros tipos de instrumentos. Entre ellos cabe citar los acuerdos de Europol y Eurojust con Estados Unidos, así como los acuerdos relativos al registro de nombres de los pasajeros (PNR) y el caso Swift, origen de un canje de notas entre funcionarios de la UE y de Estados Unidos para establecer garantías mínimas de protección de datos [2].

[1] Documento 9831/08 del Consejo, que puede consultarse en la dirección http://ec.europa.eu/justice_home/fsj/privacy/news/index_en.htm

[2] — Acuerdo entre los Estados Unidos de América y la Oficina Europea de Policía, de 6 de diciembre de 2001, y suplemento al Acuerdo entre los Estados Unidos de América y la Oficina Europea de Policía sobre el intercambio de datos personales e informaciones conexas, publicados en la sede electrónica de Europol.
— Acuerdo sobre cooperación judicial entre los Estados Unidos de América y Eurojust, de 6 de noviembre de 2006, publicado en la sede electrónica de Eurojust.
— Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (Acuerdo PNR 2007), firmado en Bruselas el 23 de julio de 2007 y en Washington el 26 de julio de 2007 (DO L 204 de 4.8.2007, p. 18).
— Canje de notas entre las autoridades de EE.UU. y de la UE sobre el Programa de Seguimiento de la Financiación del Terrorismo, de 28 de junio de 2007.

5. La UE también ha negociado y aprobado instrumentos similares de intercambio de datos personales con otros países terceros. Un ejemplo reciente es el Acuerdo entre la Unión Europea y Australia sobre el tratamiento y la transferencia de datos, generados en la Unión Europea, del registro de nombres de los pasajeros (PNR) por las compañías aéreas a los Servicios de Aduanas de Australia ([3]).

6. En este contexto, las solicitudes de información personal de las autoridades policiales y judiciales de terceros países están aumentando constantemente, y haciéndose extensivas no sólo a las bases de datos tradicionales de la Administración sino también a otros tipos de archivos de datos, en particular los recopilados por el sector privado.

7. Hay otro elemento importante de este contexto que el SEPD desea mencionar, a saber, que la cuestión de la transferencia de datos personales a terceros países en el contexto de la cooperación policial y judicial en materia penal quedará regulada en la Decisión marco del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal ([4]), que se adoptará probablemente antes de finales de 2008.

8. Lo previsible es que estos intercambios transatlánticos de datos sigan aumentando y afecten a otros sectores en los que se procesan datos personales. En este contexto, el diálogo sobre la lucha contra la delincuencia a escala transatlántica resulta a la vez bienvenido y delicado. Bienvenido porque puede dar lugar a la elaboración de un marco más claro para los intercambios de datos que se están realizando ya o que se realizarán en el futuro. Delicado porque semejante marco podría legitimar transferencias masivas de datos en un ámbito (el policial) cuyas repercusiones en las personas pueden ser especialmente graves, y en el que resulta especialmente necesario establecer salvaguardias y garantías estrictas y fiables ([5]).

9. En la sección siguiente del presente dictamen se hace balance de la situación actual y se analizan posibles formas de continuar los trabajos sobre este expediente. La sección III se centra en el ámbito de aplicación y la naturaleza de un instrumento que permita el intercambio de información. En la sección IV del dictamen se analizan, desde una perspectiva general, los aspectos jurídicos ligados al contenido de un posible acuerdo. Se abordan cuestiones como las condiciones de evaluación del nivel de protección ofrecido en Estados Unidos, se analiza la posibilidad de emplear el marco regulador de la UE como referencia para evaluar ese nivel de protección, y se enumeran los requisitos básicos que deberían figurar en el acuerdo. Por último, la sección V del dictamen contiene un análisis de los principios de protección de la vida privada anejos al informe.

([3]) DO L 213 de 8.8.2008, p. 49.

([4]) Decisión marco del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, versión del 24 de junio de 2008; puede consultarse en la dirección http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=es&DosId=193371

([5]) Por lo que se refiere a la necesidad de un marco jurídico claro, véanse las secciones III y IV del presente dictamen.

II. SITUACIÓN ACTUAL Y POSIBLES FORMAS DE CONTINUAR LOS TRABAJOS SOBRE ESTE EXPEDIENTE

10. La situación actual, según la evalúa el SEPD, es que se han hecho algunos progresos en la definición de normas comunes sobre el intercambio de información y la protección de la vida privada y los datos personales.

11. Con todo, los preparativos de un acuerdo entre la UE y Estados Unidos, cualesquiera que sean sus características, no están en modo alguno acabados. Es necesario seguir trabajando sobre este expediente. El propio Grupo de Contacto menciona en su informe una serie de cuestiones pendientes, entre las cuales la de la tutela de los derechos la más destacada. Sigue habiendo desacuerdo sobre el alcance que debe tener la tutela judicial ([6]). En el capítulo 3 del informe se mencionan otras cinco cuestiones pendientes. Por lo demás, del presente dictamen se desprende que quedan por resolver muchas otras cuestiones, como la del ámbito de aplicación y la naturaleza del instrumento de intercambio de datos.

12. Dado que la opción preferida según el informe — preferencia que el SEPD comparte — sería un acuerdo vinculante, la prudencia es de rigor. Antes de que pueda alcanzarse un acuerdo, será preciso continuar la labor de preparación de forma cuidadosa y detenida.

13. Por último, a juicio del SEPD, lo ideal sería que la celebración del posible acuerdo tuviera lugar en el contexto del Tratado de Lisboa, en el supuesto, naturalmente, de que éste entre en vigor. En efecto, el Tratado de Lisboa suprimiría toda inseguridad jurídica en cuanto a la línea divisoria entre los pilares de la UE. Además, dicho Tratado garantizaría la plena participación del Parlamento Europeo, al igual que el control judicial por el Tribunal de Justicia.

14. En estas circunstancias, la mejor manera de progresar en este expediente consistiría en elaborar un plan de trabajo para un posible acuerdo futuro. Dicho plan debería constar de los siguientes elementos:

— Directrices y calendario para la continuación de los trabajos del Grupo de Contacto (o de cualquier otro grupo).

— En una fase temprana de los trabajos, debate y, si es posible, acuerdo sobre cuestiones fundamentales como el ámbito de aplicación y la naturaleza del acuerdo.

— Partiendo de una interpretación común de estas cuestiones fundamentales, definición más precisa de los principios de protección de datos.

— Intervención de los interesados en diferentes etapas del procedimiento.

— Por parte de la Unión Europea, análisis de las restricciones institucionales.

([6]) Véase la página 5, epígrafe C, del informe.

III. ÁMBITO DE APLICACIÓN Y NATURALEZA DE UN INSTRUMENTO SOBRE INTERCAMBIO DE DATOS

15. A juicio del SEPD, es fundamental que se definan con claridad el ámbito de aplicación y la naturaleza del posible instrumento, incluidos los principios de protección de datos, antes de profundizar en la elaboración de tal instrumento.

16. En cuanto al ámbito de aplicación del instrumento, es preciso responder a varias preguntas importantes, a saber:

— ¿A qué entidades, dentro y fuera del ámbito policial y judicial, se aplicaría el acuerdo?

— ¿Qué se entiende por intercambio de datos «para fines policiales», y qué relación tiene este objetivo con otros como la seguridad nacional o, más concretamente, el control de fronteras y la salud pública?

— ¿Cómo se encajaría el instrumento en la perspectiva de un espacio transatlántico de seguridad mundial?

17. Al definir la naturaleza del acuerdo habría que aclarar las siguientes cuestiones:

— ¿En el marco de qué pilar, en su caso, se negociaría el instrumento?

— ¿Sería vinculante el instrumento para la UE y para Estados Unidos?

— ¿Tendría efectos directos, en el sentido de fijar derechos y obligaciones para las personas que pudieran alegarse ante una autoridad judicial?

— ¿Regularía el instrumento en sí el intercambio de información, o bien se limitaría a fijar normas mínimas para dicho intercambio, que se completarían después con acuerdos específicos?

— ¿Cuál sería la relación entre este instrumento y otros instrumentos ya existentes: los respetaría, los sustituiría o los completaría?

III.1. Ámbito de aplicación del instrumento

Entidades afectadas

18. Aunque el informe del Grupo de Contacto no contiene indicaciones claras sobre el ámbito de aplicación concreto del futuro instrumento, de los principios que en él se mencionan cabe deducir que la idea es que se aplique a las transferencias tanto entre los sectores público y privado ([7]) como entre autoridades públicas.

([7]) Véase, en particular, el capítulo 3 del informe, «Cuestiones pendientes relativas a las relaciones transatlánticas», punto 1: «Coherencia de las obligaciones de las entidades privadas durante las transferencias de datos».

— Entre los sectores público y privado:

19. El SEPD comprende la lógica de la aplicabilidad del posible instrumento futuro a las transferencias entre los sectores público y privado. La elaboración de dicho instrumento se inscribe en el contexto de las solicitudes de información presentadas en los últimos años por Estados Unidos a entidades del sector privado. El SEPD observa, en efecto, que el sector privado se está convirtiendo en una fuente sistemática de información para fines policiales, tanto dentro de la UE como a escala internacional ([8]). El caso SWIFT, donde se pidió a una empresa privada que transmitiera sistemáticamente datos en bloque a autoridades policiales de un país tercero, fue un importante precedente a este respecto ([9]). La recopilación de datos del registro de nombres de pasajeros (PNR) de las compañías aéreas sigue la misma lógica. Ya en su dictamen sobre la propuesta de Decisión marco del Consejo relativa a un PNR europeo ([10]), el SEPD cuestionó la legitimidad de esta tendencia.

20. Hay otras dos razones para oponerse a que se incluyan en el ámbito de aplicación del futuro instrumento las transferencias de datos entre los sectores público y privado.

21. En primer lugar, esta inclusión podría tener un efecto no deseado dentro del territorio de la propia UE. El SEPD teme que el hecho de que los datos de empresas privadas (como las entidades financieras) puedan transferirse en principio a países terceros constituya una importante presión para que ese tipo de datos se pongan a disposición de las autoridades policiales también dentro de la UE. El sistema PNR es un ejemplo de esta evolución indeseable, que comenzó con la recopilación en bloque de los datos de los pasajeros en EE.UU., y se trasladó a continuación al contexto interno de la UE ([11]), sin que se haya demostrado claramente la necesidad ni la proporcionalidad del sistema.

22. En segundo lugar, en su dictamen sobre la propuesta relativa al PNR de la UE presentada por la Comisión, el SEPD también planteó la cuestión del marco de protección de datos (primer o tercer pilar) que se aplicaría a las

([8]) Véase a este respecto el dictamen del SEPD del 20 de diciembre de 2007 acerca de la propuesta de Decisión marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros (Passenger Name Record — PNR) con fines represivos (DO C 110 de 1.5.2008, p. 1): «Hasta la fecha, ha existido siempre una separación clara entre las actividades del sector privado y las de las autoridades represivas: estas últimas son realizadas por autoridades específicamente designadas para ello, en particular la policía, pudiéndose pedir a los agentes del sector privado que, en función de las circunstancias de cada caso, comuniquen datos personales a las autoridades represivas. Se observa actualmente una tendencia a imponer de forma sistemática a los agentes del sector privado obligaciones de cooperación para fines represivos».

([9]) Véase el dictamen 10/2006 del Grupo de Trabajo del Artículo 29, del 22 de noviembre de 2006, sobre el tratamiento de datos personales por parte de la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (*Worldwide Interbank Financial Telecommunication* — SWIFT), WP 128.

([10]) Dictamen del 20 de diciembre de 2007, *op. cit.*

([11]) Véase la propuesta de Decisión marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros (Passenger Name Record — PNR) con fines represivos, mencionada en la nota a pie de página nº 8, que está siendo debatida en el Consejo.

condiciones de cooperación entre el sector público y el privado: ¿deberían basarse las normas en la naturaleza del responsable del tratamiento (sector privado) o en la finalidad perseguida (fines policiales)? Cuando se imponen al sector privado obligaciones de tratamiento de datos personales para fines policiales, la línea divisoria entre el primer y el tercer pilar no está nada clara. En este contexto, resulta significativo que el Abogado General Bot, en sus recientes conclusiones sobre el asunto de la conservación de datos ([12]), propusiera una línea de demarcación para tales situaciones, pero que añadiera a su propuesta la siguiente observación: «Esta línea de demarcación no está ciertamente exenta de toda crítica y, en ciertos aspectos, puede parecer artificial.» El SEPD observa asimismo que la sentencia del Tribunal sobre el asunto PNR ([13]) no resuelve plenamente la cuestión del marco legal aplicable. Por ejemplo, el hecho de que ciertas actividades no estén reguladas en la Directiva 95/46/CE no significa automáticamente que tales actividades puedan regularse en el tercer pilar. Como consecuencia de ello, puede quedar un vacío jurídico en lo tocante a la legislación aplicable y, en todo caso, una inseguridad jurídica en cuanto a las garantías jurídicas a las que pueden acogerse los titulares de los datos.

23. Desde esta perspectiva, el SEPD destaca la necesidad de garantizar que un futuro instrumento con principios generales de protección de datos no pueda legitimar *per se* la transferencia transatlántica de datos personales entre entidades del sector privado y del sector público. Esta transferencia sólo podría incluirse en dicho instrumento a condición de que:

— el instrumento futuro estipule que la transferencia sólo está autorizada si ha quedado demostrado que es absolutamente necesaria para un fin determinado, debiendo adoptarse una decisión según las circunstancias concretas de cada caso;

— la transferencia propiamente dicha se efectúe con elevadas garantías de protección de datos (como las que se describen en el presente dictamen).

Por otra parte, el SEPD destaca la incertidumbre existente en cuanto al marco de protección de datos aplicable, lo cual le lleva a abogar por que, en todo caso, no se incluya la transferencia de datos personales entre entidades del sector privado y del sector público en la situación actual del Derecho de la UE.

— Entre autoridades públicas:

24. El alcance exacto del intercambio de información no está claro. Antes de continuar los trabajos sobre un instrumento común, sería conveniente aclarar el ámbito de aplicación previsto de éste. En particular, subsisten preguntas sobre los siguientes puntos:

— Por lo que respecta a las bases de datos situadas en la UE, ¿se aplicaría el instrumento a las bases de datos centralizadas (parcialmente) gestionadas por la UE, como las bases de datos de Europol y Eurojust, a bases de datos descentralizadas gestionadas por los Estados miembros, o bien a ambas?

— ¿Quedarían incluidas en el ámbito de aplicación del instrumento las redes interconectadas En otras palabras, ¿se aplicarían las garantías previstas a los datos intercambiados entre Estados miembros o agencias, tanto en la UE tanto como en EE.UU.?

— ¿Cubriría el instrumento los intercambios únicamente entre bases de datos de los servicios encargados de la lucha contra la delincuencia (policía, justicia y posiblemente aduanas) o también entre otras bases de datos como las de las autoridades tributarias?

— ¿Se aplicaría también el instrumento a las bases de datos de los servicios nacionales de seguridad, o permitiría éste el acceso de dichos servicios a las bases de datos policiales del territorio de la otra parte contratante (acceso de la UE a EE.UU. y viceversa)?

— ¿Regularía el instrumento las transferencias de información caso por caso, o el acceso permanente a las bases de datos existentes?Esta última hipótesis plantearía sin duda cuestiones de proporcionalidad, que se examinan con mayor detenimiento en el punto 3 de la sección V del presente dictamen.

Fines policiales

25. Queda también un margen de incertidumbre en la definición de la finalidad del posible acuerdo. La finalidad policial se menciona tanto en la introducción como en el primero de los principios anexos al informe, que se analizan con más detenimiento en la sección V del presente dictamen. De momento, el SEPD señala que de la formulación de esas menciones se desprende que el intercambio de datos se centraría en cuestiones del tercer pilar, aunque cabe preguntarse si no se trataría más bien de un primer paso hacia un intercambio más amplio de información. Parece claro que los fines de «seguridad pública» mencionados en el informe incluyen la lucha contra el terrorismo, contra la delincuencia organizada y contra otros delitos. Sin embargo, ha de entenderse que quedaría autorizado el intercambio de datos para otros fines de interés público, como, quizá, los riesgos para la salud pública.

26. El SEPD recomienda que se delimite esta finalidad a ciertos tratamientos de datos claramente determinados, y que se justifiquen las opciones de actuación que hayan dado lugar a la definición de esa finalidad.

([12]) Conclusiones del Abogado General Bot, de 14 de octubre de 2008, sobre el asunto C-301/06, Irlanda/Parlamento Europeo y Consejo, apartado 108.

([13]) Sentencia del Tribunal, de 30 de mayo de 2006, en los asuntos acumulados C-317/04 y C-318/04, Parlamento Europeo/Consejo de la Unión Europea (asunto C-317/04) y Comisión de las Comunidades Europeas (asunto C-318/04), Rec. 2006, p. I-4721.

Espacio transatlántico de seguridad mundial

27. El amplio alcance del informe que nos ocupa debe analizarse desde la perspectiva del espacio transatlántico de seguridad mundial sobre el que está trabajando el llamado Grupo «Futuro» ([14]). El informe de este grupo, de junio de 2008, hace hincapié en la dimensión exterior de la política de asuntos de interior, y aboga por que «*antes de 2014 la Unión Europea [tome una decisión sobre el]objetivo político de hacer realidad una zona euroatlántica de cooperación con los Estados Unidos en el ámbito de la libertad, la seguridad y la justicia*». Esta cooperación iría más allá de la seguridad en sentido estricto, ya que se haría extensiva como mínimo a las cuestiones reguladas en el actual título IV del Tratado CE, como la inmigración, los visados, el asilo y la cooperación judicial en materia civil. Es necesario plantearse en qué medida un intercambio de información tan amplio puede o debe basarse en un acuerdo sobre principios básicos de protección de datos como los que se mencionan en el informe del Grupo de Contacto.

28. Si las cosas evolucionan normalmente, la estructura de pilares habrá desaparecido en 2014, y habrá una sola base jurídica para la protección de datos dentro de la UE (según el Tratado de Lisboa, el artículo 16 del Tratado de Funcionamiento de la Unión Europea). Sin embargo, el hecho de que exista una armonización a escala de la UE en lo que se refiere a la *reglamentación* de la protección de datos no implica que cualquier acuerdo con un país tercero baste para autorizar la *transferencia* de cualquier tipo de datos personales para cualquier finalidad. Para determinados ámbitos, por ejemplo el policial, puede ser necesario adaptar las garantías exigidas en materia de protección de datos en función del contexto y las condiciones del tratamiento de los datos. El SEPD recomienda que se tengan en cuenta las consecuencias de estas diferentes perspectivas en la preparación de un acuerdo futuro.

III.2 **Naturaleza del acuerdo**

Marco institucional europeo

29. A corto plazo, en cualquier caso, es indispensable determinar en el contexto de qué pilar se negociará el acuerdo, sobre todo porque no se sabe cuál de los marcos reguladores de la protección de datos de la UE se verá afectado por el acuerdo: ¿será el del primer pilar, es decir, básicamente la Directiva 95/46/CE, con su régimen específico de transferencia de datos a terceros países, o bien el del tercer pilar, en el que el régimen de transferencias a terceros países es menos estricto? ([15])

30. Aunque, como se ha indicado ya, la finalidad predominante es la policial, el informe del Grupo de Contacto menciona la recopilación de datos de entidades del sector privado; además, los fines previstos pueden interpretarse en un sentido tan amplio que va desde la mera seguridad, incluidos aspectos como la inmigración y el control de fronteras, hasta incluso la salud pública. En vista de esta ambigüedad, sería muy preferible esperar a la armonización de los pilares en el contexto del Derecho de la UE, tal como está previsto en el Tratado de Lisboa, para establecer claramente la base jurídica de las negociaciones y el cometido exacto de las instituciones europeas, en particular el Parlamento Europeo y la Comisión.

Carácter vinculante del acuerdo

31. Convendría aclarar si las conclusiones de los debates se plasmarán en un memorando de entendimiento u otro instrumento no vinculante, o bien en un acuerdo internacional vinculante.

32. El SEPD comparte la preferencia por un acuerdo vinculante que se menciona en el informe del Grupo de Contacto. A juicio del SEPD, un acuerdo oficial vinculante es un requisito previo indispensable de tota transferencia de datos fuera de la UE, con independencia de la finalidad a la que obedezca la transferencia. No puede efectuarse ninguna transferencia de datos a un país tercero sin que existan condiciones y garantías adecuadas recogidas en un marco jurídico específico (y vinculante). En otras palabras, un memorando de entendimiento u otro instrumento no vinculante puede resultar útil para orientar las negociaciones de ulteriores acuerdos vinculantes, pero no puede sustituirlos.

Efecto directo

33. Las disposiciones del instrumento deberían ser igualmente vinculantes para Estados Unidos y para la UE y sus Estados miembros.

34. Habría que garantizar asimismo que las personas puedan ejercer sus derechos, y en particular disfrutar de una tutela efectiva de éstos, sobre la base de los principios acordados. A juicio del SEPD, la mejor forma de alcanzar este resultado consiste en formular las disposiciones sustantivas del acuerdo de tal manera que tengan efecto directo respecto de los residentes de la Unión Europea y que puedan alegarse ante un órgano jurisdiccional. Por ello, es necesario que el instrumento estipule claramente que las disposiciones del acuerdo internacional tendrán efecto directo, y que establezca las condiciones de su incorporación al Derecho interno de la UE y al Derecho nacional, a fin de garantizar la eficacia de las medidas.

Relación con otros instrumentos

35. La medida en que el acuerdo puede ser un instrumento autónomo o ha de completarse según el caso con ulteriores acuerdos sobre intercambios específicos de datos es también un punto fundamental. En efecto, es cuestionable que un solo acuerdo pueda cubrir adecuadamente, con un solo cuerpo de normas, los múltiples aspectos específicos

([14]) Informe del Grupo consultivo informal de alto nivel sobre el futuro de la política europea de asuntos de interior, «Libertad, seguridad e intimidad: los asuntos de interior europeos en un mundo abierto», junio de 2008. Este informe puede consultarse en el registro público de documentos del Consejo (register.consilium.europa.eu).

([15]) Véanse los artículos 11 y 13 de la Decisión marco sobre protección de datos personales a que se hace referencia en el apartado 7 del presente dictamen.

del tratamiento de datos en el tercer pilar. Es aún más dudoso que pueda *permitir*, sin debates y garantías adicionales, la aprobación general de cualquier transferencia de datos personales, cualesquiera que sean su finalidad y la naturaleza de los datos en cuestión. Además, los acuerdos con países terceros no son necesariamente permanentes, ya que pueden estar vinculados a amenazas específicas y estar sujetos a revisión y a cláusulas de caducidad. Por otra parte, la existencia de unas normas mínimas comunes consagradas en un instrumento vinculante podría facilitar ulteriores negociaciones sobre la transferencia de datos personales en relación con una base de datos o una operación de tratamiento específicas.

36. El SEPD abogaría en consecuencia por que, en lugar de optar por un acuerdo autónomo, se elaborase un conjunto mínimo de criterios de protección de datos, que se completaría según las circunstancias de cada caso con disposiciones adicionales específicas, tal como se indica en el informe del Grupo de Contacto. Las transferencias de datos en casos concretos quedarían supeditadas a esas disposiciones adicionales específicas. Esta solución fomentaría un planteamiento armonizado de la protección de datos.

Aplicación a los instrumentos ya existentes

37. También habría que analizar cómo se combinaría un posible acuerdo general con los acuerdos ya existentes que la UE ha celebrado con EE.UU. Conviene precisar que estos acuerdos preexistentes no tienen el mismo carácter vinculante, en particular el acuerdo PNR (el que mayor seguridad jurídica presenta), los acuerdos con Europol y Eurojust o el canje de notas sobre SWIFT ([16]). Hay que plantearse si el posible nuevo marco general completaría los instrumentos ya existentes o si, por el contrario, éstos no se verían afectados, al aplicarse el nuevo marco únicamente a otros intercambios futuros de datos personales. A juicio del SEPD, la coherencia jurídica requiere un conjunto de normas armonizado que se aplique a los acuerdos vinculantes sobre transferencias de datos (tanto los existentes como los futuros) y que los complete.

38. La aplicación del acuerdo general a los instrumentos existentes tendría la ventaja de reforzar el carácter vinculante de estos, lo cual sería especialmente positivo en lo que se refiere a los acuerdos que no son jurídicamente vinculantes, como el canje de notas sobre SWIFT, ya que, al menos, obligaría a respetar un conjunto de principios generales sobre protección de la vida privada.

IV. **EVALUACIÓN JURÍDICA GENERAL**

39. En la presente sección se analizan el modo en que debe evaluarse el grado de protección que ofrece un marco o instrumento específico, los criterios de referencia que han de emplearse y los requisitos básicos necesarios.

([16]) Véase la nota 2.

Nivel de protección adecuado

40. A juicio del SEPD, debe quedar claro que una de las principales consecuencias del futuro instrumento sería que sólo podrían efectuarse transferencias de datos personales a Estados Unidos si las autoridades de este país garantizan un nivel adecuado de protección (y viceversa).

41. El SEPD considera que únicamente una prueba real de adecuación constituiría garantía suficiente del grado de protección de los datos personales. El SEPD opina que un acuerdo marco general con un ámbito de aplicación tan amplio como el que se sugiere en el informe del Grupo de Contacto difícilmente superaría, como tal, una prueba real de adecuación. Sólo se podría considerar adecuado el acuerdo general si los acuerdos específicos celebrados atendiendo a las circunstancias de cada caso resultan igualmente adecuados.

42. La valoración del grado de protección ofrecido por países terceros no es un ejercicio inhabitual, en particular para la Comisión Europea: en el primer pilar, las transferencias están supeditadas a la idoneidad de esa protección. La idoneidad se ha evaluado en varias ocasiones con arreglo al artículo 25 de la Directiva 95/46/CE a partir de criterios específicos y ha sido confirmada por decisiones de la Comisión Europea ([17]). En el tercer pilar no se ha previsto expresamente un sistema similar: la evaluación de la idoneidad de la protección de datos sólo es obligatoria en el caso específico de los artículos 11 y 13 de la Decisión marco sobre protección de datos ([18]), pendiente de adopción, y queda en manos de los Estados miembros.

43. En el caso que nos ocupa, esta evaluación afecta a aspectos policiales, y la Comisión dirige los correspondientes debates bajo la supervisión del Consejo. Estamos en un contexto que guarda menos relación con la evaluación de los principios de «puerto seguro» o la idoneidad de la legislación canadiense, que con las recientes negociaciones sobre el PNR con Estados Unidos y Australia, celebradas en el marco jurídico del tercer pilar. Sin embargo, los principios del Grupo de Contacto se han mencionado también en el contexto del Programa de Exención de Visado, que se refiere a cuestiones de fronteras e inmigración, es decir, a cuestiones del primer pilar.

44. El SEPD recomienda que las conclusiones sobre la adecuación de la protección de datos de cualquier instrumento futuro se base en la experiencia adquirida en estos

([17]) En el sitio http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm pueden consultarse diversas decisiones de la Comisión sobre la adecuación de la protección de los datos personales en países terceros, en particular en Argentina, Canadá, Suiza, Estados Unidos, Guernesey, la Isla de Man y Jersey.

([18]) Obligación limitada a aquellos casos en que un Estado miembro se propone transferir a un país tercero o a un organismo internacional datos recibidos de una autoridad competente de otro Estado miembro.

diferentes ámbitos. Recomienda asimismo que se siga trabajando sobre el concepto de «adecuación» en el contexto de un instrumento futuro, sobre la base de criterios similares a los utilizados en anteriores análisis de adecuación.

Reconocimiento mutuo — Reciprocidad

45. La cuestión del grado de protección de los datos tiene un segundo aspecto, a saber, el reconocimiento mutuo de los sistemas de la UE y de Estados Unidos. El informe del Grupo de Contacto indica a este respecto que el objetivo consistiría en «lograr que cada parte reconociera la eficacia del sistema de protección de los datos y la vida privada de la otra para los ámbitos a que se refieren estos principios» ([19]) y conseguir «una aplicación equivalente y recíproca de la legislación sobre protección de los datos y de la vida privada».

46. Para el SEPD, es obvio que el reconocimiento mutuo (o la reciprocidad) sólo es posible si queda garantizado un nivel adecuado de protección de los datos. En otras palabras, el futuro instrumento debe suponer la armonización de un nivel mínimo de protección (mediante un análisis de la adecuación, teniendo en cuenta la necesidad de acuerdos específicos celebrados atendiendo a las circunstancias de cada caso). Sólo si se cumple esta condición podrá reconocerse la reciprocidad.

47. El primer elemento que debe tenerse en cuenta es la reciprocidad de las disposiciones sustantivas sobre protección de datos. A juicio del SEPD, el posible acuerdo debería abordar el concepto de la reciprocidad de las disposiciones sustantivas de modo que quede garantizado, por una parte, que el tratamiento de datos dentro del territorio de la UE (y de Estados Unidos) respete plenamente las legislaciones nacionales sobre protección de datos y, por otra, que las operaciones de tratamiento de datos fuera del país de origen de estos que estén incluidas en el ámbito de aplicación del acuerdo respeten los principios de protección de datos recogidos en el acuerdo.

48. El segundo elemento es la reciprocidad de los mecanismos de tutela de los derechos. Hay que garantizar que los ciudadanos de la Unión Europea tengan medios adecuados para hacer valer sus derechos cuando sus datos personales estén sido objeto de tratamiento en Estados Unidos (con independencia de la legislación que se aplique al tratamiento), pero también que la Unión Europea y sus Estados miembros reconozcan derechos equivalentes a los ciudadanos estadounidenses.

49. El tercer elemento es la reciprocidad del acceso de las autoridades policiales a los datos personales. La reciprocidad significa que, si un instrumento permite a las autoridades estadounidenses acceder a datos generados en la Unión Europea, debe concederse a las autoridades de la UE el mismo acceso a los datos generados en Estados Unidos. La reciprocidad no debe ir en detrimento de la eficacia de la protección del titular de los datos. Esta condición debe cumplirse antes de que pueda autorizarse el acceso «transatlántico» de las autoridades policiales. Concretamente, esto significa que:

— No debe permitirse el acceso directo de las autoridades estadounidenses a datos existentes en el territorio de la UE (y viceversa). El acceso debe realizarse únicamente de manera indirecta, en el marco de un sistema de exportación o transmisión de los datos (sistema *push*).

— Este acceso debe efectuarse bajo el control de las autoridades de protección de datos y las autoridades judiciales del país en el que tenga lugar el tratamiento de datos.

— El acceso de las autoridades estadounidenses a bases de datos de la UE debe respetar las disposiciones sustantivas sobre protección de datos (véase *supra*) y garantizar plenamente la tutela efectiva de los derechos del titular de los datos.

Precisión del instrumento

50. La especificación de las condiciones de evaluación (adecuación, equivalencia, reconocimiento mutuo) es esencial puesto que determina el contenido, en términos de precisión, la seguridad jurídica y la eficacia de la protección. El contenido del posible acuerdo futuro debe ser preciso y exacto.

51. Por otra parte, debe quedar claro que cualquier acuerdo específico que se celebre en una etapa ulterior deberá incluir asimismo garantías detalladas y completas de protección de datos en relación con el tema del intercambio de datos previsto. Sólo duplicando así los principios concretos de protección de datos se quedará garantizada la estrecha correspondencia necesaria entre el acuerdo general y los acuerdos específicos, como se ha indicado ya en los apartados 35 y 36 del presente dictamen.

Elaboración de un modelo para otros países terceros

52. Hay otra cuestión sobre la cual vale la pena reflexionar expresamente, a saber, hasta qué punto un acuerdo con Estados Unidos podría servir de modelo para otros países terceros. El SEPD observa que, además de EE.UU., el informe del Grupo «Futuro» antes mencionado alude también a Rusia como socio estratégico de la UE. Si los principios son neutros y acordes con las salvaguardias fundamentales de la UE, podrían constituir un valioso precedente. Sin embargo, las características específicas asociadas, por ejemplo, al marco jurídico del país receptor de los datos o a la finalidad de la transferencia impiden proceder mediante un mero calco del acuerdo. Igualmente determinante debe ser la situación democrática de los países terceros en cuestión: es preciso asegurarse de que los principios acordados se garanticen y apliquen efectivamente en el país receptor.

¿Con qué criterios de referencia evaluar el nivel de protección de los datos?

53. La idoneidad implícita o explícita de la protección de datos debe evaluarse, en cualquier caso, con arreglo al marco jurídico europeo e internacional, y en especial las salvaguardias de protección de datos comúnmente aceptadas,

([19]) Véase el epígrafe A del informe, «Acuerdo internacional vinculante» (página 8).

que están recogidas en los Principios rectores de las Naciones Unidas, el Convenio n.o 108 del Consejo de Europa y su Protocolo adicional, las Directrices de la OCDE y el proyecto de Decisión marco del Consejo, así como la Directiva 95/46/CE ([20]). Todos estos instrumentos contienen principios similares que gozan de un reconocimiento más amplio que los principios básicos de la protección de datos personales.

54. Las repercusiones que podría tener un acuerdo como el previsto en el informe del Grupo de Contacto hacen que resulte especialmente importante tener debidamente en cuenta los principios antes mencionados. Un instrumento relativo a la totalidad del sector *policial* de un país tercero sería, en efecto, un caso sin precedentes. Las decisiones sobre la adecuación de la protección de datos adoptadas en el marco del primer pilar y los acuerdos celebrados con países tercer en marco del tercer pilar de la UE (Europol, Eurojust) siempre han estado ligados a una transferencia específica de datos, mientras que ahora podrían resultar factibles transferencias de mucho mayor alcance, dado que se persiguen unos fines muy generales (combatir la delincuencia, garantizar la seguridad pública, la seguridad nacional, y el control de fronteras) y que se desconoce el número de bases de datos que se verían afectadas.

Requisitos básicos

55. Las condiciones que deben cumplirse cuando se transfieren datos personales a países terceros se han formulado en un documento del Grupo de Trabajo del Artículo 29 ([21]). Cualquier acuerdo sobre principios mínimos de respeto de la vida privada debe superar una prueba de adecuación que garantice la efectividad de las salvaguardias de protección de datos.

— Por lo que respecta a las normas sustantivas: los principios de protección de datos deben garantizar un nivel elevado de protección y ser acordes con los principios de la UE. Los doce principios incluidos en el informe del Grupo de Contacto se analizan con mayor detenimiento desde esta perspectiva en la sección V del presente dictamen.

— Por lo que respecta a la especificidad: las normas y procedimientos deben formularse con suficiente detalle para permitir su aplicación efectiva y en función de la naturaleza del acuerdo, sobre todo si se trata de un acuerdo internacional oficial.

— Por lo que respecta al control: a fin de garantizar el cumplimiento de las normas acordadas, deben establecerse mecanismos de control específicos, tanto a nivel interno (auditorías) como externo (inspecciones). Las dos partes del acuerdo deben tener idénticas posibilidades de aplicar estos mecanismos. El control incluye mecanismos para garantizar el cumplimiento a escala general (como mecanismos de inspección conjunta) y particular (como la tutela efectiva de los derechos de las personas).

56. Además de estos tres requisitos básicos, habría que prestar especial atención a los aspectos específicos del tratamiento de datos personales en el contexto policial. En efecto, se trata de un ámbito en el que los derechos fundamentales pueden sufrir restricciones, por lo que deben adoptarse salvaguardias para compensar las restricciones de los derechos de los particulares, sobre todo en lo que se refiere a los siguientes aspectos, dadas sus repercusiones en las personas:

— Transparencia: la información y el acceso a los datos personales pueden verse limitados en un contexto policial, debido, por ejemplo, a las necesidades confidencialidad de las investigaciones. En el marco de la UE, suelen instaurarse mecanismos adicionales para compensar esta limitación de los derechos fundamentales (a menudo mediante la intervención de autoridades independientes de protección de datos), pero debe garantizarse que tales mecanismos de compensación sigan existiendo una vez que la información se transfiere a un país tercero.

— Tutela de los derechos: por las razones antes mencionadas, las personas deben disponer de posibilidades alternativas de defensa de sus derechos, en particular mediante la intervención de autoridades de supervisión independientes y de órganos jurisdiccionales.

— Conservación de datos: la justificación del periodo de conservación de los datos puede no ser transparente. Deben tomarse medidas para que ello no impida el ejercicio efectivo de los derechos del titular de los datos o de las autoridades de supervisión.

([20]) — Principios rectores de las Naciones Unidas sobre la reglamentación de los ficheros computadorizados de datos personales, adoptados por la Asamblea General el 14 de diciembre de 1990 (pueden consultarse en inglés en www.unhchr.ch/html/menu3/b/71.htm).
— Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981 (puede consultarse en http://www.boe.es/boe/dias/1985/11/15/pdfs/A36000-36004.pdf).
— Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales, adoptadas el 23 de septiembre de 1980 (pueden consultarse en www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html).
— Proyecto de Decisión marco del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (puede consultarse en http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=es&DosId=193371).
— Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31).

([21]) Documento de trabajo del 24 de julio de 1998 sobre las transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE (doc. WP 12).

— Rendición de cuentas de las autoridades policiales: cuando no existe una transparencia efectiva, los mecanismos de control ofrecidos a las personas o a las instituciones interesadas no pueden aplicarse de manera exhaustiva. Sin embargo, sigue siendo crucial que tales controles estén firmemente establecidos, dado que se trata de datos especialmente protegidos y que su tratamiento puede dar lugar a la aplicación de medidas coercitivas. La rendición de cuentas es una cuestión decisiva en lo que respecta a los mecanismos nacionales de control del país receptor de los datos, pero también en lo que respecta a las posibilidades de inspección por parte del país o región de origen de los datos. Estos mecanismos de inspección están previstos en acuerdos específicos como el acuerdo PNR, y el SEPD recomienda encarecidamente que se incluyan también en el instrumento general.

V. **ANÁLISIS DE LOS PRINCIPIOS**

Introducción

57. En la presente sección se analizan los doce principios mencionados en el documento del Grupo de Contacto desde la siguiente perspectiva:

— Estos principios muestran cierta convergencia entre Estados Unidos y la UE: se observan similitudes con los principios del Convenio nº 108.

— Sin embargo, un acuerdo sobre los principios no es suficiente: un instrumento jurídico debe establecer mecanismos lo suficientemente fuertes para garantizar el cumplimiento.

— El SEPD lamenta que los principios no vayan acompañados de una exposición de motivos.

— Debe quedar claro, antes de entrar en la descripción de los principios, que ambas partes interpretan de la misma manera los términos empleados, por ejemplo los conceptos de información personal o de personas protegidas. En este sentido, sería de agradecer la presencia de definiciones.

1. Especificación de la finalidad

58. El primer principio de la lista del anexo al informe del Grupo de Contacto indica que el tratamiento de información personal se efectuará para fines policiales legítimos. Como se ha mencionado antes, se trata, para la Unión Europea, de la prevención, descubrimiento, investigación o persecución de infracciones penales. En la interpretación de Estados Unidos, en cambio, la finalidad policial va más allá de las infracciones penales e incluye «el control de fronteras, la seguridad pública y la seguridad nacional». La consecuencia de esta discrepancia entre los fines declarados por la UE y Estados Unidos no está clara. Si bien el informe indica que, en la práctica, la finalidad perseguida puede coincidir en gran medida, sigue siendo crucial saber con precisión en qué medida *no* hay coincidencia. En el ámbito policial, por la forma en que las medidas adoptadas repercuten en las personas, el principio de la limitación a una finalidad específica debe cumplirse rigurosamente y la finalidad declarada debe estar clara y circunscrita. Teniendo en cuenta la reciprocidad prevista en el informe, la aproximación de los fines perseguidos parece también esencial. En otras palabras, es necesario aclarar la interpretación de este principio.

2. Integridad y calidad de los datos

59. El SEPD considera muy oportuna la disposición que exige que la información personal sea exacta, pertinente, oportuna y completa, según las exigencias del tratamiento legítimo. Este principio es una condición fundamental de cualquier operación legítima de tratamiento de datos.

3. Necesidad y proporcionalidad

60. Este principio establece un nexo claro entre la información recopilada y la necesidad de disponer de ella para efectuar una labor policial estipulada por la ley. La exigencia de contar con una base jurídica es un elemento positivo para determinar la legitimidad del tratamiento de los datos. El SEPD observa, no obstante, que aunque tal principio refuerza la seguridad jurídica del tratamiento, la base jurídica del tratamiento de los datos es la legislación de un país tercero. La legislación de un país tercero no puede, en sí misma, constituir una base legítima para una transferencia de datos personales ([22]). En el contexto del informe del Grupo de Contacto, todo indica que se parte, en principio, del reconocimiento de la legitimidad de la legislación de un país tercero, en este caso Estados Unidos. Debe tenerse presente que, aunque tal razonamiento puede justificarse en este caso, considerando que Estados Unidos es un país democrático, no es válido ni puede calcarse sin más en las relaciones con cualquier otro país tercero.

61. Según consta en el anexo del informe del Grupo de Contacto, toda transferencia de datos personales debe ser pertinente, necesaria y apropiada. El SEPD destaca que, para ser proporcionado, el tratamiento no debe suponer una intrusión indebida, y que las modalidades del tratamiento deben ser equilibradas, teniendo en cuenta los derechos e intereses de los titulares de los datos.

62. Por esta razón, el acceso a la información debe quedar autorizado en función de las circunstancias de cada caso y de las necesidades prácticas de una investigación concreta. El acceso permanente de las autoridades policiales de un país tercero a bases de datos situadas en la UE debe considerarse desproporcionado e insuficientemente justificado. El SEPD recuerda que incluso los acuerdos de intercambio de datos existentes, por ejemplo el

([22]) Véase, en particular, el artículo 7, letras c) y e), de la Directiva 95/46/CE. En su dictamen 6/2002 del 24 de octubre de 2002, relativo a la transmisión de listas de pasajeros y otros datos de compañías aéreas a los Estados Unidos, el Grupo del Artículo 29 indicó que «no parece aceptable que una decisión unilateral, tomada por un tercer país por motivos que tan solo obedecen a sus propios intereses públicos, lleve a efectuar de manera periódica y sistemática las transferencias de datos protegidos mediante la Directiva».

acuerdo PNR, prevén que el intercambio debe obedecer a circunstancias específicas, y se celebran por un periodo de tiempo limitado ([23]).

63. Siguiendo la misma lógica, debe regularse el periodo de conservación de los datos: estos deben conservarse sólo mientras sean necesarios para la finalidad específica que se persiga. Si dejan de ser pertinentes para ese fin, deben suprimirse. El SEPD se opone firmemente a que se constituyan almacenes de datos para conservar información acerca de personas sobre las cuales no exista ninguna sospecha por si sus datos pudieran resultar necesarios más adelante.

4. Seguridad de la información

64. El SEPD considera satisfactorio que en los principios enumerados en el informe se mencionen medidas y procedimientos para evitar que los datos se empleen o se alteren indebidamente, y para protegerlos de otros riesgos, así como una disposición destinada a limitar el acceso a los datos a las personas autorizadas.

65. Este principio podría completarse con una disposición que estipule que deben llevarse registros de todas las personas que accedan a los datos, ya que ello daría mayor eficacia a las salvaguardias sobre limitación del acceso a los datos y evitaría la utilización indebida de estos.

66. Por otra parte, debe preverse una obligación de información mutua en caso de vulneración de las normas de seguridad: los organismos receptores de los datos tanto en Estados Unidos como en la UE serían responsables de informar a sus homólogos si los datos que han recibido son divulgados ilegalmente. Con ello se contribuirá a que las partes se responsabilicen en mayor medida de lograr que el tratamiento de los datos se efectúe en condiciones de seguridad.

5. Categorías especiales de datos personales

67. El SEPD considera que la excepción que permite efectuar cualquier operación de tratamiento de datos especialmente protegidos siempre y cuando la legislación nacional establezca «salvaguardias apropiadas» supone un importante menoscabo del principio de prohibición del tratamiento de este tipo de datos. Precisamente por la protección especial de que gozan estos datos, cualquier excepción al principio de prohibición debe justificarse adecuadamente y con precisión, indicándose una lista de fines y circunstancias en relación con los cuales un tipo determinado de datos especialmente protegidos pueda ser objeto de tratamiento, y precisándose la condición de los responsables del tratamiento que están autorizados para efectuar el tratamiento de tales datos. Entre las salvaguardias que deben adoptarse, el SEPD considera que los datos especialmente protegidos no deben constituir como tales un elemento que pueda desencadenar una investigación. Podrían estar disponibles en determinadas circunstancias, pero sólo como información adicional sobre una persona que ya esté siendo investigada. Estas salvaguardias y condiciones deben enumerarse exhaustivamente en el texto de este principio.

6. Rendición de cuentas

68. Como se ha indicado en los apartados 55 y 56 del presente dictamen, debe garantizarse efectivamente que las entidades públicas que traten datos personales estén obligadas a rendir cuentas de sus actos, y el acuerdo debe contener garantías acerca de la forma en que se asegurará esta rendición de cuentas. Este aspecto es especialmente importante dada la opacidad que suele ir asociada al tratamiento de datos personales en el contexto policial. En este sentido, mencionar — como se hace en el anexo del informe — que las entidades públicas deberán rendir cuentas de sus actos sin dar más explicaciones sobre las modalidades y consecuencias de la rendición de cuentas no resulta una garantía satisfactoria. El SEPD recomienda que tal explicación figure en el texto del instrumento.

7. Supervisión independiente y efectiva

69. El SEPD es firme partidario de la inclusión de una disposición que ordene una supervisión independiente y efectiva a cargo de una o varias autoridades públicas de supervisión. Considera que debe aclararse la interpretación del concepto de independencia, en particular de quién son independientes estas autoridades y ante quién deben rendir cuentas. Es preciso a este respecto establecer criterios que tengan en cuenta los aspectos de independencia institucional y funcional, en relación con los poderes ejecutivo y legislativo. El SEPD recuerda que se trata de un elemento indispensable para garantizar el cumplimiento efectivo de los principios acordados. Las atribuciones de intervención y coerción de estas autoridades también revisten gran importancia, a efectos de la cuestión ya mencionada de la rendición de cuentas de las entidades públicas que tratan datos personales. Para que los ciudadanos puedan ejercer sus derechos, es preciso que se les informe claramente de la existencia y las competencias de las autoridades de supervisión, en especial si existen varias autoridades competentes en función del contexto del tratamiento de datos.

70. Por otra parte, el SEPD recomienda que el posible acuerdo futuro prevea también mecanismos de cooperación entre las autoridades de supervisión.

8. Acceso individual y rectificación

71. En el contexto policial, el derecho de acceso a los datos y de rectificación de estos requieren garantías específicas. En este sentido, el SEPD se congratula de que se mencione en el informe el principio de que «se dará/debe darse al interesado acceso a sus datos personales y los medios para obtener la rectificación o la supresión de sus datos personales». Sin embargo, subsisten ciertas ambigüedades por lo que respecta a la definición de «los interesados» (todos los titulares de datos deben estar protegidos, y no sólo los ciudadanos del país de que se trate) y a las condiciones en que los interesados podrán oponerse

([23]) El acuerdo caducará y dejará de surtir efecto a los siete años de su firma, a menos que las partes convengan en sustituirlo por otro.

al tratamiento de sus datos. Es necesario precisar los «casos oportunos» en que el interesado estará facultado o no para oponerse al tratamiento. Debe indicarse con claridad en qué circunstancias podrá el interesado ejercer sus derechos (en función, por ejemplo, del tipo de autoridad, del tipo de investigación o de otros criterios).

72. Por otra parte, si no hay posibilidad directa de oponerse al tratamiento de los datos por razones justificadas, debe existir un mecanismo indirecto de verificación, a través de la autoridad independiente responsable de la supervisión del tratamiento de datos.

9. Transparencia y notificación

73. El SEPD destaca una vez más la importancia de la transparencia efectiva, a fin de que los interesados puedan ejercer sus derechos y para contribuir a la obligación general de las autoridades públicas que tratan datos personales de rendir cuentas de sus actos. Apoya la formulación dada a este principio, e insiste en particular en la necesidad de que se dé al interesado una notificación general y personal. Así se refleja en el texto del principio 9 del anexo del informe.

74. Sin embargo, en el capítulo 2 del informe, epígrafe B («Principios acordados»), se indica que en Estados Unidos la transparencia puede plasmarse «en todas o alguna de las opciones siguientes: la publicación en el Registro Federal, la notificación personal y la comunicación en un procedimiento judicial». Debe quedar claro que una publicación en un boletín oficial no basta *per se* para garantizar la adecuada información del interesado. Además de la necesidad de una notificación personal, el SEPD recuerda que es preciso que la información se facilite de modo y manera que resulte fácilmente comprensible para el interesado.

10. Tutela de los derechos

75. Para garantizar que los interesados puedan ejercer efectivamente sus derechos, es preciso que puedan presentar una reclamación ante una autoridad independiente de protección de datos, además de poder interponer un recurso ante un órgano judicial independiente e imparcial. Es necesario que se les ofrezcan ambas posibilidades de tutela de sus derechos.

76. El acceso a una autoridad independiente de protección de datos es necesario porque permite obtener una ayuda flexible y menos costosa en un contexto (el policial) que puede resultar bastante opaco para el particular. Las autoridades de protección de datos también pueden ofrecerle otra ayuda ejerciendo los derechos de acceso en nombre del interesado, cuando las excepciones previstas impidan a éste acceder directamente a sus datos personales.

77. El acceso al sistema judicial es una garantía adicional e indispensable de tutela de los derechos del interesado por una autoridad del sistema democrático distinta de las instituciones públicas que realizan el tratamiento de sus datos. El Tribunal de Justicia de las Comunidades Europeas ha dictaminado que la existencia de una vía de recurso efectiva de carácter jurisdiccional es «esencial para garantizar al particular la protección efectiva de su derecho (…) [y] constituye un principio general de Derecho comunitario que se deriva de las tradiciones constitucionales comunes a los Estados miembros y que se ve sancionada en los artículos 6 y 13 del Convenio Europeo de los Derechos Humanos» ([24]). La existencia de una vía de recurso judicial también está expresamente prevista en el artículo 47 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 22 de la Directiva 95/46/CE, sin perjuicio de los recursos de carácter administrativo.

11. Decisiones individuales automatizadas

78. El SEPD considera muy oportuna la disposición que prevé salvaguardias adecuadas en caso de tratamiento automatizado de datos personales. Observa que sería de agradecer una interpretación común de lo que se entiende por «un acto que produzca un perjuicio significativo para los intereses del titular de los datos», a fin de aclarar las condiciones de aplicación de este principio.

12. Transferencias ulteriores de los datos recibidos a otros países terceros

79. Algunas de las condiciones establecidas para las transferencias ulteriores a otros países terceros no están muy claras. En particular, en los que respecta a las transferencias sujetas a convenios y acuerdos internacionales celebrados entre el país que envía los datos y el que los recibe, es preciso especificar si se trata de acuerdos entre los dos países que efectuaron la primera transferencia, o entre los que realizan la transferencia ulterior. A juicio del SEPD, es necesario en todo caso que los dos países que efectúan la primera transferencia hayan llegado a un acuerdo.

80. El SEPD también observa que el concepto de «intereses públicos legítimos» se ha definido de forma muy general y autoriza la transferencia ulterior de los datos recibidos. El alcance del concepto de seguridad pública queda poco claro; además, la ampliación de las transferencias en caso de incumplimiento de los principios éticos o de las condiciones aplicables a las profesiones reguladas no está justificado y resulta excesivo en un contexto policial.

VI. **CONCLUSIÓN**

81. El SEPD se congratula de la labor conjunta realizada por las autoridades estadounidenses y de la UE sobre las transferencias de datos en el ámbito policial, donde la protección de datos es fundamental. Desea insistir, no obstante, en que la complejidad de esta cuestión, en particular por lo que respecta a su alcance y naturaleza concretos, hacen necesario un análisis cuidadoso y en profundidad. Las

([24]) Asunto 222/84, *Johnston*, Rec. 1986, p. 1651; asunto 222/86, *Heylens*, Rec. 1987, p. 4097; asunto C-97/91, *Borelli*, Rec. 1992, p. I-6313.

repercusiones de un instrumento transatlántico de protección de datos deben examinarse con detenimiento en relación con el marco jurídico existente y sus posibles consecuencias en los ciudadanos.

82. El SEPD pide mayor claridad y disposiciones concretas en especial sobre los aspectos siguientes:

— Aclaración de la naturaleza del instrumento, que debería ser jurídicamente vinculante a fin de garantizar una seguridad jurídica suficiente.

— Una evaluación concreta de la adecuación , a partir de los requisitos esenciales aplicables a los aspectos sustantivos, específicos y de supervisión del sistema. A juicio del SEPD, sólo puede considerarse que el instrumento general sea adecuado si se combina con acuerdos específicos adecuados que atiendan a las circunstancias de cada caso.

— Delimitación del ámbito de aplicación, con una definición clara y común de los fines policiales que se persiguen.

— Precisiones sobre las modalidades según las cuales las entidades privadas pueden participar en los sistemas de transferencia de datos.

— Cumplimiento del principio de proporcionalidad, que supone que los intercambios de datos se realicen atendiendo a las circunstancias de cada caso y cuando exista una necesidad concreta.

— Mecanismos rigurosos de supervisión, y mecanismos de tutela de derechos al alcance de todos los titulares de datos, incluidos los recursos tanto administrativos como judiciales.

— Medidas que garanticen efectivamente el ejercicio de los derechos de todos los titulares de datos, con independencia de su nacionalidad.

— Participación de autoridades independientes de protección de datos, especialmente en relación con la supervisión y la asistencia a los titulares de datos.

83. El SEPD insiste en la necesidad de evitar toda precipitación en la elaboración de los principios, ya que sólo dará lugar a soluciones insatisfactorias, con efectos contrarios a los deseados en materia de protección de datos. La mejor forma de continuar los trabajos en esta fase consistiría pues en elaborar un plan de trabajo para llegar a un posible acuerdo más adelante.

84. El SEPD pide asimismo más transparencia en el proceso de elaboración de los principios de protección de datos. Sólo si se recaba la participación de todas las partes, incluido el Parlamento Europeo, se conseguirá que el instrumento sea objeto de un debate democrático y goce del apoyo y el reconocimiento necesarios.

Hecho en Bruselas, el 11 de noviembre de 2008.

Peter HUSTINX

Supervisor Europeo de Protección de Datos