

I

(Resoluciones, recomendaciones, orientaciones y dictámenes)

DICTÁMENES

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Tercer Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta 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

(2007/C 139/01)

EL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS,

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

Vista la Carta de los Derechos Fundamentales de la Unión Europea y, 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 ⁽¹⁾,

Visto el Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos ⁽²⁾ 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

1. El 19 de diciembre de 2005 y el 29 de noviembre de 2006, el SEPD emitió dos dictámenes ⁽³⁾ sobre la propuesta 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, presentada por la Comisión. En estos dictámenes se subrayaba la importancia de la propuesta como instrumento eficaz para la protección de datos personales en el ámbito cubierto por el título VI del Tratado UE. En el segundo, concretamente, el SEPD manifestaba su preocupación ante el hecho de que las negociaciones estuvieran evolucionando hacia un nivel de protección de los datos personales que no sólo era inferior a los criterios establecidos en la Directiva 95/46/CE, sino también incompatible con la formulación más general del Convenio 108 del Consejo de Europa ⁽⁴⁾.
2. En enero de 2007, la Presidencia alemana formuló una serie de elementos fundamentales para revisar la propuesta, con el fin de eliminar las reservas pendientes y mejorar la protección de datos del tercer pilar ⁽⁵⁾. El proyecto de propuesta revisada ⁽⁶⁾ se presentó al Parlamento Europeo en una segunda consulta el 13 de abril de 2007.

⁽¹⁾ DO L 281 de 23.11.1995, p. 31.

⁽²⁾ DO L 8 de 12.1.2001, p. 1.

⁽³⁾ El primero de ellos está en el JO C 47 du 25.2.2006, p. 27; el segundo, en el sitio internet del SEPD (www.edps.europa.eu).

⁽⁴⁾ Convención para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, del Consejo de Europa, 28 de enero de 1981.

⁽⁵⁾ Documento del Consejo 5435/07, de 18 de enero de 2007; puede consultarse en register.consilium.europa.eu.

⁽⁶⁾ Documento del Consejo 7315/07, de 13 de marzo de 2007; puede consultarse en register.consilium.europa.eu.

3. Tanto los cambios de fondo que contiene la propuesta revisada como la importancia de la misma requieren un nuevo dictamen del SEPD. Este dictamen se centrará en los principales motivos de inquietud del SEPD y no volverá sobre las observaciones formuladas en los dictámenes anteriores, ya que estas siguen siendo válidas para la propuesta revisada.

II. NUEVO IMPULSO DE LA PRESIDENCIA ALEMANA

4. El SEPD celebra que la Presidencia alemana esté dedicando un gran esfuerzo a las negociaciones de esta Decisión Marco del Consejo. Es bien sabido que las negociaciones se vieron bloqueadas en el Consejo, debido a diferencias fundamentales de opinión entre los Estados miembros sobre cuestiones clave. Por ello, la Presidencia ha tomado una decisión acertada al imprimir a estas negociaciones un impulso renovado presentando un texto nuevo.
5. El que la Presidencia alemana haya dado un nuevo impulso a las negociaciones es en sí algo muy positivo. Sin embargo, tras estudiar exhaustivamente el texto más reciente, el SEPD no está satisfecho con el contenido. En efecto, el texto presentado por la Presidencia alemana no está a la altura de las expectativas, y ello por los motivos siguientes:
 - El texto disminuye la protección del ciudadano, ya que se han suprimido de él una serie de disposiciones fundamentales para esta protección que figuraban en la propuesta de la Comisión.
 - En muchos aspectos, la propuesta revisada queda incluso por debajo del nivel de protección establecido en el Convenio 108. Por lo tanto, no es satisfactorio e incluso resultará incompatible con las obligaciones internacionales de los Estados miembros.
 - El texto aumenta la complejidad de este asunto, ya que cubre el tratamiento de datos que realicen Europol, Eurojust y el Sistema de Información Aduanero del tercer pilar, y abre el debate sobre la supervisión de estos organismos. En concreto, el presente dictamen tratará de si una Decisión Marco del Consejo es un instrumento jurídico adecuado para estos temas.
 - La calidad legislativa del texto deja que desear. Aparte del tipo de instrumento jurídico elegido, varias disposiciones incumplen las normas de las directrices comunes sobre la calidad de la redacción de la legislación comunitaria ⁽⁷⁾. En concreto, el texto no está redactado de manera clara, sencilla y precisa, lo que hace difícil para los ciudadanos el determinar sus derechos y obligaciones inequívocamente.
 - La escasa protección que ofrece esta propuesta no puede contribuir adecuadamente a la creación de un espacio de libertad, seguridad y justicia en el que la policía y las autoridades judiciales puedan intercambiar información sobre la aplicación de la ley con independencia de las fronteras nacionales. De hecho, a falta de un nivel de protección de datos que sea elevado y aplicable en general, la propuesta sigue sometiendo los intercambios de información a distintas «normas de origen» y «estándares dobles» nacionales que repercuten de manera importante en la eficiencia de la cooperación para la aplicación de la ley sin mejorar la protección de los datos personales ⁽⁸⁾.
6. El SEPD es bien consciente de lo difícil que resulta llegar a la unanimidad en el Consejo. Sin embargo, el procedimiento de toma de decisiones no puede justificar el que se adopte un planteamiento de mínimo común denominador que iría en menoscabo de los derechos fundamentales de los ciudadanos de la UE y restaría eficiencia a la aplicación de la ley. En este sentido, sería de desear que la experiencia en protección de datos se tomara plenamente en consideración y que se integraran debidamente las recomendaciones formuladas por el Parlamento Europeo en sus resoluciones ⁽⁹⁾.

⁽⁷⁾ Acuerdo interinstitucional de 22 de diciembre de 1998 relativo a las directrices comunes sobre la calidad de la redacción de la legislación comunitaria (DO C 73 de 17.3.1999, p. 1). En el capítulo V del presente dictamen pueden encontrarse ejemplos de ello.

⁽⁸⁾ Véase, por ejemplo, el artículo 14, relativo a las transferencias a autoridades competentes de terceros países o a organismos internacionales; el artículo 12.1.d), relativo al tratamiento posterior de datos personales; el artículo 10, relativo al respeto de los plazos de supresión y comprobación; y el artículo 13, relativo al cumplimiento de las restricciones nacionales de tratamiento.

⁽⁹⁾ El Parlamento Europeo adoptó su primera resolución sobre la propuesta inicial de la Comisión el 27 de septiembre de 2006. Está prevista una segunda resolución, sobre la propuesta revisada, para junio.

III. MARCO JURÍDICO Y OBJETIVO DEL PRESENTE DICTAMEN

7. Una Decisión Marco sobre la protección de datos personales en el tercer pilar es un elemento fundamental para el desarrollo de un espacio de libertad, seguridad y justicia. La creciente importancia que está adquiriendo la cooperación policial y judicial en asuntos penales, así como las actuaciones derivadas del Programa de La Haya ⁽¹⁰⁾, han puesto de manifiesto la necesidad de adoptar criterios comunes para la protección de datos en el tercer pilar.
8. Por desgracia, tal como ha afirmado reiteradamente el SEPD así como otros interesados competentes ⁽¹¹⁾, los instrumentos existentes de rango europeo son insuficientes. El Convenio 108 del Consejo de Europa, que es vinculante para los Estados miembros, establece principios fundamentales generales sobre la protección de datos, pero aun cuando ha de interpretarse a la luz de la jurisprudencia del Tribunal Europeo de Derechos Humanos, no otorga la precisión necesaria, cosa que el SEPD ha afirmado ya en varias ocasiones ⁽¹²⁾. La Directiva 95/46/CE, que integraba y especificaba los principios del Convenio 108 respecto del mercado interior, se adoptó ya en 1995. Esta Directiva no se aplica a las actividades que entran en el ámbito de aplicación del tercer pilar. Para las actividades del ámbito de la cooperación policial y judicial, todos los Estados miembros han suscrito la Recomendación n° R (87) 15 ⁽¹³⁾, que especifica hasta cierto punto el Convenio 108 para el sector policial, pero este no es un instrumento jurídico vinculante.
9. En este contexto, el artículo 30.1.b) del TUE establece que las actuaciones comunes en el ámbito de la cooperación policial que supongan el tratamiento de información por parte de servicios con funciones coercitivas estén sujetas «a las disposiciones correspondientes en materia de protección de datos personales». A falta de una Decisión Marco del Consejo con un contenido satisfactorio, tales disposiciones no existen.
10. Puede establecerse fácilmente un paralelismo con el desarrollo del mercado interior, ámbito en el que se consideró que un elevado nivel de protección de los datos personales en toda la Comunidad era un elemento fundamental para eliminar los obstáculos a la libre circulación de bienes, servicios, capitales y personas, lo que llevó a la adopción de la Directiva 95/46/CE. Por analogía, un espacio de libertad, seguridad y justicia en el que la información circule libremente entre las autoridades encargadas del cumplimiento de la ley, tanto en el plano nacional como en el de la Unión Europea, requiere un nivel de protección de los datos personales que sea elevado y uniforme en todos los Estados miembros.
11. Todo esto contrasta con la situación actual, en la que no existe tal marco general, sino que las disposiciones sobre la protección de los datos personales en el tercer pilar son específicas a este sector y se hallan dispersas en distintos instrumentos jurídicos ⁽¹⁴⁾. Algunas propuestas recientes ⁽¹⁵⁾ confirman y potencian la fragmentación ya existente de las disposiciones sobre protección de datos en este ámbito y hacen peligrar su coherencia. Por otra parte, la falta de un marco general afecta a la rapidez de la adopción de muchas propuestas en el ámbito de la cooperación policial y judicial.
12. Por estos motivos, el SEPD ha respaldado decididamente en sus dictámenes anteriores la propuesta de la Comisión y ha formulado recomendaciones pertinentes para mejorar una propuesta que resultaba necesaria para garantizar un nivel adecuado de protección del ciudadano. El SEPD ha sostenido reiteradamente que un marco general para la protección de datos en el tercer pilar ha de garantizar un nivel de protección elevado y coherente, aprovechando los principios establecidos en el Convenio 108 y en la Directiva 95/46/CE, y teniendo en cuenta asimismo, cuando proceda, la especificidad de las actividades de aplicación de la ley.
13. La coherencia de este marco general con los principios de protección de datos del primer pilar es tanto más importante en un contexto en el que la participación creciente del sector privado en la aplicación de la ley supone que los datos personales pasan del primer al tercer pilar (como ocurre en el caso del

⁽¹⁰⁾ Véase asimismo el Plan de Acción del Consejo y de la Comisión por el que se aplica el Programa de La Haya sobre el refuerzo de la libertad, la seguridad y la justicia en la Unión Europea (DO C 198 de 12.8.2005, p. 1).

⁽¹¹⁾ El 24 de enero de 2006, la Conferencia de Primavera de las Autoridades Europeas de Protección de Datos emitió un dictamen, que puede consultarse en register.consilium.europa.eu con la signatura 6329/06. El Comité Consultivo del Consejo de Europa para el Convenio Europeo para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, adoptó el 20 de marzo de 2007 un documento en el que se exponen sus observaciones iniciales; este documento está en www.coe.int/dataprotection/.

⁽¹²⁾ La más reciente de ellas, en el dictamen del SEPD de 4 de abril de 2007 sobre la Iniciativa de quince Estados miembros con vistas a la adopción de una Decisión del Consejo sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, punto 60.

⁽¹³⁾ Recomendación n° R (87) 15 del Comité de Ministros a los Estados miembros, dirigida a regular la utilización de datos de carácter personal en el sector de la policía, adoptada el 17 de septiembre de 1987; puede consultarse en www.coe.int/dataprotection/.

⁽¹⁴⁾ Como, por ejemplo, los instrumentos jurídicos que regulan Europol, Eurojust y el Sistema de Información Aduanera del tercer pilar.

⁽¹⁵⁾ Tales como las iniciativas recientes sobre Europol, el Tratado de Prüm y el acceso a la base de datos VIS por parte de las autoridades de aplicación de la ley.

registro de nombres de los pasajeros, o PNR), o bien del tercero al primero. Ejemplos pertinentes pueden encontrarse fácilmente: la utilización de listas de exclusión con personas a las que no debería permitirse entrar en los aviones, listas elaboradas por las compañías aéreas para las autoridades de aplicación de la ley, a efectos del primer pilar (con fines comerciales así como por motivos de seguridad aérea), así como la propuesta sobre el acceso para las autoridades de aplicación de la ley a la base VIS, creada como instrumento de una política común de visados ⁽¹⁶⁾. En consecuencia, el SEPD recalca que los principios sobre protección de datos del primer pilar deben aplicarse también al tercer pilar. Sin embargo, la especificidad de las actividades de aplicación de la ley pueden hacer necesarias disposiciones complementarias o excepcionales ⁽¹⁷⁾.

14. Es esencial contar con salvaguardas adecuadas, coherentes y aplicables ampliamente a la protección de datos en el tercer pilar, no sólo para garantizar el derecho fundamental a la protección de datos de las personas, sino también para promover la eficiencia de la cooperación en la aplicación de la ley en el espacio de libertad, seguridad y justicia.
15. En este contexto, el presente dictamen evalúa hasta qué punto la propuesta revisada actual establece disposiciones adecuadas sobre la protección de datos personales con arreglo al artículo 30.1.b) del TUE. Al hacerlo, el SEPD remite a algunas de las recomendaciones que hizo en los dictámenes anteriores. En el presente dictamen se evalúa también si la propuesta revisada respeta las obligaciones internacionales que para los Estados miembros derivan del Convenio 108 del Consejo de Europa y de la jurisprudencia del Tribunal Europeo de Derechos Humanos, así como los principios establecidos en la Recomendación n° R (87) 15 sobre la utilización de datos personales en el ámbito policial. Por otra parte, el SEPD estudiará hasta qué punto lo dispuesto en la propuesta repercutirá en la eficiencia de la cooperación policial y judicial.

IV. PRINCIPALES PREOCUPACIONES

IV.1. Aplicabilidad del tratamiento nacional de datos personales

16. La propuesta incluye ahora un considerando en que se afirma que los Estados miembros aplicarán las normas de la Decisión marco a sus sistemas nacionales de tratamiento de datos para que, a la hora de recopilar los datos, se cumplan ya las condiciones de su transmisión (considerando 6 bis). Este considerando trata de atender a las preocupaciones manifestadas no sólo por el SEPD en sus dictámenes anteriores, sino también por muchos otros interesados. De hecho, el Parlamento Europeo, la Conferencia de autoridades de protección de datos, e incluso el Comité Consultivo sobre tratamiento y protección de datos del Consejo de Europa (integrado por representantes de los Gobiernos europeos con competencias en materia de protección de datos), han puesto de manifiesto en varias ocasiones que la aplicabilidad de la Decisión Marco al tratamiento nacional de datos personales es condición esencial no sólo para garantizar una protección suficiente de los datos personales, sino también para hacer posible una cooperación eficaz entre las autoridades policiales ⁽¹⁸⁾
17. Con todo, el considerando como tal no puede imponer una obligación que no esté establecida expresamente en la parte dispositiva. Desgraciadamente, el artículo 1 (Objetivo y ámbito de aplicación) limita explícitamente la aplicabilidad de la propuesta a los datos intercambiados entre los Estados miembros o los organismos de la UE, garantizando «la plena protección de los derechos y libertades fundamentales, y en particular la intimidad, de los interesados cuando los datos personales se transmitan [...]».
18. Por consiguiente, la versión actual del texto otorga plena discreción a los Estados miembros a la hora de aplicar principios uniformes de protección de datos al tratamiento nacional de datos personales y no obliga a los Estados miembros a aplicar las mismas normas comunes de protección de datos, todo ello en un ámbito de cooperación policial y judicial en que deben suprimirse las fronteras. En estas circunstancias, el SEPD vuelve a poner de relieve que la posibilidad de que existan distintos niveles de protección de datos entre los distintos Estados miembros dentro del tercer pilar sería:
 - incoherente con la creación de un espacio de libertad, seguridad y justicia en el que los ciudadanos circulen libremente y con una adecuada aproximación de las legislaciones de conformidad con el artículo 34.2.b) del TUE;
 - inapropiada para la protección de datos personales, habida cuenta del artículo 30.1.b) del TUE;

⁽¹⁶⁾ Véase la propuesta de Decisión del Consejo sobre el acceso para consultar el Sistema de Información de Visados (VIS) por las autoridades de los Estados miembros responsables de la seguridad interior y por Europol, con fines de prevención, detección e investigación de los delitos de terrorismo y otros delitos graves (COM (2005) 600 final).

⁽¹⁷⁾ En este sentido, véase asimismo la exposición de motivos de la Recomendación n° R (87) 15, punto 37.

⁽¹⁸⁾ Véanse los documentos mencionados en la nota 9.

- ineficaz e inviable para las autoridades policiales, para las cuales constituirían una carga indebida las distinciones difíciles de manejar entre los datos nacionales y los datos transmitidos o disponibles para la transmisión, que en la mayoría de los casos formarán parte del mismo expediente ⁽¹⁹⁾;
19. El SEPD aconseja encarecidamente al legislador que amplíe el ámbito de la aplicabilidad, obligando -y no tan sólo invitando- a los Estados miembros a que apliquen la Decisión Marco al tratamiento nacional de los datos personales. Además, no existen argumentos jurídicos de peso para respaldar la opinión según la cual la aplicación a los datos nacionales no estaría autorizada por el artículo 34 del TUE.

IV.2. Limitación de los fines adicionales para los cuales pueden tratarse los datos personales

20. El principio de limitación de los fines es uno de los principios básicos de la protección de datos. En particular, el Convenio 108 establece que los datos de carácter personal «se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades» (artículo 5.b)); Sólo se permiten excepciones a este principio en la medida en que las establezca la ley y constituyan una medida necesaria en una sociedad democrática para, entre otras cosas, «la represión de infracciones penales» (artículo 9). La jurisprudencia del Tribunal Europeo de Derechos Humanos ha enunciado claramente que tales excepciones han de ser proporcionadas, precisas y predecibles, de conformidad con el artículo 8.2 del Convenio Europeo de Derechos Humanos ⁽²⁰⁾
21. En la propuesta actual, las disposiciones relativas a la limitación de los fines se establecen en los artículos 3 y 12. El artículo 3 autoriza el tratamiento adicional con fines compatibles con el fin para el que los datos se recopilaron y está, por lo tanto, en consonancia con los principios básicos de la protección de datos.
22. No obstante, el artículo 3 es excesivamente amplio y no comprende una limitación adecuada de los fines de almacenamiento, como exige también el artículo 5.b) del Convenio 108 anteriormente citado. Los fines del título VI del Tratado UE a que se hace referencia no pueden considerarse como «finalidades determinadas y legítimas». La finalidad de la cooperación policial y judicial no es legítima por naturaleza ⁽²¹⁾ y, desde luego, no es determinada.
23. El artículo 3 no contiene ninguna excepción de las que podría contener de conformidad con el artículo 9 del Convenio 108. Sin embargo, el artículo 12 de la propuesta establece una serie sumamente amplia y no claramente definida de excepciones respecto del principio de limitación de los fines en el contexto de los datos personales recibidos de otro Estado miembro o puesto a disposición por éste. Concretamente, no se establece de forma explícita en este artículo la condición de que serán necesarias unas excepciones. En segundo lugar, no queda claro cuáles son los «otros procedimientos judiciales» respecto de los cuales el artículo 12.1.d autoriza que se traten los datos personales recogidos y transmitidos para un fin distinto. Por otra parte, el artículo 12.1.d autoriza que se traten con «cualquier otro fin», con la única condición de que las autoridades competentes que hayan transmitido los datos personales den su consentimiento. En este contexto, cabe señalar que no podrá considerarse, bajo ningún concepto, que el consentimiento de la autoridad transmisora sustituye el consentimiento del interesado ni que constituye un motivo de derecho para apartarse del principio de limitación de los fines. Por consiguiente, el SEPD hace hincapié en que esta excepción amplia y abierta no satisface los requisitos básicos de una protección de datos adecuada e incluso contradice los principios fundamentales del Convenio 108. Por consiguiente, el SEPD recomienda al legislador que vuelva a redactar las disposiciones pertinentes.
24. Una última observación se refiere al artículo 12.2, que ofrece la posibilidad de que las decisiones del Consejo correspondientes al tercer pilar primen sobre el apartado 1 cuando se hayan previsto las condiciones adecuadas para el tratamiento de los datos personales. El SEPD destaca que la formulación de este apartado es de carácter muy general y no hace justicia a la naturaleza de la Decisión Marco del Consejo en tanto que ley general aplicable a la cooperación policial y judicial. Esta ley general debería aplicarse a todo el tratamiento de datos personales en este ámbito.
25. El SEPD opina que las disposiciones actuales relativas al tratamiento posterior de datos personales afectan al principio fundamental de limitación de los fines e incluso se sitúan por debajo del nivel actual que establece el Convenio 108. Por consiguiente, el SEPD recomienda al legislador que vuelva a redactar las disposiciones pertinentes a la luz de las normas internacionales de protección de datos existentes y de la jurisprudencia pertinente.

⁽¹⁹⁾ Para un razonamiento más pormenorizado, véase el segundo dictamen del SEPD, puntos 11 a 13.

⁽²⁰⁾ Dentro de la jurisprudencia consolidada en este ámbito, el caso más explícito es el de Rotaru contra Rumanía.

⁽²¹⁾ No basta con partir de la premisa de que la policía, en todas las circunstancias y en todos los casos, actúa dentro de los límites de las obligaciones que les marca la ley.

IV.3. Protección adecuada en el intercambio de datos personales con terceros países

26. El Convenio 108 también trata las transferencias a terceros países. El Protocolo adicional relativo a las autoridades de control y los flujos transfronterizos de datos establece el principio general -sujeto a determinadas excepciones- de que se permite la transferencia de datos personales a un país tercero solamente si esa parte garantiza un nivel adecuado de protección para la transferencia considerada. El principio de «protección adecuada» se ha ejecutado y se ha especificado en varios instrumentos jurídicos de la Unión Europea, no sólo en instrumentos del primer pilar sobre protección de datos, como la Directiva 95/46/CE ⁽²²⁾, sino también en instrumentos jurídicos del tercer pilar, como los instrumentos jurídicos por los que se creaban Europol y Eurojust.
27. El considerando 12 de la propuesta actual afirma que, en caso de transferencia de datos personales a terceros países u organismos internacionales, estos datos «deberían, en principio, gozar de un nivel de protección adecuado». Además, el artículo 14 permite que se transfieran datos personales transmitidos de otro Estado miembro a terceros países u organismos internacionales cuando la autoridad que los transmite haya dado su consentimiento a la transferencia de acuerdo con su Derecho nacional. Por lo tanto, las disposiciones de la propuesta no establecen ninguna necesidad de protección adecuada, ni prevén criterio o mecanismo común alguno para evaluar la adecuación. Esto significa que cada Estado miembro evaluará conforme a su propia discreción el nivel de adecuación previsto por el tercer país o el organismo internacional. Por consiguiente, la lista de países y organizaciones internacionales adecuados -a los cuales se permite una transferencia- variará considerablemente de un Estado miembro a otro.
28. Este marco jurídico también obstaculizaría la cooperación policial y judicial. En efecto, las autoridades policiales de un Estado miembro, al decidir sobre una solicitud de un expediente penal determinado presentada por un tercer país, no solamente tendrán que considerar la adecuación de ese país, sino que también habrán de tener en cuenta si cada uno de los demás Estados miembros (hasta 26) que han contribuido al expediente ha dado su consentimiento, con arreglo a su propia evaluación de la adecuación del tercer país de que se trate.
29. A este respecto, el artículo 27 de la propuesta (Relación con acuerdos con terceros Estados) añade más incertidumbre, al estipular que la Decisión Marco no afectará a las obligaciones y compromisos contraídos por los Estados miembros o la UE en virtud de acuerdos bilaterales o multilaterales con terceros Estados. Según el SEPD, esta disposición debería limitarse claramente a los acuerdos vigentes y debería establecer que los futuros acuerdos estén en consonancia con las disposiciones de la presente propuesta.
30. El SEPD cree que las disposiciones actuales sobre transferencias de datos personales a terceros países y organizaciones internacionales no serían adecuadas para proteger los datos personales, ni viables para las autoridades policiales. Por tanto, el SEPD reitera ⁽²³⁾ la necesidad de garantizar un nivel adecuado de protección cuando se transfieran datos personales a terceros países u organizaciones internacionales y que se creen mecanismos que garanticen normas comunes y decisiones coordinadas en relación con las constataciones. Esta misma opinión expresaron con anterioridad el Parlamento Europeo y el Comité sobre tratamiento y protección de datos del Consejo de Europa.

IV.4. Calidad de los datos

31. El artículo 5 del Convenio 108 establece los principios para garantizar la calidad de los datos personales. Más información al respecto figura en otros instrumentos no vinculantes como la Recomendación nº R (87) 15 y en sus tres evaluaciones realizadas hasta la fecha.
32. Al comparar la propuesta actual con los instrumentos jurídicos antes mencionados, se pone claramente de manifiesto que en la versión revisada faltan determinadas garantías importantes, en algunos casos ya previstas en la propuesta de la Comisión:
 - El artículo 3 de la propuesta no garantiza que los datos se obtendrán y tratarán lealmente, como exige el artículo 5 del Convenio 108.

⁽²²⁾ Por lo que se refiere a este punto, cabe señalar que la Comisión ha declarado recientemente, en su *Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el seguimiento del programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos*, que las normas establecidas por la Directiva 95/46/CE en relación con transferencias de datos personales a terceros países son sustancialmente apropiadas y no requieren modificación.

⁽²³⁾ Véanse las inquietudes expresadas en el primer dictamen, apartado IV.8, y en el segundo dictamen, puntos 22 y 23.

- La propuesta ya no incluye ninguna disposición que establezca — tal y como exige el principio 3.2 de la Recomendación nº R (87) 15 — que las diferentes categorías de datos se clasifiquen según su grado de exactitud y fiabilidad, y que los datos basados en hechos se distingan de los basados en opiniones o apreciaciones personales ⁽²⁴⁾. La falta de un requisito común de este tipo podría ir justamente en detrimento de los datos intercambiados entre autoridades policiales, al no poder éstas establecer si los datos pueden entenderse como «prueba», «hecho», «información irrefutable» o «información no probatoria». La consecuencia podría ser no sólo obstaculizar tratamientos de seguridad y recogida de información que se basan en estas distinciones, sino también dificultar a los tribunales la salvaguardia de las condenas.
 - No existe distinción entre diferentes categorías de interesados (delincuentes, sospechosos, víctimas, testigos, etc.) ni garantías específicas para datos relacionados con personas no sospechosas, contrariamente al principio 2 de la Recomendación nº R (87) 15 y sus informes de evaluación ⁽²⁵⁾. De nuevo, estas distinciones no sólo resultan necesarias a efectos de la protección de los datos personales de los ciudadanos, sino también a efectos de la capacidad de los destinatarios para poder utilizar plenamente los datos recibidos. Sin estas distinciones, los servicios policiales destinatarios no pueden utilizar los datos de forma inmediata, sino que primero tienen que determinar la calificación de los datos y, posteriormente, la manera de utilizarlos y compartirlos a efectos de la aplicación de la ley.
 - La comprobación regular prevista en el artículo 6 no garantiza el control regular de la calidad de los datos ni que los expedientes policiales no contengan datos superfluos o inexactos y actualizados, como exige la Recomendación nº R (87) 15 ⁽²⁶⁾. La importancia de dicha comprobación para la protección de datos no sólo es obvia, sino esencial, una vez más, para el tratamiento eficaz de los servicios de policía. La información anticuada y caducada puede, en el mejor de los casos, resultar inútil y, en el peor de los casos, desviar los recursos destinados a las prioridades en curso hacia asuntos que no son ni deben ser el centro de la investigación.
 - En caso de que existan indicios de que los datos personales -transmitidos por otro Estado miembro- son inexactos, no existe obligación ni mecanismos para garantizar su rectificación en el Estado miembro de origen. Una vez más, la cuestión de la exactitud resulta esencial para el trabajo eficaz de la policía y la judicatura. Si no se puede garantizar la calidad de los datos, se perjudicará la utilidad de la transferencia de datos como instrumento para la lucha contra la delincuencia transfronteriza.
33. En estas circunstancias, el SEPD opina que las disposiciones de la propuesta actual relacionadas con la calidad de los datos no son ni adecuadas ni completas, en particular teniendo en cuenta la Recomendación nº R (87) 15 suscrita por todos los Estados miembros, e incluso se sitúan por debajo del nivel de protección exigido por el Convenio 108. Asimismo resulta útil recordar una vez más que la exactitud de los datos personales redundaba en el interés tanto de las propias autoridades policiales como de los particulares ⁽²⁷⁾.

IV.5. Intercambio de datos personales con autoridades no competentes y particulares

34. Según el principio 5 (Comunicación de datos) de la Recomendación nº R (87) 15, la comunicación de datos personales por las autoridades de aplicación de la ley a otros órganos públicos o particulares sólo debería permitirse en condiciones específicas y estrictas. Estas disposiciones, que figuran en la propuesta inicial de la Comisión y que el SEPD y el Parlamento Europeo acogieron favorablemente, han sido suprimidas ahora en la versión revisada. Por ello, el nuevo texto no establece garantías específicas para la transferencia de datos personales a particulares o a autoridades que no sean responsables de la aplicación de la ley.

⁽²⁴⁾ El punto 52 de la exposición de motivos de la Recomendación estipula que se debe poder distinguir entre datos corroborados y no corroborados, incluidas las apreciaciones de comportamiento humano, entre hechos y opiniones, entre información fiable (y sus diversas vertientes) y conjetura, entre causa razonable para creer que la información es exacta y una convicción infundada de su exactitud. Véase también la segunda evaluación de la significación de la Recomendación nº R (87) 15 que regula la utilización de datos personales en el ámbito policial (1998), punto 5.1.

⁽²⁵⁾ Véase, en particular, el punto 5.2 de la segunda evaluación antes mencionada y los puntos 24 a 27 de la tercera evaluación de la Recomendación nº R (87) 15 que regula la utilización de datos personales en el ámbito policial (2002).

⁽²⁶⁾ Véase el principio 7 (período de conservación y actualización de datos) y la exposición de motivos, puntos 96 a 98.

⁽²⁷⁾ Exposición de motivos de la Recomendación nº R (87) 15, punto 74.

35. Además, el acceso y la ulterior utilización por las autoridades de la aplicación de la ley de los datos personales controlados por los particulares se permitirá únicamente sobre la base de unas condiciones y limitaciones bien definidas. En particular, como ya indicó el SEPD en sus anteriores dictámenes, el acceso por las autoridades de aplicación de la ley sólo se autorizará considerando cada caso individual, en determinadas circunstancias y para fines específicos, y estará bajo el control judicial en los Estados miembros. Las últimas novedades, como la Directiva 2006/24/CE ⁽²⁸⁾ sobre la conservación de datos, el acuerdo con los Estados Unidos sobre el registro de nombres de pasajeros (PNR) ⁽²⁹⁾ y el acceso por las autoridades de aplicación de la ley a los datos mantenidos por SWIFT ⁽³⁰⁾ confirman la importancia fundamental que tienen estas garantías. Es de lamentar que en la actual propuesta no se establezcan garantías específicas sobre el acceso y la ulterior utilización por las autoridades de aplicación de la ley de los datos personales recogidos por particulares.
36. En este contexto, el SEPD observa que, por lo se refiere al intercambio de datos personales con particulares y autoridades no competentes, la actual propuesta no cumple los principios de la Recomendación n° R (87) 15 ni aborda la cuestión fundamental del acceso y de la ulterior utilización por las autoridades de aplicación de la ley de los datos personales controlados por particulares.

IV.6. Otros puntos importantes

37. Además de los aspectos principales antes mencionados, el SEPD desea llamar la atención del legislador sobre los puntos que figuran a continuación, y que en la mayoría de los casos ya han sido tratados con mayor detalle en sus anteriores dictámenes.
- **Categorías especiales de datos.** El artículo 7 de la propuesta revisada contradice la prohibición establecida en el artículo 6 del Convenio 108. Además, no hace referencia a los datos personales relativos a las condenas penales, que son indudablemente de gran importancia en el contexto de la cooperación policial y judicial, ni establece salvaguardias específicas con respecto a los datos biométricos y perfiles de ADN.
 - **Decisiones individuales automatizadas.** El SEPD se congratula de que el artículo 8 incorpore esta disposición en la propuesta revisada.
 - **Registro y documentación.** El artículo 11, para ser eficaz a efectos de verificación de la legalidad del tratamiento de datos, debería establecer mecanismos adecuados para registrar o documentar no sólo todas las transmisiones de datos, sino también *todos los accesos* a datos.
 - **Derecho a ser informado.** El artículo 16 es incompleto, ya que no menciona la información acerca de la identidad de la persona responsable de tratamiento y de los destinatarios. Además, el considerando 13 («Podrá requerirse informar a las personas en cuestión del tratamiento de sus datos [...]») habla de la información como de una mera posibilidad, en lugar de una obligación fundamental de la persona responsable del tratamiento.
 - **Derecho de acceso.** El artículo 17 es incompleto, ya que el acceso debería incluir también *los fines* para los que se tratan los datos y la comunicación en una *forma inteligible*. Por otra parte, las excepciones establecidas en el apartado 2 –como el caso de que el acceso «suponga perjuicio para los intereses nacionales»– son demasiado amplias e imprevisibles. Por último, no hay ningún mecanismo que garantice que un recurso presentado ante el organismo de control permita la concesión de acceso cuando éste se haya denegado de forma ilegal.

V. NUEVAS CUESTIONES PLANTEADAS EN LA PROPUESTA REVISADA

38. La propuesta revisada incluye un elemento completamente nuevo con respecto a la propuesta de la Comisión. La propuesta da cabida a actividades de las instituciones y organismos europeos en el tercer pilar (artículo 1.2 de la propuesta). Según el considerando 20, se incluye el tratamiento de datos por Europol, Eurojust y el Sistema de Información Aduanero del tercer pilar. El artículo 1.2 no sólo menciona a los organismos europeos, sino también a las instituciones, lo que significa que, por ejemplo,

⁽²⁸⁾ Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (DO L 105 de 13.4.2006, p. 54).

⁽²⁹⁾ 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 (DO L 298 de 27.10.2006, p. 29).

⁽³⁰⁾ Véase el dictamen del Grupo del artículo 29 sobre el tratamiento de datos personales por parte de la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (Society for Worldwide Interbank Financial Telecommunication — SWIFT), que se puede consultar en http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf, y el dictamen del SEPD sobre el papel del Banco Central Europeo en el asunto SWIFT, disponible en el sitio web del SEPD.

el tratamiento de datos dentro del Consejo debería estar sujeto a la Decisión Marco del Consejo. No está claro si los autores del texto deseaban que el ámbito de aplicación fuera tan amplio, o más bien que se limitara a los tres organismos mencionados en el considerando 20. En cualquier caso, debería aclararse el texto para evitar la incertidumbre jurídica.

39. Esto nos lleva a hacer una observación más general. Según el SEPD, es sumamente importante que se garantice un nivel adecuado de protección de datos en todo el tercer pilar, ya que sólo así se facilitaría de manera suficiente el intercambio de información en un espacio de libertad, seguridad y justicia sin fronteras internas. Ello implica aplicar el marco general sobre la protección de datos a los organismos europeos dentro del tercer pilar. El SEPD puso de relieve esta necesidad en la parte IV de su dictamen sobre la propuesta de una Decisión del Consejo sobre Europol.
40. No obstante, teniendo en cuenta la eficacia de la labor legislativa, el SEPD alberga serias dudas acerca de si la presente Decisión Marco del Consejo debe cubrir o no las actividades de los organismos europeos que actúan en el tercer pilar. El primer argumento en contra de un ámbito de aplicación tan amplio como el indicado guarda relación con la política legislativa. El SEPD teme que la inclusión de los organismos europeos en el texto actual entrañaría el riesgo de que los debates en el Consejo se centren en este nuevo elemento, en lugar de hacerlo en las disposiciones básicas sobre la protección de datos, lo cual complicaría el proceso legislativo. El segundo argumento es de naturaleza jurídica. A primera vista, parece que una Decisión Marco del Consejo -un instrumento que es comparable a una Directiva según el Tratado CE- no es el instrumento jurídico adecuado para reglamentar los derechos y obligaciones de los organismos europeos. El artículo 34 del Tratado UE introduce este instrumento para la aproximación de las disposiciones legales y reglamentarias de los Estados miembros. En cualquier caso, existe el grave riesgo de que la base jurídica se ponga en entredicho durante el proceso legislativo o con posterioridad al mismo.
41. El SEPD comparte un punto de vista similar, también en lo que se refiere al instrumento jurídico elegido, sobre el artículo 26 del proyecto, que prevé el establecimiento de un nuevo órgano común de control que sustituya a las autoridades existentes que supervisan el tratamiento de datos en los organismos del tercer pilar. Considerada en sí misma, la intención de establecer semejante órgano puede parecer lógica, ya que podría llevar a un sistema de supervisión aún más eficaz y, además, garantizar la coherencia del nivel de protección de los organismos establecidos en el tercer pilar.
42. No obstante, en el momento actual no existe la necesidad inmediata de semejante nuevo órgano de control. El control propiamente dicho funciona de modo satisfactorio. Además, el presidente de Eurojust ha hecho algunas objeciones contra la aplicación de este sistema de control a Eurojust. Sin entrar en el fondo de dichas objeciones, está claro que incluir la cuestión del control de los organismos de la UE en la Decisión Marco del Consejo dificultaría aún más el proceso legislativo. Por otra parte, este enfoque no sería coherente con otras propuestas en este ámbito que son actualmente objeto de debate ⁽³¹⁾ o que se han adoptado recientemente ⁽³²⁾.
43. En pocas palabras, el SEPD recomienda que no se incluyan disposiciones sobre tratamiento de datos por los órganos de la UE en el texto de la Decisión marco del Consejo. El SEPD da este consejo por razones de eficacia legislativa. Es importante que todos los esfuerzos que se realicen en el Consejo se concentren en la parte dispositiva de la protección de datos para dar al ciudadano la protección necesaria.

VI. CONCLUSIONES

44. El SEPD acoge con satisfacción el nuevo impulso dado por la Presidencia alemana. La adopción de un marco general para la protección de datos dentro del tercer pilar es esencial, como los SEPD y otros actores pertinentes han destacado ya en varias ocasiones, a fin de apoyar el desarrollo un espacio de libertad, seguridad y justicia en el que el derecho de los ciudadanos a la protección de los datos personales esté garantizado de modo uniforme y la cooperación entre las autoridades policiales pueda tener lugar sin tener en cuenta las fronteras nacionales.
45. Sin embargo, la propuesta revisada tampoco cumple ninguno de estos objetivos. Efectivamente, faltando un nivel elevado y aplicable a nivel general de protección de datos, la propuesta hace que los intercambios de información estén aún sujetos a diversas «normas de origen» y «dobles raseros» nacionales que afectan en grado importante a la eficacia de la cooperación policial sin que la protección de datos personales se vea mejorada.

⁽³¹⁾ Como la reciente propuesta de Comisión sobre la creación de la Oficina Europea de Policía, COM(2006) 817 final.

⁽³²⁾ Reglamento (CE) n° 1987/2006 del Parlamento Europeo y del Consejo de 20 de diciembre de 2006 relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II) (DO L 381 de 28.12.2006, p. 4).

46. Para dar un ejemplo concreto, esto significaría que un órgano policial a nivel nacional o de la UE, al tratar un expediente penal -consistente en información procedente de diversas autoridades, nacionales, de otros Estados miembros y de la UE- tendría que aplicar diversas normas de tratamiento a los diferentes elementos de información, en función de lo siguiente: si se han recabado al nivel nacional o no los datos personales; si cada uno de los organismos que transmiten los datos ha dado su consentimiento para la finalidad prevista; si el almacenamiento cumple los plazos establecidos por las leyes aplicables de cada uno de los organismos transmisores; si ulteriores restricciones al tratamiento pedidas por cada uno de los organismos transmisores no prohíben dicho tratamiento; en caso de solicitud de un tercer país, si de los organismos transmisores ha dado su consentimiento de acuerdo con su propia evaluación de la adecuación y/o de los compromisos internacionales. Además, la protección de los ciudadanos y sus derechos variarán enormemente y estarán sujetos a diversas excepciones generales dependiendo del Estado miembro en que tenga lugar el tratamiento.
47. Además, el SEPD lamenta que la calidad legislativa del texto no sea satisfactoria y que la propuesta añada nuevas complejidades al expediente, al ampliar la aplicabilidad de la Decisión marco a Europol, Eurojust y al Sistema de Información Aduanera del tercer pilar, y también al proponer la creación de un órgano común de control sobre la base de un instrumento jurídico inadecuado.
48. El SEPD expresa su preocupación por el hecho de que el texto actual hace desaparecer disposiciones esenciales para la protección de los datos personales contenidas en la propuesta de la Comisión. De esta manera, debilita perceptiblemente el nivel de protección de los ciudadanos. En primer lugar, no consigue aportar valor añadido al Convenio 108, lo que haría que sus disposiciones fueran apropiadas desde el punto de vista de la protección de los datos, como requiere el artículo 30.1 del TUE. En segundo lugar, tampoco consigue llegar en muchos aspectos al nivel de protección requerido por el Convenio 108. Por lo tanto, el SEPD cree que esta propuesta necesitaría mejoras sustanciales antes de poder servir de base para debatir un marco general adecuado en materia de protección de los datos dentro del tercer pilar. Estas mejoras deberían asegurar que este marco general:
- aporta valor añadido al Convenio 108, estableciendo las disposiciones apropiadas sobre protección de datos personales requeridas por el artículo 30.1 del TUE;
 - es aplicable al tratamiento nacional de datos personales por las autoridades policiales;
 - es coherente con los principios de protección de datos del primer pilar, al tiempo que tiene en cuenta, en caso necesario, las especificidades de las actividades policiales.
 - coincide con los principios establecidos por el Convenio 108 y la Recomendación nº R (87) 15, en especial por lo que se refiere a:
 - la limitación de los fines adicionales para los cuales pueden tratarse los datos personales
 - la calidad de datos, incluida la distinción entre diversas categorías de los afectados por los datos (delincuentes, sospechosos, víctimas, testigos, etc.), la evaluación del diverso grado de exactitud y la fiabilidad de los datos personales, los mecanismos para asegurar la verificación y la rectificación periódicas;
 - las condiciones para las transferencias de datos personales a las autoridades no competentes y a los particulares, así como para el acceso y utilización ulterior de los datos personales controlados por particulares por parte de las autoridades policiales;
 - asegura la protección adecuada en el intercambio de datos personales con terceros países, también por lo que se refiere a acuerdos internacionales;
 - aborda los otros puntos mencionados en el presente dictamen, como en dictámenes anteriores del SEPD.
49. El SEPD es plenamente consciente de las dificultades para alcanzar la unanimidad en el Consejo. Sin embargo, el proceso de toma de decisiones no puede justificar un planteamiento basado en el mínimo común denominador, que pondría trabas a los derechos fundamentales de los ciudadanos de la UE y obstaculizaría la eficacia de la acción policial.

Hecho en Bruselas, el 27 de abril de 2007.

Peter HUSTINX

Supervisor Europeo de Protección de Datos