SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Decisión marco del Consejo sobre el intercambio de información en virtud del principio de disponibilidad (COM(2005) 490 final)

(2006/C 116/04)

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,

Vista la solicitud de dictamen con arreglo al artículo 28.2 del 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,

HA ADOPTADO EL PRESENTE DICTAMEN:

I. CONSIDERACIONES PRELIMINARES

1. La Comisión remitió al SEPD la propuesta de Decisión marco del Consejo sobre el intercambio de información en virtud del principio de disponibilidad mediante carta con fecha de 12 de octubre de 2005. El SEPD entiende que dicha carta constituye una solicitud de consulta de instituciones y organismos comunitarios a tenor del artículo 28.2 del Reglamento (CE) nº 45/2001. El SEPD opina que el presente dictamen debería mencionarse en el preámbulo de la Decisión marco.

2. La naturaleza del presente dictamen ha de entenderse en el contexto descrito en el punto II. Como allí se indica, no existe certeza alguna de que la presente propuesta -o el planteamiento de la disponibilidad que en ella se adoptavayan a tener como resultado la adopción de un instrumento jurídico. Un número considerable de Estados miembros aboga por que se adopten otros planteamientos.

3. En cambio, sí es patente que el tema de la disponibilidad de información policial y judicial a través de las fronteras interiores -o, más ampliamente, el intercambio de esa información- ocupa un lugar importante en la agenda de los Estados miembros, tanto dentro del Consejo como fuera de él, así como en el Parlamento Europeo.

4. Es igualmente patente que este tema tiene gran importancia desde el punto de vista de la protección de datos personales, como demostrará el presente dictamen. El SEPD recuerda que la presente propuesta fue presentada por la Comisión de forma estrechamente vinculada a 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, que fue objeto de un dictamen del SEPD presentado el 19 de diciembre de 2005.

5. El SEPD aprovechará esta ocasión para presentar en su dictamen algunos puntos de vista generales y más fundamentales en cuanto a los temas del intercambio de información policial y judicial y de los planteamientos para la regulación de aquélla. Al presentar el presente dictamen, el SEPD pretende garantizar que en los futuros debates en torno a este tema se tenga debidamente en cuenta la perspectiva de la protección de datos.

6. En una fase ulterior podrán presentarse consultas adicionales al SEPD, en función de la evolución pertinente del proceso legislativo sobre esta propuesta, así como sobre otras propuestas que guarden relación con ella.

II. LA PROPUESTA EN SU CONTEXTO

7. En el Programa de La Haya se introdujo el principio de disponibilidad como principio jurídico nuevo e importante. Supone que la información necesaria para la lucha contra la delincuencia pueda atravesar las fronteras interiores de la UE sin encontrar obstáculos. El objetivo de la presente propuesta es que ese principio se aplique como instrumento jurídico vinculante.

8. El intercambio de información policial entre distintos países es un tema popular entre los legisladores, tanto dentro como fuera del marco de la UE. Recientemente, el SEPD ha observado las iniciativas que se indican a continuación.

9. En primer lugar, el 4 de junio de 2004 Suecia propuso una Decisión marco sobre la simplificación del intercambio de información e inteligencia entre los cuerpos de seguridad de los Estados miembros de la Unión Europea. El Consejo llegó a un acuerdo sobre una orientación general relativa a esta propuesta en su sesión del 1 de diciembre de 2005.

10. En segundo lugar, el 27 de mayo de 2005, siete Estados miembros firmaron en Prüm (Alemania) un Tratado relativo a la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal. Entre otras cosas, este Tratado introduce medidas para la mejora del intercambio de información sobre ADN y huellas dactilares. El Tratado está abierto a la adhesión de cualquier Estado miembro de la Unión Europea. Las partes contratantes tienen como objetivo incorporar las disposiciones del Tratado al marco jurídico de la Unión Europea.

11. En tercer lugar, la disponibilidad de información policial y judicial a través de las fronteras interiores de la Unión Europea se facilitará asimismo mediante otros instrumentos jurídicos como las propuestas relativas a la segunda generación del Sistema de Información de Schengen (SIS II), la propuesta sobre el acceso a la consulta del Sistema de Información sobre Visados (VIS) y la propuesta de Decisión marco relativa a la organización y al contenido del intercambio de información de los registros de antecedentes penales entre los Estados miembros. A este respecto, también será útil mencionar la Comunicación sobre una mayor eficacia, interoperabilidad y sinergia entre la bases de datos europeas en el ámbito de la Justicia y los Asuntos de Interior, presentada por la Comisión el 25 de enero de 2005.

12. Del hecho que se hayan presentado todas esas iniciativas se desprende que la presente propuesta de Decisión marco sobre disponibilidad no debe estudiarse en sí misma, sino que han de tenerse en cuenta otros planteamientos relacionados con el intercambio de información policial y judicial. Esto es tanto más importante cuanto que la tendencia actual en el Consejo consiste en dar preferencia a otros planteamientos sobre intercambio de información y sobre el concepto de disponibilidad, distintos del planteamiento general que la Comisión propone en la presente propuesta. El texto actual de la propuesta podría incluso no ser objeto de debate en el Consejo.

13. Además, la propuesta está íntimamente vinculada a la propuesta de Decisión marco relativa a la protección de datos personales. El presente dictamen debe entenderse en relación con el dictamen más pormenorizado sobre esa Decisión marco.

14. En su dictamen en torno a la propuesta de Decisión marco relativa a la protección de los datos personales, el SEPD destacó la importancia de la protección adecuada de los datos, como consecuencia necesaria de un instrumento jurídico sobre su disponibilidad. Según el SEPD, ese instrumento jurídico no debe adoptarse sin garantías esenciales en materia de protección de datos.

15. El SEPD adopta la misma posición respecto de la adopción de otros instrumentos jurídicos que faciliten el flujo de información policial y judicial a través de las fronteras interiores de la UE. Por ello, el SEPD se congratula de que el Consejo y el Parlamento Europeo hayan dado prioridad a la propuesta de Decisión marco relativa a la protección de datos personales anteriormente mencionada.

III. EL PRINCIPIO DE DISPONIBILIDAD EN SÍ MISMO

16. En sí mismo, el principio de disponibilidad es sencillo. La información de que disponen determinadas autoridades en un Estado miembro debe facilitarse también a las autoridades equivalentes de otros Estados miembros. La información debe intercambiarse con la mayor rapidez y facilidad posibles entre las autoridades de los Estados miembros y, preferiblemente, permitiendo el acceso directo en línea.

17. Las dificultades surgen debido al entorno en que debe aplicarse el principio de disponibilidad:

— La organización heterogénea de la policía y del poder judicial en los Estados miembros, con controles y equilibrios diferentes.

— La inclusión de diversos tipos de información (sensible) (como el ADN o las huellas dactilares).

— Las diferentes formas de acceso de las autoridades competentes a la información pertinente, incluso dentro de los Estados miembros.

— La dificultad de garantizar que la información procedente de otro Estado miembro se interprete correctamente debido a las diferencias lingüísticas, de sistemas técnicos (interoperabilidad) y de ordenamientos jurídicos.

— La necesidad de incluir este principio en el extenso mosaico existente de disposiciones legales sobre intercambio de información policial y judicial entre los distintos países.

18. Con independencia de este complicado entorno, se entiende fácilmente que el principio no puede funcionar por sí mismo. Son necesarias medidas adicionales para garantizar que la información pueda hallarse y que pueda accederse a ella con eficacia. En cualquier caso, esas medidas deberán facilitar que las autoridades competentes averigüen si las autoridades competentes de otros Estados miembros disponen de la información pertinente y dónde puede hallarse esa información. Las medidas adicionales podrían consistir en interfaces que diesen acceso directo a todos los datos en posesión de otros Estados miembros, o a algunos datos específicos. La propuesta de Decisión marco relativa a la disponibilidad introduce por ello el concepto de «datos índice», es decir datos concretos a los que podrá accederse directamente a través de las fronteras.

19. En términos generales, el principio de disponibilidad debería facilitar el flujo de información entre Estados miembros. Se suprimirán las fronteras interiores y los Estados miembros deberán permitir que la información de que dispongan sus autoridades policiales sean cada vez más accesibles para otras autoridades. Los Estados miembros perderán la competencia de controlar el flujo de información, lo que tendrá como resultado que no podrán ya confiar en que sus legislaciones nacionales sean un instrumento suficiente para proteger adecuadamente la información.

20. Por esa razón, es necesario prestar una atención específica a la propuesta, desde el punto de vista de la protección de los datos personales. En primer lugar, se deberá facilitar a las autoridades de otros Estados miembros información que es habitualmente confidencial y que está bien protegida. En segundo lugar, para que el sistema funcione será necesario establecer datos índice, que habrán de ponerse a disposición de las autoridades de otros Estados miembros. La consecuencia de la aplicación del principio será que se generarán más datos que aquellos de los que actualmente se dispone.

IV. **ELEMENTOS PRINCIPALES**

Ámbito de aplicación del principio de disponibilidad

21. Primeramente es esencial definir a qué tipo de información se va a aplicar el principio de disponibilidad. El ámbito de aplicación de este principio se define, en términos generales, en el artículo 2 de la propuesta, en combinación con los artículos 1.1 y 3 a). El principio se aplicará a la información:

— existente

— incluida en la lista del Anexo II, que define seis tipos de información

— que esté a disposición de las autoridades competentes.

Estos son los tres elementos esenciales del ámbito de aplicación del principio que figuran en la propuesta de la Comisión. El ámbito de aplicación se define con más precisión en el artículo 2. El artículo 2.1 limita la aplicación del principio de disponibilidad a la etapa anterior al inicio de un proceso judicial, mientras que el artículo 2, apartados 2, 3 y 4, establece restricciones más específicas.

22. Para entender las consecuencias de la propuesta, es preciso efectuar un análisis más profundo de los tres elementos esenciales antes mencionados. Los primeros dos elementos del ámbito de aplicación son razonablemente claros por sí mismos. La definición de «información existente» se encuentra en el artículo 2.2, en el que se estipula que la Decisión marco no supone obligación alguna de recoger y almacenar información con el único objeto de hacerla accesible, y la lista del Anexo II no admite interpretaciones diferentes. Es el tercer elemento, en sí mismo y en combinación con los dos primeros, el que necesita aclararse más.

23. La propuesta no especifica si la «información disponible» consiste simplemente en la información que ya está bajo control de las autoridades competentes, o si incluye también la que estas autoridades puedan posiblemente obtener. Comoquiera que sea, según el SEPD, puede interpretarse que la propuesta incluye a ambas.

24. En efecto, mientras que el artículo 2.2 parece sugerir un ámbito más limitado al especificar que la Decisión marco «no implica ninguna obligación de recoger y almacenar información […] con el único fin de hacerla accesible», el artículo 3.a) permite una interpretación más amplia, al establecer que por «información» se entenderá «la información existente enumerada en el Anexo II».

25. El Anexo II menciona como mínimo dos categorías de datos que habitualmente controlan otras personas distintas de la policía. La primera categoría es la información relativa a la matriculación de vehículos. En muchos Estados miembros, las bases de datos que contienen esta información no están bajo el control de las autoridades policiales, aunque éstas tienen frecuentemente acceso a ellas. ¿Debe incluirse este tipo de información en el ámbito de aplicación de la «información disponible» que, a tenor del artículo 1, ha de facilitarse a las autoridades competentes equivalentes de otros Estados miembros? La segunda categoría de datos enumerada en el Anexo II que debe mencionarse son los números de teléfono y demás datos de comunicaciones: ¿Deben considerase «disponibles» estos datos, incluso cuando no estén bajo el control de las autoridades competentes, sino de empresas privadas?

26. Además, otras disposiciones de la propuesta, y más especialmente sus artículos 3 d) y 4.1 c), respaldan la opinión según la cual las «autoridades designadas», o incluso las «partes designadas» podrán controlar información que esté «disponible» para las «autoridades competentes». Del texto de la propuesta se desprende asimismo que la «autoridad competente» de un Estado miembro será la autoridad contemplada en el artículo 29, primer guión, del Tratado UE, mientras que cualquier autoridad nacional puede ser una «autoridad designada».

27. A juicio del SEPD, la aplicación del principio de disponibilidad a la información controlada por las autoridades y partes designadas plantea los siguientes interrogantes:

— ¿Establece el artículo 30.1 b) una base jurídica suficiente, puesto que son las autoridades y partes designadas las que dan acceso a la información contenida en unas bases de datos que no corresponden al marco del tercer pilar?

— ¿Será de aplicación la Decisión marco relativa a la protección de datos personales, como se da por supuesto, por ejemplo, en el artículo 8 de la propuesta?

— De lo contrario ¿se ajusta el tratamiento a las obligaciones que impone la Directiva 95/46/CE?

28. La aplicación de un principio tan amplio como el «principio de disponibilidad» exige una definición clara y exacta de los datos que se considerarán disponibles. Por ello, el SEPD recomienda lo siguiente:

— Aclarar el ámbito de aplicación.

— Como primera posibilidad, limitar el ámbito de aplicación del principio de disponibilidad a la información controlada por las autoridades competentes.

— Como segunda posibilidad, en caso de adoptarse un ámbito de aplicación más amplio, garantizar las salvaguardias suficientes para proteger los datos personales. Deben tenerse en consideración las preguntas que se formulan en el punto 27 anterior.

Otros puntos relacionados con el ámbito de aplicación

29. A tenor del artículo 2.1 de la propuesta, la Decisión marco se aplicará al tratamiento de la información previo al inicio de un proceso judicial. Su ámbito de aplicación es más limitado que el de la propuesta de Decisión marco relativa a la protección de datos personales, que se aplica plenamente a la cooperación judicial en materia penal.

30. Sin embargo, según el SEPD, esta limitación no limita por sí misma el ámbito de aplicación de la propuesta a la cooperación policial. Podría incluir también la cooperación judicial en materia penal, ya que en cierto número de Estados miembros las autoridades judiciales son también competentes en las investigaciones penales previas al enjuiciamiento. Con todo, el hecho de que la propuesta se base exclusivamente en el artículo 30.1 b) del TUE parece indicar que se aplica únicamente a la cooperación policial. Sería de agradecer una aclaración en lo que a este aspecto se refiere.

31. La presente propuesta se aplica a la transmisión de información a Europol, mientras que la propuesta de Decisión marco relativa a la protección de datos personales excluye el tratamiento de datos personales por parte de Europol. El SEPD aconseja que se limite el intercambio de información con Europol a los objetivos de la propia Europol, como se mencionan el artículo 2 del Convenio Europol y su Anexo. Además deben tenerse en cuenta las normas de desarrollo sobre intercambio de datos con Europol, que establecen ya varios actos del Consejo.

Ninguna nueva base de datos que contenga datos personales

32. El punto de partida de la propuesta es que no supondrá creación alguna de bases de datos nuevas que contengan datos personales. En este sentido, el artículo 2.2 es claro: no supondrá obligación alguna de recoger y almacenar información con la única finalidad de hacerla accesible. Desde el punto de vista de la protección de datos, este es un elemento importante y positivo de la propuesta. El SEPD recuerda su dictamen sobre la propuesta de Directiva sobre la retención de los datos procesados en conexión con la prestación de servicios públicos de comunicación electrónica ([1]), en el que destacaba que las obligaciones legales que conllevan la creación de grandes bases de datos suponen riesgos especiales para las personas a que se refieren los datos, entre otras cosas debido al riesgo de que se utilicen de forma ilegítima.

33. Sin embargo:

— Es importante garantizar que la propuesta no propiciará la interconexión incondicional de bases de datos y, por ende, la creación de una red de bases de datos que sería difícil de supervisar.

— Hay una excepción al supuesto de partida que acaba de mencionarse: el artículo 10 de la propuesta, que garantiza el acceso en línea a los datos índice. Estos pueden contener datos personales o, en cualquier caso, revelar su existencia.

Acceso directo e indirecto a la información

34. La propuesta contempla el acceso directo e indirecto a la información. El artículo 9 de la propuesta contempla el acceso directo en línea a la información contenida en las bases de datos a las que tengan acceso directo en línea las autoridades nacionales correspondientes. El artículo 10 prevé el acceso indirecto. Los datos índice de la información no accesible en línea deberán estar a disposición, para su consulta, de las autoridades competentes equivalentes de otros Estados miembros y de Europol. Cuando la consulta de los datos índice tenga resultado positivo, esta autoridad podrá cursar una solicitud de información y remitirla a la autoridad designada con el fin de obtener la información determinada mediante el dato índice.

35. El acceso directo no supone el establecimiento de bases de datos nuevas, pero sí exige la interoperabilidad de las bases de datos de los sistemas competentes equivalentes dentro de los Estados miembros. Además, introducirá necesariamente un nuevo uso de las bases de datos existentes, al facilitar a todas las autoridades competentes de los Estados miembros un servicio al que hasta ese momento sólo tenían acceso las autoridades competentes nacionales. El acceso directo supondrá automáticamente que un número creciente de personas tenga acceso a las bases de datos, lo cual implica un aumento del riesgo de que se utilicen indebidamente.

([1]) Dictamen del 26 de septiembre de 2005 en relación con la Directiva del Parlamento Europeo y del Consejo sobre la retención de los datos procesados en conexión con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE (COM (2005) 438 final).

36. Tratándose del acceso directo por parte de una autoridad competente de otro Estado miembro, las autoridades designadas del Estado miembro de origen no tendrán control alguno sobre el acceso y posterior utilización de los datos. Esta consecuencia del acceso directo, tal como lo contempla la propuesta, debe estudiarse adecuadamente, ya que:

— Parece invalidar la facultad de las autoridades designadas de denegar el suministro de la información (a tenor del artículo 14).

— Plantea interrogantes en cuanto a las responsabilidades sobre la exactitud y la actualización de las bases de datos, una vez que se ha tenido acceso a éstas. ¿Cómo puede garantizar la autoridad designada del Estado miembro de origen que los datos se mantengan actualizados?

— No solamente la autoridad designada se verá ya en la imposibilidad de cumplir todas sus obligaciones a tenor de la legislación sobre protección de datos, sino que la autoridad del Estado miembro de origen encargada de la protección de datos tampoco podrá supervisar el cumplimiento de las obligaciones, al carecer de toda competencia frente a las autoridades policiales y judiciales de otros Estados miembros.

— Estos problemas son todavía más acuciantes tratándose del acceso a las bases de datos por parte de las autoridades designadas y de las partes designadas, al no ser éstas autoridades policiales ni judiciales (véanse los puntos 25 a 28 del presente dictamen).

Esta consecuencia del acceso directo es una de las razones importantes por las que la adopción de la presente propuesta debe supeditarse a que se adopte una Decisión marco relativa a la protección de datos personales. Queda un último problema: resulta difícil de imaginar cómo las autoridades designadas podrían denegar el suministro de información a tenor del artículo 14.

37. Por lo que se refiere al acceso indirecto a través de los datos índice que dan información con arreglo a un sistema de respuesta positiva/negativa, éste no es un fenómeno nuevo, sino que es la base del funcionamiento de los sistemas europeos de información a gran escala, como el Sistema de Información de Schengen. El establecimiento de un sistema de datos índice tiene la ventaja de permitir que el Estado miembro de origen controle el intercambio de información de sus expedientes policiales. Cuando la consulta de los datos índice dé una respuesta positiva, la autoridad solicitante podrá cursar una solicitud de información en relación con la persona de que se trate. La autoridad requerida podrá evaluar adecuadamente esta solicitud.

38. Con todo, es necesario llevar a cabo un análisis adecuado, porque el establecimiento de un sistema de datos índice -en ámbitos en los que hasta ahora no existían esos sistemas, si se exceptúan los sistemas europeos de información a gran escala- puede crear nuevos riesgos para las personas a que se refieren los datos. El SEPD subraya que aunque los datos índice no contienen mucha información en cuanto a las personas objeto de los datos, la consulta de datos índice puede llevar a resultados altamente sensibles, al poder revelar que una persona se encuentra incluida en un expediente policial relacionado con delitos penales.

39. Por todo ello es de la mayor importancia que el legislador europeo establezca las normas apropiadas, por lo menos en lo que se refiere a la creación de los datos índice, a la gestión de los sistemas de archivo de datos índice y a la adecuada organización del acceso a éstos. Según el SEPD, la propuesta no es satisfactoria en cuanto a estos puntos. De momento el SEPD presenta tres observaciones:

— No está clara la definición de datos índice. No está claro si éstos deben verse como metadatos, claves primarias o ambas cosas a la vez. El concepto de dato índice debe aclararse, porque repercute directamente en el nivel de protección de los datos y en las salvaguardias necesarias.

— La propuesta debe aclarar el papel desempeñado por los puntos de contacto nacionales en lo que a los datos índice se refiere. Podría resultar necesaria la participación de los puntos de contacto nacionales, sobre todo cuando la interpretación de los datos índice exija conocimientos especializados, como por ejemplo tratándose de la posible concordancia de huellas dactilares.

— La propuesta deja la adopción de las normas necesarias para la creación de los datos índice a la legislación de aplicación, de conformidad con el procedimiento de comitología que contempla el artículo 19. Si bien pueden ser necesarias unas normas de desarrollo, las normas básicas para la creación de los datos índice deben incluirse en la Decisión marco misma.

Autorización previa de las autoridades judiciales

40. El intercambio de información no impedirá que los Estados miembros soliciten la autorización previa de las autoridades judiciales para transmitir la información a la autoridad solicitante, cuando esa información se encuentre bajo control judicial en el país requerido. Esto es importante porque, según una encuesta en relación con las competencias policiales en materia de intercambio de datos personales ([1]), no en todos los Estados miembros puede la policía acceder de forma autónoma a esos datos. A juicio del SEPD, el principio de disponibilidad no debe socavar la obligación que establecen las legislaciones nacionales de obtener una autorización previa para la información, o por lo menos establecer normas específicas relacionadas con las categorías de datos para las que deba obtenerse una autorización previa, que se aplicará en todos los Estados miembros.

([1]) Respuestas al cuestionario relativo a la Decisión marco sobre la simplificación del intercambio de información e inteligencia entre los cuerpos de seguridad de los Estados miembros de la Unión Europea, en particular en relación con delitos graves, incluidos los actos de terrorismo (doc. nº 5815/15 del Consejo).

41. Esta obligación ha de interpretarse en relación con el artículo 11.2 de la propuesta de Decisión marco relativa a la protección de datos personales, que también prevé que el Estado miembro transmisor tiene algo que decir en cuanto a la utilización ulterior de los datos en el Estado miembro al que se hayan transmitido. El SEPD advierte de la importancia de este principio, que es necesario para garantizar que la disponibilidad no lleve a eludir las legislaciones nacionales restrictivas en cuanto a la utilización ulterior de los datos personales.

Observación final

42. Estos elementos exigen unos elevados estándares de protección de datos. Deberá prestarse especial atención a garantizar los principios de limitación de la finalidad y del tratamiento ulterior, así como a la exactitud y la fiabilidad de la información a la que se tenga acceso (véase también el dictamen del SEPD sobre la Decisión marco relativa a la protección de datos personales, puntos IV.2 y IV.6).

V. OTROS PLANTEAMIENTOS

Propuesta de Suecia

43. La propuesta sueca no se limita a tipos específicos de información, sino que abarca toda la información *y la inteligencia*, incluso la información e inteligencia que se encuentre en posesión de otras personas distintas de las autoridades policiales y judiciales competentes. La propuesta propicia la cooperación estableciendo plazos límite para dar respuesta a las solicitudes de información, y suprimiendo la discriminación entre el intercambio dentro de un Estado miembro y el intercambio transfronterizo de información. No establece medida adicional alguna que garantice que pueda accederse efectivamente a la información. Por esa razón, se comprende con facilidad que la Comisión no quedara satisfecha con la propuesta de Suecia en sí misma como instrumento adecuado en materia de disponibilidad ([1]).

44. El planteamiento adoptado en la propuesta de Suecia tiene las siguientes implicaciones generales desde el punto de vista de la protección de datos:

— Es positivo que la propuesta se limite estrictamente al tratamiento de los datos existentes, y que no lleve a la creación de nuevas bases de datos, ni siquiera de «datos índice».

— Sin embargo, la falta de «datos índice» no es un elemento positivo por definición. Los datos índice, si se garantizan adecuadamente, pueden facilitar una investigación selectiva y, por eso mismo, menos invasora, de los datos de índole sensible. También puede permitir filtrar mejor las solicitudes, así como una mayor supervisión.

— En cualquier caso, la propuesta conlleva el aumento del intercambio transfronterizo de datos personales, con riesgos para la protección de éstos, entre otras cosas porque afecta a la competencia de los Estados miembros para controlar plenamente al intercambiador de datos. No debe adoptarse independientemente de la adopción de la Decisión marco relativa a la protección de datos personales.

([1]) Véase el Anexo del documento de trabajo de los servicios de la Comisión relativo a la propuesta de Decisión marco sobre el intercambio de información en virtud del principio de disponibilidad, SEC(2005) 1270 de 12.10.2005.

Tratado de Prüm

45. El Tratado de Prüm adopta otro planteamiento sobre la aplicación del principio de disponibilidad. Mientras que la presente propuesta de Decisión marco establece un planteamiento general -al no fijar normas específicas para el intercambio de tipos concretos de información, sino que se aplica a todos sus tipos en la medida en que figuren en la lista del Anexo II (véanse los puntos 21 a 28 del presente dictamen)-, el planteamiento del Tratado de Prüm es gradual.

46. Este planteamiento se conoce algunas veces como «planteamiento de campo de datos por campo de datos». Se aplica a tipos específicos de información (ADN, huellas dactilares y datos sobre matriculación de vehículos), y establece la obligación de tener en cuenta la naturaleza específica de los datos. El Tratado estipula la obligación de abrir y mantener ficheros de análisis de ADN para la investigación de delitos penales. Una obligación similar se aplica a las huellas dactilares. En cuanto a los datos sobre matriculación de vehículos, debe facilitarse el acceso directo a los puntos de contacto nacionales de los demás Estados miembros.

47. El enfoque del Tratado de Prüm da lugar a tres tipos de observaciones.

48. En primer lugar, no hace falta decir que el SEPD no aprueba el proceso que conduce a dicho Tratado, fuera del marco institucional de la Unión Europea, y por lo tanto sin participación sustantiva de la Comisión. Además, ello significa ausencia de control democrático por parte del Parlamento Europeo y ausencia de control judicial por parte del Tribunal de Justicia y como resultado de todo ello menos garantías de que se equilibren de igual modo todos los intereses (públicos). Ello incluye la perspectiva de la protección de datos. En resumidas cuentas, las instituciones de la Unión Europea no tienen la oportunidad de valorar -antes de que se establezca el sistema- el impacto de las elecciones políticas en la protección de datos personales.

49. En segundo lugar, resulta obvio que algunos elementos del Tratado de Prüm afectan más a la persona a la que se refieren los datos que la propuesta de una Decisión marco sobre disponibilidad. El Tratado necesariamente conduce al establecimiento de nuevas bases de datos, lo que en sí mismo presenta riesgos para la protección de datos personales. La necesidad y la proporcionalidad de la creación de estas nuevas bases de datos debería demostrarse. Deberían facilitarse garantías adecuadas de protección de los datos personales.

Un planteamiento de campo de datos por campo de datos

50. En tercer lugar, tal y como se ha dicho anteriormente, el Tratado adopta un planteamiento de campo de datos por campo de datos. Más arriba el SEPD mencionó las dificultades e incertidumbres relacionadas con el entorno en el que el principio de disponibilidad tiene que hacerse efectivo. En dichas circunstancias, en opinión del SEPD resulta preferible no establecer un sistema para una diversidad de datos, sino comenzar con un enfoque más cauto que abarque un solo tipo de datos y controlar hasta qué punto el principio de disponibilidad puede efectivamente servir de apoyo a las fuerzas y cuerpos de seguridad, así como vigilar los riesgos específicos para la protección de datos personales. A partir de dichas experiencias, el sistema podría posiblemente ampliarse a otros tipos de datos o modificarse con el fin de ser más efectivo.

51. Este planteamiento de campo de datos por campo de datos cumpliría mejor los requisitos del principio de proporcionalidad. Según el SEPD, las necesidades de un mejor intercambio transfronterizo de datos por lo que respecta a las fuerzas y cuerpos de seguridad podría justificar la adopción de un instrumento jurídico a escala de la UE, pero el instrumento, para ser proporcional, debería ser adecuado para la consecución de su objetivo, que podrá determinarse más correctamente tras un período de experiencias prácticas. Además, el instrumento no debería perjudicar de manera desproporcionada a la persona a la que se refieran los datos. El intercambio debería limitarse a los tipos de datos que sean estrictamente necesarios, con posibilidad de intercambio anónimo de datos, y debería tener lugar en condiciones estrictas de protección de datos.

52. Por otra parte, un enfoque más cauteloso tal y como recomienda el SEPD podría incluir -posiblemente además del planteamiento de campo de datos por campo de datos- el inicio de la aplicación del principio de disponibilidad únicamente mediante acceso indirecto, a través de datos índice. El SEPD menciona esto como un punto que debe tenerse en cuenta en el futuro proceso legislativo.

VI. ¿QUÉ DATOS?

53. En el Anexo II se enumeran los tipos de información que podrán obtenerse con arreglo a la Decisión marco propuesta. Los seis tipos de información que allí figuran son datos personales en la mayoría de las circunstancias, ya que todos contienen una relación con una persona identificable o identificada.

54. Con arreglo al artículo 3, letra g) de la propuesta, se entenderá por datos índice «datos cuya finalidad es identificar claramente la información, y que pueden interrogarse mediante una rutina de búsqueda, con el fin de comprobar si la información está o no disponible» [1]. En el «Planteamiento de la aplicación del principio de disponibilidad» se califican como datos índice los siguientes:

— la identificación de las personas afectadas

— un número de identificación de los objetos (vehículos, documentos, etc.)

— impresiones dactilares y fotografías digitales.

Otro tipo de datos que podrían calificarse como datos índice serían los perfiles de ADN. Esta lista de datos índice revela que los datos índice pueden contener datos personales y por lo tanto, se requiere una adecuada protección.

55. El SEPD aborda específicamente el tema de los perfiles de ADN. Se ha demostrado que el análisis del ADN resulta de significativo valor para las investigaciones de delitos y un intercambio eficiente de datos de ADN puede resultar esencial para la lucha contra la delincuencia. Sin embargo, resulta esencial que el concepto de datos de ADN se defina claramente y que se tengan debidamente en cuenta las características específicas de dichos datos. Ciertamente, desde el punto de vista de la protección de datos, existe una gran diferencia entre las muestras de ADN y los perfiles de ADN.

56. Las muestras de ADN (a menudo recogidas y almacenadas por autoridades policiales) deberían considerarse como particularmente sensibles, ya que lo más probable es que contengan el conjunto del ADN de una persona. Pueden facilitar información sobre las características genéticas y el estado de salud de una persona, cosa que puede necesitarse para fines totalmente distintos tales como dar consejos médicos a personas o a jóvenes parejas.

57. Los perfiles de ADN, en cambio, contienen únicamente alguna información parcial de ADN extraída de la muestra de ADN: pueden utilizarse para verificar la identidad de una persona, pero en principio no revelan características genéticas de una persona. Con todo, los progresos científicos pueden aumentar la información que puede revelarse mediante perfiles de ADN: lo que se considera un perfil de ADN «inocente» en un determinado momento, puede revelar en una fase posterior mucha más información de la esperada y necesitada, y en particular información relativa a las características genéticas de una persona. La información que puede revelarse mediante perfiles de ADN debería, por lo tanto, considerarse dinámica.

58. Teniendo en cuenta lo anteriormente enunciado, el SEPD observa que tanto el Tratado de Prüm como la propuesta de la Comisión fomentan el intercambio de datos de ADN entre fuerzas y cuerpos de seguridad, pero existen diferencias sustantivas en la manera de llevarse a cabo.

[1] Documento de la Presidencia al Consejo de 5 de abril de 2005 (doc. nº 7641/05).

59. El SEPD acoge con satisfacción que la propuesta de la Comisión no establezca ninguna obligación de recoger datos de ADN y que limite claramente el intercambio de datos de ADN a los perfiles de ADN. El Anexo II define los perfiles de ADN mediante una lista inicial común de marcadores de ADN utilizados en análisis forenses de ADN en los Estados miembros. Dicha lista -basada en los siete marcadores de ADN del Conjunto de normas europeas (European Standard Set) definidos en el Anexo I de la Resolución del Consejo de 25 de junio de 2001 relativa al intercambio de resultados de análisis de ADN ([1])- garantiza que los perfiles de ADN no contengan, en el momento de su extracción, ninguna información sobre características hereditarias específicas.

60. El SEPD subraya que la Resolución del Consejo establece algunas salvaguardias muy importantes que se relacionan específicamente con el carácter dinámico de los perfiles de ADN. En efecto, la sección III de la Resolución, tras limitar los intercambios de los resultados de análisis de ADN a las «zonas cromosómicas […] de las que no se tenga constancia que contengan información sobre características hereditarias específicas», recomienda además a los Estados miembros no seguir utilizando los marcadores de ADN que, debido a los avances científicos, puedan proporcionar información sobre características hereditarias específicas.

61. El Tratado de Prüm establece un planteamiento diferente, ya que obliga a las Partes Contratantes a crear y mantener ficheros de análisis del ADN para los fines de la persecución de los delitos. Por lo tanto, supone la creación de nuevas bases de datos de ADN y una recopilación incrementada de datos de ADN. Además, no resulta claro qué tipo de datos se incluyen en los ficheros de análisis del ADN, y el Tratado no tiene en cuenta la evolución dinámica de los perfiles de ADN.

62. El SEPD subraya que cualquier instrumento jurídico por el que se establezcan intercambios de ADN debería:

— Limitar claramente y definir el tipo de información de ADN que podrá intercambiarse (también con respecto a la diferencia fundamental entre muestras de ADN y perfiles de ADN).

— Establecer unas normas técnicas comunes que tengan como objetivo evitar que las variaciones en el manejo de las bases de datos de ADN de la policía científica en los Estados miembros generen dificultades y resultados incorrectos a la hora de intercambiar datos.

— Facilitar garantías adecuadas y legalmente obligatorias para evitar que los avances científicos lleven a obtener de los perfiles de ADN datos personales que no sólo sean sensibles, sino también innecesarios para el objetivo para el que fueron recogidos.

([1]) DO C 187, p. 1.

63. Teniendo en cuenta lo dicho anteriormente, el SEPD confirma e incorpora aquí las observaciones recogidas en su dictamen sobre la Decisión marco relativa a la protección de datos (punto 80). En dicho dictamen el SEPD señaló que, con respecto a los datos de ADN, deberían establecerse garantías específicas, con el fin de garantizar que: la información disponible sólo se utilice para identificar a personas con el fin de prevenir, descubrir o investigar delitos; se tenga cuidadosamente en cuenta el grado de precisión de los perfiles de ADN y el interesado pueda impugnarlos por medios de fácil accesibilidad; se garantice plenamente el respeto de la dignidad de la persona ([2]).

64. Estas consideraciones llevan, además, a la conclusión de que la legislación sobre el establecimiento de perfiles de ADN y el intercambio de datos de dichos perfiles debería adoptarse únicamente tras una evaluación de impacto en la que hayan podido sopesarse correctamente los beneficios y los riesgos. El SEPD recomienda que dicha legislación contenga obligaciones relativas a su evaluación periódica tras su entrada en vigor.

65. Por último, el Anexo II contempla otros tipos de información que podrá intercambiarse. En ella se incluye información procedente de entidades privadas, ya que los números de teléfono y otros datos relativos a las comunicaciones, así como los datos relativos al tráfico, proceden normalmente de operadores telefónicos. La exposición de motivos confirma que los Estados miembros están obligados a garantizar que la información pertinente a efectos policiales controlada por autoridades o por entidades privadas designadas al efecto se comparta con las autoridades competentes equivalentes de otros Estados miembros y con Europol. Visto que la propuesta se refiere a datos personales procedentes de entidades privadas, el marco legal aplicable debería -según el SEPD- contener garantías adicionales con el fin de proteger a las personas a las que se refieran los datos así como de garantizar la precisión de dichos datos.

VII. **PRINCIPIOS DE LA PROTECCIÓN DE DATOS**

66. Las normas sobre la protección de datos personales no figuran específicamente en la Decisión Marco del Consejo propuesta, mientras que en otros instrumentos, como el Tratado de Prüm o la propuesta sueca, hay algunas disposiciones específicas sobre la protección de los datos personales. La ausencia de normas específicas sobre la protección de datos personales en la propuesta de disponibilidad sólo será aceptable en la medida en que las normas generales recogidas en la propuesta de Decisión marco sobre protección de datos dentro del tercer pilar sean plenamente aplicables y proporcionen protección suficiente. Asimismo, las normas relativas a la protección de datos personales establecidas mediante instrumentos específicos, tales como la propuesta sueca y el Tratado de Prüm, no deberían reducir el nivel de protección garantizado por el marco general. El SEPD recomienda añadir una cláusula específica sobre posibles conflictos entre las diferentes normas de protección de datos.

([2]) En la misma línea, véase además el *Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data* del Consejo de Europa, febrero de 2005.

67. Así las cosas, el SEPD desearía hacer de nuevo hincapié, al recordar su dictamen relativo a la Decisión marco sobre protección de datos personales, la importancia de disponer de normas de protección de datos coherentes y exhaustivas en lo que se refiere a la cooperación policial que se aplique a todo tratamiento. Asimismo, el SEPD reitera las demás observaciones que se hacen en ese dictamen. En este apartado, se ponen de relieve los siguientes temas relacionados con la protección de datos:

— Tratamiento lícito de datos personales. El SEPD apoya el enfoque de que la información esté disponible sólo si ha sido recogida de manera lícita (como se menciona en el artículo 2.2 respecto a la información recogida mediante medidas coercitivas). El tratamiento lícito de los datos personales garantizaría además que la información de que se disponga y que se intercambie puede emplearse de manera apropiada en un procedimiento judicial. De hecho, aunque la información tratada tras el inicio de un proceso quede fuera del ámbito del instrumento propuesto, sigue siendo posible que la información intercambiada antes por las autoridades policiales concluya utilizándose en procedimientos judiciales.

— La calidad de los datos personales reviste particular importancia, dado que el principio de disponibilidad favorece que autoridades policiales que actúen fuera del contexto en el que se recogieron los datos hagan uso de ellos. Esas autoridades tendrán incluso acceso directo a bases de datos de otros Estados miembros. La calidad de los datos personales sólo podrá garantizarse si se comprueba periódica y adecuadamente su exactitud, si la información se discrimina según las diferentes categorías de las personas en cuestión (víctimas, sospechosos, testigos, etc.) y si, de ser necesario, se indica el grado de exactitud (véase el Dictamen del SEPD sobre la protección de datos personales, IV.6).

Estos puntos ponen aún más en claro por qué las normas de protección de datos, y especialmente las normas sobre exactitud, deberían ser aplicables a todo tipo de tratamiento, también los nacionales. De no ser así, los datos personales a que se tenga acceso directamente podrían ser incorrectos u obsoletos y perjudicar tanto los derechos de los interesados como la eficacia de las investigaciones.

— Limitación de la finalidad. De acuerdo con el principio de disponibilidad, las autoridades competentes equivalentes de otros Estados miembros podrán acceder a los datos personales. Ahora bien, las competencias de las autoridades policiales podrán ser sustancialmente diferentes entre países. Es por ello esencial garantizar el respeto del principio básico de limitación de finalidad, pese a los diferentes ámbitos de competencias de las diferentes autoridades competentes que intercambien datos. Así, la información que recoja y trate una determinada autoridad con una finalidad concreta no podrá emplearse con finalidad distinta sólo en virtud de las competencias diferentes, quizás más amplias, de la autoridad receptora.

Por ello, el SEPD aprecia el artículo 7 de la Decisión Marco propuesta, que debería entenderse como una precisión de las normas generales establecidas en la Decisión marco propuesta sobre protección de datos personales. Además, el SEPD señala que la evaluación de la equivalencia entre diferentes autoridades (que en la propuesta actual se pone en manos de un procedimiento de comitología) debería hacerse con mucha atención y con el debido respeto del principio de limitación de finalidad.

— Los plazos de almacenamiento de la información intercambiada deberían considerarse también teniendo en cuenta el principio de limitación de finalidad; la información a que se haya tenido acceso o que se haya intercambiado con una finalidad deberá borrarse en cuanto ya no sea necesaria para esa finalidad. Esto evitará duplicaciones innecesarias de datos personales y permitirá a la vez a las autoridades competentes tener acceso (actualizado) de nuevo a la información disponible, en caso de que sea necesario para otra finalidad legítima.

— Registro de la información transmitida según el principio de disponibilidad. El registro se hará en ambas partes, es decir, tanto en el Estado miembro requerido como en el requirente. Deberán conservarse los registros de acceso, no sólo los registros de intercambio (véase el Dictamen del SEPD sobre la protección de datos personales, punto 133), también con vista a garantizar que las autoridades nacionales competentes confíen las unas en las otras y no pierdan completamente el control sobre la información disponible. La necesidad de trazabilidad de la información supone también la posibilidad de actualizar o corregir la información.

— Derechos de los interesados. Los sistemas de intercambio de información entre las autoridades policiales de la UE hacen que aumenten las situaciones en las que los datos personales sean tratados (temporalmente) a la misma vez por autoridades competentes en diferentes Estados miembros. Esto quiere decir, por un lado, que deberán establecerse normas comunes a escala de la UE sobre los derechos de los interesados y, por otro, que los interesados deberán poder ejercer sus derechos hasta el punto permitido por las normas de protección de datos dentro del tercer pilar, en lo que respecta tanto a las autoridades que ponen los datos a disposición de otras como a las que tengan acceso y traten esos datos.

— Supervisión. El SEPD indica que, según los casos, más de una autoridad nacional de supervisión podrá ser competente del seguimiento del tratamiento de datos personales transmitidos conforme a las propuestas actuales. En ese sentido, el acceso directo en línea a información policial exige un aumento de la supervisión y de la coordinación por parte de las autoridades nacionales responsables de la protección de datos.

VIII. CONCLUSIONES

Conclusiones generales relativas al principio de disponibilidad

68. El SEPD aprovecha la ocasión para presentar en su dictamen algunas opiniones más generales y fundamentales sobre el tema del intercambio de información policial y sobre los enfoques para la reglamentación de este tema. El SEPD estará disponible para consultas adicionales en una fase posterior, de resultas de la pertinente evolución del proceso legislativo sobre esta propuesta o sobre otras propuestas relacionadas.

69. Según el SEPD, el principio de disponibilidad debería aplicarse dentro de un instrumento jurídico vinculante mediante un enfoque más cauto y gradual que incluya un solo tipo de datos y debería controlarse en qué medida el principio de disponibilidad puede ser de verdadera utilidad para la actividad policial, sin olvidar los riesgos específicos que supone para la protección de datos personales. Este enfoque más cauto podría empezar con la aplicación del principio de disponibilidad sólo por acceso indirecto, mediante datos índice. Sobre la base de estas experiencias, el sistema podría quizás ampliarse a otros tipos de datos o modificarse para ser más eficaz.

70. No debería adoptarse ningún instrumento jurídico que aplique el principio de disponibilidad sin la previa adopción de garantías esenciales de protección de datos, tal y como se recogen en la propuesta de Decisión marco sobre la protección de datos personales.

Recomendaciones destinadas a modificar la presente propuesta

71. El SEPD recomienda aclarar el ámbito de aplicación del principio de disponibilidad como sigue:

    — Añadir una definición clara y precisa de los datos que se habrán de considerar disponibles.

    — Como primera opción, limitar el ámbito del principio de disponibilidad a información controlada por las autoridades competentes.

    — Como segunda opción, en caso de un ámbito más amplio, garantizar las salvaguardas suficientes para la protección de los datos personales. Deberán tenerse en cuenta las cuestiones planteadas en el punto 27 del presente dictamen.

72. El SEPD hace las siguientes observaciones sobre el acceso directo a bases de datos por parte de una autoridad competente de otro Estado miembro:

    — El tema deberá tratarse adecuadamente, dado que, en caso de acceso directo, las autoridades designadas del Estado miembro de origen no tendrán control sobre el acceso a los datos y su uso posterior.

    — La propuesta no podrá favorecer una interconexión incondicional de bases de datos, pues, de ser así, sería muy difícil de supervisar una red de bases de datos.

73. La Decisión marco deberá ser más precisa respecto al establecimiento de un sistema de datos índice. Más en concreto:

    — La propuesta deberá fijar normas adecuadas, al menos sobre la creación de datos índice, sobre la gestión de los sistemas de alimentación de los índices de datos y sobre la adecuada organización del acceso a los datos índice.

    — Es preciso aclarar la definición de datos índice.

    — La propuesta deberá aclarar el cometido de los puntos de contacto nacionales en lo que se refiere a los datos índice.

    — Las normas básicas para la creación de datos índice deberán incluirse en la propia Decisión marco y no dejarse en manos de la legislación de desarrollo conforme al procedimiento de comitología.

74. El SEPD observa que la propuesta -en la medida en que establece intercambios de datos de ADN- debería:

    — Limitar claramente y definir el tipo de información sobre ADN que pueda intercambiarse (también en lo que se refiere a la diferencia fundamental entre muestras ADN y perfiles ADN).

    — Establecer normas técnicas comunes destinadas a evitar que las variaciones en las prácticas relativas a bases de datos de ADN de la policía científica en los Estados miembros puedan acarrear dificultades y resultados inexactos cuando se intercambien los datos.

    — Proporcionar las apropiadas salvaguardias legalmente vinculantes destinadas a evitar que la evolución científica suponga obtener de los perfiles de ADN datos personales que no sólo sean sensibles, sino también innecesarios para la finalidad para la que se recolectaron.

    — Adoptarse sólo previa evaluación de impacto.

75. El SEPD aconseja limitar el intercambio de información con Europol a las finalidades de la propia Europol, tal y como se mencionan en el artículo 2 del Convenio Europol y en su Anexo.

Hecho en Bruselas el 28 de febrero de 2006.

Peter HUSTINX

Supervisor Europeo de la Protección de Datos