ISSN 1725-244X

Diario Oficial de la Unión Europea

C 298

Edición en lengua española

Comunicaciones e informaciones

48º año

29 de noviembre de 2005

Número de información | Sumario | Página

ES

I

(Comunicaciones)

DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

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

(2005/C 298/01)

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]), y la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) ([2]),

Visto el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos ([3]), y, en particular, su artículo 41,

Vista la solicitud de dictamen, de conformidad con el artículo 28, apartado 2, del Reglamento (CE) nº 45/2001, recibida de la Comisión el 23 de septiembre de 2005,

HA ADOPTADO EL SIGUIENTE DICTAMEN:

I. **Introducción**

1. El Supervisor Europeo de Protección de Datos (SEPD) acoge con satisfacción que se le consulte de conformidad con el artículo 28, apartado 2, del Reglamento (CE) nº 45/2001. Sin embargo, teniendo en cuenta el carácter obligatorio del artículo mencionado, el presente Dictamen debe mencionarse en el preámbulo de la Directiva.

2. El SEPD reconoce la importancia que tiene para los servicios policiales de los Estados miembros disponer de todos los instrumentos jurídicos necesarios, en especial en la lucha

([1]) DO L 281 de 23.11.1995, p. 31.

([2]) DO L 201 de 31.7.2002, p. 37.

([3]) DO L 8 de 12.1.2001, p. 1.

contra el terrorismo y otros tipos de delincuencia grave. Una disponibilidad adecuada de determinados datos de tráfico y de localización de los servicios electrónicos públicos puede ser un instrumento decisivo para dichos servicios policiales y puede contribuir a la seguridad física de las personas. Además, cabe observar que esto no implica automáticamente la necesidad de los nuevos instrumentos según lo previsto en la presente propuesta.

3. Es igualmente evidente que la propuesta tiene un impacto considerable en la protección de datos personales. Si la propuesta se considera solamente desde la perspectiva de la protección de datos, los datos de tráfico y de localización no deben retenerse en absoluto con fines represivos. Debido a la protección de datos, la Directiva 2002/58/CE establece como principio jurídico que los datos de tráfico deben borrarse cuando el almacenamiento ya no sea necesario a efectos de la propia comunicación en sí (inclusive con fines de facturación). Las excepciones a este principio jurídico están sujetas a condiciones estrictas.

4. En el presente Dictamen, el SEPD pondrá de relieve el impacto de la propuesta sobre la protección de los datos personales. Por otra parte, el SEPD tendrá en cuenta que la propuesta no tenga como consecuencia, a pesar de su importancia para los servicios policiales, que los particulares se vean privados del derecho fundamental a la protección de su intimidad.

5. El presente Dictamen del SEPD debe considerarse a la luz de dichas consideraciones. El SEPD prevé un planteamiento equilibrado, en el que la necesidad y la proporcionalidad de la interferencia con la protección de datos desempeñen un papel central.

6. En lo que se refiere a la propuesta misma, debe verse como una reacción a la iniciativa por parte de la República Francesa, de Irlanda, del Reino de Suecia y del Reino Unido de una Decisión marco sobre la retención de datos tratados y almacenados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de datos trasmitidos por redes públicas de comunicaciones, a efectos de prevención, investigación, descubrimiento y represión de la delincuencia y las infracciones penales, con inclusión del terrorismo (en adelante «el proyecto de Decisión marco»), rechazado por el Parlamento Europeo (en el procedimiento de consulta).

7. El SEPD no ha sido consultado sobre el proyecto de Decisión marco, ni ha emitido un dictamen por iniciativa propia. El SEPD no se plantea por ahora emitir un dictamen sobre el proyecto de Decisión marco, pero se referirá en el presente Dictamen a dicho proyecto de Decisión, cuando lo considere útil.

II. **Observaciones generales**

El impacto de la propuesta sobre la protección de datos personales

8. Es esencial para el SEPD que la propuesta respete los derechos fundamentales. Una medida legislativa que conculcase la protección garantizada por el Derecho comunitario y, más en especial, por la jurisprudencia del Tribunal de Justicia y del Tribunal Europeo de Derechos Humanos no sólo es inaceptable, sino también ilegal. Las circunstancias en la sociedad pueden haber cambiado debido a ataques terroristas, pero esto no puede tener como efecto que se comprometan los estándares elevados de protección en el Estado de Derecho. La legislación asegura la protección con independencia de las necesidades policiales reales. Por otra parte, la propia jurisprudencia permite las excepciones, en caso de necesidad, en una sociedad democrática.

9. La propuesta tiene un impacto directo sobre la protección garantizada por el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH). La jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH) ha considerado que:

— el almacenamiento de información sobre un individuo era una injerencia en la vida privada, incluso aunque no contuviera ningún dato sensible [Amann ([1])],

— lo mismo se aplica a la práctica de la «medición» de llamadas telefónicas, que implica el uso de un dispositivo que registra automáticamente los números marcados en un teléfono y el tiempo y la duración de cada llamada [Malone ([2])],

— las justificaciones para la injerencia deben ser más importantes que las consecuencias perjudiciales que la existencia misma de las disposiciones legislativas de que se trata pudiera entrañar para las personas [Dudgeon ([3])].

10. El artículo 6, apartado 2, del Tratado UE establece que la Unión respetará los derechos fundamentales tal y como se garantizan en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. En el párrafo anterior se ha mostrado que, conforme a la jurisprudencia del Tribunal Europeo de Derechos Humanos, la obligación de retener datos entra dentro del ámbito del artículo 8 del CEDH y que es necesaria una justificación

([1]) Sentencia del TEDH de 16 de febrero de 2000, Amann, 2000-II, Demanda nº 27798/95.

([2]) Sentencia del TEDH de 2 de agosto de 1984, Malone, A82, Demanda nº 8691/79.

([3]) Sentencia del TEDH de 22 de octubre de 1981, Dudgeon, A45, Demanda nº 7525/76.

apremiante que respete el criterio de la sentencia Dudgeon. Se debe demostrar la necesidad y la proporcionalidad de la obligación de retener datos, en su sentido más extenso.

11. Además, la propuesta tiene un impacto enorme sobre los principios de protección de datos reconocidos por el Derecho comunitario:

— hay que retener los datos durante un plazo mucho más largo que los plazos que son habituales para la retención por los proveedores de servicios de las comunicaciones electrónicas públicamente disponibles o por una red de comunicaciones públicas (en lo sucesivo se hará referencia a ambos servicios como «proveedores»),

— conforme a la Directiva 2002/58/CE, más en especial a su artículo 6, los datos sólo se pueden recoger y almacenar por motivos relacionados directamente con la propia comunicación, incluso a efectos de facturación ([1]). Más tarde, los datos deben borrarse (sin perjuicio de las excepciones). Conforme a la actual propuesta, la retención a efectos de la aplicación del Derecho penal es obligatoria. Así pues, el punto de partida es contrario,

— la Directiva 2002/58/CE garantiza la seguridad y la confidencialidad. Esta propuesta no puede crear lagunas en ese campo; se requieren salvaguardias estrictas y debe aclararse la delimitación de la finalidad,

— la introducción de la obligación de retener datos, según lo previsto por la propuesta, se traduce en bases de datos sustanciales y conlleva riesgos particulares para la persona objeto de los datos. Cabría pensar en el uso comercial de los datos, así como en el uso de los datos para las operaciones de búsqueda aleatoria de información y/o de la extracción de los datos por parte de las autoridades policiales y aduaneras o de los servicios de seguridad nacional.

12. Finalmente, tanto la protección de la intimidad como la protección de datos personales han sido reconocidas en la Carta de los Derechos Fundamentales, como se ha mencionado en la exposición de motivos.

13. El impacto de la propuesta sobre la protección de datos personales requiere un análisis completo. En este análisis, el SEPD tomará los elementos anteriormente mencionados en consideración y llegará a la conclusión de que son necesarias más salvaguardias. Una simple referencia al marco jurídico vigente en relación con la protección de datos no es suficiente (en especial, las Directivas 95/46/CE y 2002/58/CE).

Necesidad de la retención de los datos de tráfico y de localización

14. El SEPD recuerda la conclusión, de 9 de noviembre de 2004, del Grupo de protección de datos del artículo 29 sobre el proyecto de Decisión marco. El Grupo declaró que no es aceptable la retención obligatoria de los datos de tráfico, bajo las condiciones previstas en el proyecto de Decisión marco. Esta conclusión se basó, entre otras cosas, en la imposibilidad de facilitar cualquier prueba en lo que se refiere a la necesidad de la retención a efectos de orden público, ya que el análisis mostró que la mayoría de los datos de tráfico exigidos por los servicios policiales no superaba los seis meses.

15. Según el SEPD, las consideraciones del Grupo de protección de datos del artículo 29 mencionado anteriormente deben ser el punto de partida para la valoración de la actual propuesta. Sin embargo, el resultado de dichas consideraciones no puede transponerse sin más a la presente propuesta. Tiene que tenerse en cuenta que las circunstancias pueden cambiar. Según el SEPD, los siguientes desarrollos podrían ser pertinentes para la valoración.

16. En primer lugar, se han presentado algunas cifras para demostrar que, en la práctica, los servicios policiales reclaman datos de tráfico de una antigüedad máxima de un año. Tanto la Comisión como la Presidencia del Consejo conceden importancia a un estudio de la policía del Reino Unido ([2]) que muestra que aunque el 85 % de los datos de tráfico requeridos por la policía tengan un máximo de seis meses de antigüedad, los datos de entre seis meses y un año se utilizan en investigaciones complejas de delitos más graves. Se han presentado igualmente algunos ejemplos de casos. El plazo de retención en la propuesta —de un año para datos telefónicos — refleja estas prácticas de los servicios policiales.

17. El SEPD no está convencido de que estas cifras representen las pruebas de la necesidad de la retención hasta un año de los datos de tráfico. El hecho de que en algunos casos la disponibilidad de los datos del tráfico y/o de localización ayudara a resolver un delito no significa automáticamente que esos datos sean necesarios, en general, como instrumento para los servicios policiales. Sin embargo, no pueden ignorarse las cifras. Representan por lo menos una tentativa seria de demostrar la necesidad de la retención. Por otra parte, las cifras indican claramente que no se requiere un plazo de retención de más de un año desde la perspectiva de las prácticas corrientes de los servicios policiales.

18. En segundo lugar, los proveedores no utilizan siempre las posibilidades de que disponen conforme a la Directiva 2002/58/CE para retener datos de tráfico a efectos de facturación, dado que en un número cada vez mayor de casos no se realiza en absoluto la retención de datos a efectos de facturación (tarjetas de prepago para comunicaciones desde teléfonos móviles, suscripciones a tarifas planas, etc.). En esos

([1]) Véase también el punto 3 del presente Dictamen.

([2]) *Liberty and security, striking the right balance* (Libertad y seguridad: mantener un equilibrio adecuado). Documento de la Presidencia británica de la Unión Europea de 7 de septiembre de 2005.

casos —que en la práctica están llegando a ser cada vez más frecuentes— los datos de tráfico y de localización no se almacenarán en absoluto sino que se borrarán inmediatamente después de la comunicación. Lo mismo ocurre con las llamadas infructuosas. Esto puede tener un impacto sobre la eficacia de los servicios policiales.

19. Por otra parte, este desarrollo en servicios de telecomunicaciones puede generar perturbaciones en el funcionamiento del mercado interior, entre otras cosas debido a la adopción (inminente) de medidas legislativas en los Estados miembros de conformidad con el artículo 15 de la Directiva 2002/58/CE. Por ejemplo, el Gobierno italiano publicó recientemente un decreto que obliga a los proveedores a almacenar datos telefónicos durante cuatro años. Esta obligación acarreará considerables costes en determinados Estados miembros, como Italia.

20. En tercer lugar, los métodos de trabajo de las autoridades policiales se han desarrollado también: las investigaciones proactivas y el uso del apoyo técnico se han vuelto más importantes. Estos progresos requieren que las autoridades dispongan de instrumentos adecuados y formulados con precisión para que puedan trabajar con el debido respeto a los principios de la protección de datos. Uno de los instrumentos de que disponen generalmente las autoridades de los Estados miembros es la preservación de los datos o congelación de los datos de las comunicaciones solicitados en una investigación concreta. Se ha puesto de relieve que este instrumento, que en sí mismo tiene menos impacto sobre esos principios que el instrumento que se propone ahora (retención de datos), podría no ser siempre suficiente, en especial por no seguir la pista de las personas implicadas en el terrorismo u otros delitos graves que no hayan sido sospechosas previamente de ninguna actividad delictiva. Sin embargo, son necesarias más pruebas para determinar si éste es realmente el caso.

21. En cuarto lugar, ha aumentado la preocupación por los atentados terroristas. El SEPD comparte el punto de vista, tal como se expresa en el contexto de las propuestas sobre la retención de datos, de que la seguridad física tiene, en cuanto tal, una importancia máxima. La sociedad necesita protegerse. Por esta razón los Gobiernos tienen la obligación, en caso de ataques contra la sociedad, de demostrar que conceden la mayor consideración a esta necesidad de protección y de investigar si tienen que reaccionar introduciendo nuevas medidas legislativas. Es evidente que el SEPD aprueba completamente el esfuerzo de los Gobiernos —tanto a nivel nacional como europeo— para proteger a la sociedad y para demostrar que hacen todo lo necesario para asegurar la protección, inclusive mediante la adopción de nuevas medidas, legítimas y eficaces, como consecuencia de sus investigaciones.

22. El SEPD reconoce que las circunstancias cambian, pero por ahora no está convencido de la necesidad de la retención de datos de tráfico y de localización a efectos policiales, según lo establecido en la propuesta. Pone de relieve la importancia del principio jurídico establecido por la Directiva 2002/58/CE de que los datos de tráfico deben borrarse en cuanto el almacenamiento ya no sea necesario para fines que no estén relacionados con la propia comunicación. Además, las cifras facilitadas no prueban que el marco jurídico existente no ofrezca los instrumentos que son necesarios para proteger la seguridad física, ni que los Estados miembros ejerzan plenamente sus competencias conforme a la legislación europea para cooperar según les garantiza el marco jurídico vigente (pero sin los resultados necesarios).

23. Sin embargo, si el Parlamento Europeo y el Consejo, tras haber sopesado cuidadosamente los intereses en juego, llegan a la conclusión de que la necesidad de la retención de los datos de tráfico y de localización está suficientemente demostrada, el SEPD considera que la retención sólo puede justificarse conforme al Derecho comunitario en la medida en que se respete el principio de proporcionalidad y se otorguen las salvaguardias adecuadas, de conformidad con el presente Dictamen.

La proporcionalidad

24. La proporcionalidad de la medida legislativa propuesta en sí depende de la sustancia de las disposiciones que comprende: ¿aporta la propuesta una respuesta adecuada y proporcionada a las necesidades de la sociedad?

25. La primera consideración tiene que ver con la adecuación de la propuesta: ¿cabe esperar que la propuesta aumente la seguridad física de los habitantes de la Unión Europea? Una razón para poner en duda la adecuación, a menudo mencionada en el debate público, es que los datos de tráfico y los datos de localización no están siempre ligados a un individuo específico, por lo que conocer un número de teléfono, o un número de acceso a Internet, no revela necesariamente la identidad de un individuo. Otro motivo de duda, más grave aún, es si efectivamente la existencia de bases de datos gigantescas permite que los servicios policiales encuentren fácilmente lo que necesitan en un caso dado.

26. El SEPD considera que la sola retención de datos de tráfico y de localización no constituye por sí misma una respuesta adecuada o eficaz. Son necesarias medidas adicionales, a fin de asegurar a las autoridades un acceso directo y rápido a los datos necesarios en un caso concreto. La retención de datos sólo es adecuada y eficaz en la medida en que existen motores de búsqueda eficaces.

27. La segunda consideración se refiere a la proporcionalidad de la respuesta. Para ser proporcional, la propuesta debe:

— limitar los plazos de retención. Los plazos tienen que reflejar las necesidades demostradas de los servicios policiales,

— limitar la cantidad de datos que deben almacenarse. Esta cantidad debe reflejar las necesidades demostradas de los servicios policiales y debe asegurarse de que no sea posible acceder a datos de contenido,

— contener medidas de seguridad adecuadas, a fin de limitar el acceso y el uso posterior, garantizar la seguridad de los datos y asegurarse de que las propias personas a las que se refieren los datos puedan ejercer sus derechos.

28. El SEPD subraya la importancia de estas limitaciones estrictas, con salvaguardias adecuadas orientadas a un acceso restringido. Considera que desde la perspectiva de la importancia de los tres elementos mencionados en el punto anterior, los Estados miembros pueden, en lo que se refiere a estos tres elementos, no tomar medidas nacionales adicionales que perjudiquen la proporcionalidad. Se profundizará en esta necesidad de armonización en la sección IV.

Medidas de seguridad adecuadas

29. El efecto de la propuesta será que los proveedores dispondrán de bases de datos en las que se encontrará almacenada una cantidad significativa de datos de tráfico y de localización.

30. En primer lugar, la propuesta tendrá que asegurarse de que el acceso a estos datos y su utilización ulterior se limiten únicamente a determinadas circunstancias y para un número limitado de fines concretos.

31. En segundo lugar, habrá que proteger adecuadamente las bases de datos (seguridad de los datos). Con este fin, debe asegurarse que al final de los plazos de retención los datos se borren efectivamente. No debe haber ningún dumping o explotación de los datos. En pocas palabras, esto requiere un nivel elevado de seguridad de los datos y medidas técnicas y organizativas de seguridad adecuadas.

32. Una protección elevada de los datos es tanto más importante en cuanto que la simple existencia de datos podría llevar a solicitudes de acceso y de uso, por lo menos por parte de tres grupos de interesados:

— los propios proveedores. Les podría tentar el utilizar los datos para sus propios objetivos comerciales. Son necesarias garantías que impidan la reproducción de estos ficheros,

— las autoridades responsables de la aplicación de la ley: la propuesta les ofrece un derecho de acceso, pero solamente en casos específicos y de conformidad con la legislación nacional (artículo 3, apartado 2, de la propuesta). No debe haber ningún acceso a fines de prospección de datos o de operaciones de búsqueda aleatoria de información. El intercambio de datos con las autoridades de otros Estados miembros debe estar regulado de forma clara,

— los servicios de inteligencia (responsables de la seguridad nacional).

33. En lo que se refiere al acceso por los servicios de inteligencia, el SEPD observa que, de conformidad con el artículo 33 del Tratado UE y el artículo 64 del Tratado CE, las intervenciones en el ámbito de los pilares primero y tercero no afectarán al ejercicio de las responsabilidades que incumben a los Estados miembros en materia de mantenimiento del orden público y salvaguardia de la seguridad interior. Según el SEPD, resulta de estas disposiciones que la Unión Europea carece de competencia para controlar el acceso de los servicios de seguridad o inteligencia a los datos retenidos por los proveedores. En otras palabras, la legislación de la Unión Europea no afecta ni al acceso de dichos servicios a los datos de tráfico y de localización de los proveedores ni a la utilización posterior de la información adquirida por dichos servicios. Es éste un elemento que hay que tener en cuenta en la valoración de la propuesta. Son los Estados miembros los que deben tomar las medidas necesarias para regular el acceso de los servicios de inteligencia.

34. En tercer lugar, los efectos descritos en los párrafos anteriores tienen implicaciones potenciales para la persona a la que se refieren los datos. Las salvaguardias adicionales son necesarias a fin de asegurarse de que el interesado pueda ejercer sencilla y rápidamente sus derechos en tanto que persona a la que se refieren los datos. El SEPD señala la necesidad de un control efectivo del acceso y de la utilización posterior, de preferencia por las autoridades judiciales de los Estados miembros. Las salvaguardias deben aplicarse también en el caso del acceso y de la utilización posterior de los datos de tráfico por las autoridades de otros Estados miembros.

35. En este contexto, el SEPD hace referencia a iniciativas para un nuevo marco jurídico relativo a la protección de datos aplicable a los servicios policiales (en el tercer pilar del Tratado UE). En su Dictamen, un marco jurídico tal requiere salvaguardias adicionales y no podría limitarse a una reafirmación de los principios generales de protección de datos del primer pilar ([1]).

36. En cuarto lugar, hay una relación directa entre la adecuación de las medidas de seguridad y los costes de dichas medidas. Una normativa adecuada sobre la retención de los datos debe por lo tanto contener incentivos para que los proveedores inviertan en la infraestructura técnica. Tal incentivo podría consistir en una indemnización a los proveedores por los costes adicionales de las medidas de seguridad adecuadas.

37. En resumen, las medidas de seguridad adecuadas deben:

— limitar el acceso a los datos y su posterior utilización,

— prever medidas técnicas y organizativas de seguridad adecuadas para la protección de las bases de datos. Esto incluye que se borren correctamente los datos al final del

([1]) Véase, en el mismo sentido, el documento de la posición sobre los servicios policiales y el intercambio de información en la UE, adoptado en la Conferencia de primavera de las autoridades europeas encargadas de la protección de datos, Cracovia, 25 y 26 de abril de 2005.

plazo de retención y que diferentes grupos de interesados tomen nota de las solicitudes de acceso y de uso,

— asegurar el ejercicio de los derechos de las personas a las que se refieren los datos, no sólo reafirmando los principios generales de protección de datos,

— contener incentivos para que los proveedores inviertan en la infraestructura técnica.

III. La base jurídica y el proyecto de Decisión marco

38. La propuesta está basada en el Tratado CE y, en concreto, en su artículo 95, y aspira, según su artículo 1, a armonizar las obligaciones de los proveedores en relación con el tratamiento y la retención de los datos de tráfico y de localización. Declara que los datos solamente se proporcionarán a las autoridades nacionales competentes en casos individuales, relacionados con infracciones penales, pero deja a la discreción de los Estados miembros una definición más exacta de su objetivo, así como del acceso a los datos y su posterior utilización, sin perjuicio de las salvaguardias del marco comunitario existente en materia de protección de datos.

39. A este respecto, la propuesta tiene un alcance más limitado que el proyecto de Decisión marco, que está basado en el artículo 31, apartado 1, letra c), del Tratado UE y que contiene disposiciones complementarias sobre el acceso a los datos retenidos, así como sobre peticiones de acceso de otros Estados miembros. La exposición de motivos da una justificación para esta restricción del ámbito de la propuesta. Declara que el acceso y el intercambio de información entre los servicios policiales pertinentes es una cuestión que queda fuera del ámbito del Tratado CE.

40. Al SEPD no le convence esta declaración de la exposición de motivos. Una intervención de la Comunidad basada en el artículo 95 del Tratado CE (mercado interior) debe tener como principal objetivo la supresión de obstáculos al comercio. Según la jurisprudencia del Tribunal de Justicia, tal intervención debe ser auténticamente apropiada para contribuir a la supresión de dicho obstáculo. Sin embargo, en su intervención, el legislador comunitario debe garantizar la observancia de los derechos fundamentales (artículo 6, apartado 2, del Tratado UE; véase la sección II del presente Dictamen). Por todos estos motivos, el establecimiento a nivel comunitario de normas sobre la retención de datos en interés del mercado interior puede requerir que también se trate a nivel de la Comunidad Europea la observancia de los derechos fundamentales. Si el legislador comunitario no pudiera establecer normas sobre el acceso y el uso de datos, no podría cumplir su obligación de conformidad con el artículo 6 del Tratado UE, dado que dichas normas son imprescindibles para asegurarse de que los datos se retengan con el respeto debido a los derechos fundamentales. En otras palabras, en opinión del SEPD las normas sobre el acceso, el uso y el intercambio de datos son inseparables de la propia obligación de conservar los datos.

41. En lo que se refiere a la determinación de las autoridades competentes, el SEPD admite que esta competencia incumbe a los Estados miembros, lo mismo que la organización de los servicios policiales y la protección judicial. Sin embargo, un acto comunitario puede imponer condiciones a los Estados miembros en lo que se refiere a la designación de las autoridades competentes, el control judicial o el acceso de los ciudadanos a la justicia. Estas disposiciones garantizan la existencia de mecanismos convenientes a nivel nacional para garantizar la plena eficacia del acto, incluido el cumplimiento completo de la legislación en materia de protección de datos.

42. El SEPD suscita otra cuestión, relacionada con la base jurídica. Corresponde al legislador comunitario elegir la base jurídica adecuada y, en consecuencia, el procedimiento legislativo adecuado. Esta opción trasciende la misión del SEPD. Sin embargo, habida cuenta de los importantes problemas fundamentales en juego, el SEPD expresa en las condiciones actuales una preferencia marcada por el procedimiento de codecisión. Solamente este procedimiento constituye un proceso transparente de toma de decisiones con la plena participación de las tres instituciones implicadas y con el debido respeto a los principios en que se funda la Unión.

IV. Necesidad de armonización

43. La propuesta de Directiva armoniza los tipos de datos sujetos a retención, los plazos durante los cuales deben retenerse los datos y los fines para los cuales pueden suministrarse los datos a las autoridades competentes. La propuesta prevé la armonización completa de estos elementos. Posee, a este respecto, un carácter fundamentalmente diferente del proyecto de Decisión marco, que establece normas mínimas.

44. El SEPD subraya la necesidad de la armonización completa de estos elementos, teniendo en cuenta el funcionamiento del mercado interior, las necesidades de los servicios policiales y, en último lugar, pero no por ello menos importante, el CEDH y los principios de protección de datos.

45. En lo que se refiere al funcionamiento del mercado interior, la armonización de las obligaciones de retención de datos justifica la elección de la base jurídica de la propuesta (artículo 95 del Tratado CE). Permitir diferencias esenciales entre las leyes de los Estados miembros no eliminaría las perturbaciones existentes en el mercado interior de las comunicaciones electrónicas, que se deben entre otras cosas a la adopción (inminente) de medidas legislativas en los Estados miembros de conformidad con el artículo 15 de la Directiva 2002/58/CE (véase el punto 19 del presente Dictamen).

46. Esto es tanto más importante en cuanto que para una gran cantidad de comunicaciones electrónicas es competente la jurisdicción de más de un Estado miembro. Ejemplos ilustrativos son: las llamadas telefónicas transfronterizas, la itinerancia de las comunicaciones, el cruce de fronteras *durante* las comunicaciones móviles y el uso de un proveedor en otro Estado miembro que el país de residencia del individuo.

47. Además, la falta de armonización en este contexto perjudicaría las necesidades de los servicios policiales, en la medida en que las autoridades competentes tienen que cumplir diversos requisitos legales. Esto podría dificultar el intercambio de información entre las autoridades de los Estados miembros.

48. Finalmente, el SEPD pone de relieve —haciendo referencia a su responsabilidad según el artículo 41 del Reglamento (CE) nº 45/2001— que la armonización integral de los elementos principales incluidos en la propuesta es imprescindible para cumplir con el CEDH y los principios de protección de datos. Cualquier medida legislativa que obligue a retener los datos de tráfico y de localización tiene que delimitar claramente el número de datos que deben retenerse, los plazos de retención y (los fines de) acceso y posterior utilización de los datos, para que sea aceptable desde la perspectiva de la protección de datos y para cumplir con los requisitos de necesidad y de proporcionalidad.

V. Comentarios sobre los artículos de la propuesta

Artículo 3: obligación de retener datos

49. El artículo 3 es la disposición clave de la propuesta. El artículo 3, apartado 1, introduce la obligación de retener datos de tráfico y datos de localización, mientras que el artículo 3, apartado 2, da efecto al principio de restricción de la finalidad. El artículo 3, apartado 2, establece tres restricciones importantes. Los datos retenidos se proporcionarán únicamente:

— a las autoridades nacionales competentes,

— en casos específicos,

— para la prevención, investigación, detección y procesamiento de infracciones penales graves, tales como terrorismo y delincuencia organizada.

El artículo 3, apartado 2, remite a la legislación nacional de los Estados miembros para la especificación de otras restricciones.

50. El SEPD acoge con satisfacción el artículo 3, apartado 2, como disposición importante, pero considera que las limitaciones no son lo suficientemente precisas, que el acceso y la utilización posterior deben regularse explícitamente conforme a la Directiva y que son necesarias salvaguardias adicionales. Como se ha dicho en la sección III del presente Dictamen, el SEPD no está convencido de que la no inclusión de disposiciones (precisas) sobre el acceso y la posterior utilización de los datos de tráfico y de localización sea una consecuencia inevitable de la base jurídica de la propuesta (artículo 95 del Tratado CE). Esto lleva a los siguientes comentarios.

51. En primer lugar, no se especifica que otros interesados, como el proveedor mismo, no tengan acceso a los datos. De conformidad con el artículo 6 de la Directiva 2002/58/CE, los proveedores sólo pueden tratar datos de tráfico hasta el final del plazo en el que los datos se retienen a efectos de facturación. Según el SEPD no existe justificación alguna para que los proveedores u otras partes interesadas tengan un acceso diferente del previsto conforme a la Directiva 2002/58/CE y supeditado a las condiciones establecidas en dicha Directiva.

52. El SEPD recomienda que se añada una disposición en el texto para asegurarse de que los individuos distintos de las autoridades competentes no tengan acceso a los datos. Esta disposición podría formularse del siguiente modo: «solamente se podrá acceder o tratar los datos para el objetivo establecido en el artículo 3, apartado 2» o «los proveedores garantizarán efectivamente que el acceso solamente se concede a las autoridades competentes».

53. En segundo lugar, la limitación a casos específicos parece prohibir el acceso rutinario a operaciones de búsqueda aleatoria de información o a actividades de prospección de datos. Sin embargo, el texto de la propuesta debería especificar que los datos sólo pueden proporcionarse cuando sea necesario en relación con una infracción penal concreta.

54. En tercer lugar, el SEPD acoge con satisfacción que la finalidad del acceso se restrinja a infracciones penales graves, tales como el terrorismo y la delincuencia organizada. En otros casos menos graves, el acceso a los datos de tráfico o de localización no se proporcionará fácilmente. Sin embargo, el SEPD duda que esta limitación sea lo suficientemente precisa, especialmente cuando se solicite el acceso en relación con un delito grave distinto del terrorismo y la delincuencia organizada. La práctica en los Estados miembros será divergente. El SEPD ha puesto de relieve en la sección IV del presente Dictamen la necesidad de la armonización completa de los principales elementos incluidos en la propuesta. El SEPD recomienda por lo tanto que la disposición se limite a *determinadas* infracciones penales graves.

55. En cuarto lugar, al contrario que el proyecto de Decisión marco, la propuesta no contiene una disposición sobre el acceso. En opinión del SEPD, el acceso y la posterior utilización de los datos no deberían omitirse en la Directiva, por formar parte inseparable del asunto (véase la sección III del presente Dictamen).

56. El SEPD recomienda la adición a la propuesta de uno o más artículos sobre el acceso a los datos de tráfico y de localización por parte de las autoridades competentes y sobre la utilización posterior de los datos. El objetivo de estos artículos debería ser asegurarse de que los datos se utilizan únicamente para los fines mencionados en el artículo 3, apartado 2, de que las autoridades garantizan la calidad, la confidencialidad y la seguridad de los datos que han obtenido y de que dichos datos se borrarán cuando ya no sean

necesarios para la prevención, investigación, detección y procesamiento de la infracción penal concreta. Por otra parte, debería establecerse que el acceso en casos específicos debería estar supeditado al control judicial en los Estados miembros.

57. En quinto lugar, la propuesta no contiene salvaguardias adicionales para la protección de datos. Los considerandos hacen simplemente referencia a salvaguardias de la legislación existente y más en concreto a la Directiva 95/46/CE y a la Directiva 2002/58/CE. El SEPD discrepa con este planteamiento limitado de la protección de datos a pesar de la importancia particular de las salvaguardias (adicionales) (véase la sección II del presente Dictamen).

58. Por lo tanto, el SEPD recomienda que se incluya un apartado en materia de protección de datos. En dicho apartado podrían insertarse las recomendaciones anteriores referentes al artículo 3, apartado 2, así como otras disposiciones sobre la protección de datos, tal como disposiciones relacionadas con el ejercicio de sus derechos por parte de las personas a las que se refieren los datos (véase la sección II del presente Dictamen), con la calidad y la seguridad de los datos, y con los datos de tráfico y de localización de personas no sospechosas de infracciones penales.

Artículo 4: categorías de datos que deben retenerse

59. En líneas generales, el SEPD acoge con satisfacción el artículo y el anexo, a causa de:

— la técnica legislativa elegida, con descripciones funcionales en el articulado de la Directiva y con detalles técnicos en un anexo. Es suficientemente flexible para responder de forma adecuada a los progresos tecnológicos y da seguridad jurídica al ciudadano,

— la distinción entre los datos sobre telecomunicaciones y los datos de Internet, a pesar del hecho de que la distinción llegue a ser tecnológicamente menos importante. Sin embargo, desde la perspectiva de la protección de datos, la distinción es importante, dado que en Internet no está bien delimitada la frontera entre datos de contenido y datos de tráfico (véase, por ejemplo, el reconocimiento en el artículo 1, apartado 2, de la Directiva de que la información consultada en Internet se considera datos de contenido),

— el nivel de armonización: la propuesta prevé un alto nivel de armonización con una lista exhaustiva de las categorías de los datos que deben retenerse (por oposición al proyecto de Decisión marco, que contiene una lista mínima con un margen amplio para que los Estados miembros añadan datos). Desde la perspectiva de la protección de datos, la armonización completa es esencial (véase la sección IV).

60. El SEPD recomienda las siguientes modificaciones:

— el artículo 4, párrafo segundo, debe contener criterios más sustanciales para asegurarse de que no estén incluidos los datos de contenido. Debe añadirse la siguiente frase: «El anexo no podrá incluir datos que revelen el contenido de una comunicación.»,

— el artículo 5 abre la posibilidad de revisión del anexo por una directiva de la Comisión («comitología»). El SEPD aconseja que las revisiones del anexo con un impacto significativo en la protección de datos se hagan de preferencia mediante una directiva, de conformidad con el procedimiento de codecisión ([1]).

Artículo 7: plazos de retención

61. El SEPD acoge con satisfacción que los plazos de retención en la propuesta sean perceptiblemente más cortos que los plazos previstos en el proyecto de Decisión marco:

— recordando las dudas expresadas en el presente Dictamen sobre la prueba de la necesidad de la retención de datos de tráfico hasta un año, el plazo de un año refleja las prácticas de los servicios policiales, *por haberse indicado* mediante las cifras proporcionadas por la Comisión y la Presidencia del Consejo,

— estas cifras muestran igualmente que, salvo en casos excepcionales, la retención de datos durante períodos más largos no refleja las prácticas de los servicios policiales,

— un plazo más corto de seis meses para los datos relacionados con las comunicaciones electrónicas efectuadas utilizando única o principalmente el protocolo de Internet es importante desde la perspectiva de la protección de datos, puesto que la retención de resultados de las comunicaciones de Internet en vastas bases de datos (estos datos generalmente no se retienen a efectos de facturación), la distinción con los datos de contenido es vaga y la retención durante más de seis meses no refleja las prácticas de los servicios policiales.

62. Debe aclararse en el texto que:

— los plazos de retención de seis meses y de un año son plazos máximos de retención,

([1]) Véase, en el mismo sentido, el Dictamen del SEPD de 23 de marzo de 2005 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el sistema de información de visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros (punto 3.12).

— los datos se borran al final del plazo de retención. El texto debería aclarar también cómo deben borrarse los datos. Según el SEPD, el proveedor tiene que borrar los datos por medios automatizados, por lo menos a diario.

Artículo 8: requisitos de almacenamiento para datos retenidos

63. Este artículo está estrechamente relacionado con el artículo 3, apartado 2, y contiene una disposición importante capaz de asegurar que el acceso en casos específicos pueda limitarse a los datos que son específicamente necesarios. El artículo 8 y el artículo 3, apartado 2, presuponen que los datos requeridos son transmitidos por los proveedores a las autoridades y que estas últimas no tienen acceso directo a las bases de datos. El SEPD recomienda que se establezca esta presunción explícitamente en el texto.

64. La disposición debe especificarse, previendo que:

— los datos requeridos son transmitidos por los proveedores a las autoridades (véase el punto 63),

— los proveedores deben instalar el entramado técnico necesario, incluidos motores de búsqueda, para facilitar el acceso directo a los datos específicos,

— los proveedores deben asegurarse de que solamente los miembros de su personal con responsabilidades técnicas específicas tengan acceso a las bases de datos por motivos técnicos, y de que esos miembros del personal son conscientes del carácter sensible de los datos y trabajan subordinados a normas internas estrictas de confidencialidad,

— la transmisión de los datos no sólo debe efectuarse sin retraso injustificado, sino también sin revelar otros datos de tráfico y de localización distintos de los datos necesarios a efectos de la solicitud.

Artículo 9: estadísticas

65. La obligación de que los proveedores suministren estadísticas anualmente ayuda a las instituciones comunitarias a supervisar la eficacia de la ejecución y aplicación de la presente propuesta. Es necesaria una información adecuada.

66. Según el SEPD, esta obligación da efecto al principio de transparencia. El ciudadano europeo tiene derecho a saber cuál es la eficacia de la retención de los datos. Por esta razón, el proveedor debe además tener la obligación de seguir manteniendo listas de enlaces y de llevar a cabo auditorías (internas) sistemáticas, para permitir que las autoridades nacionales de protección de datos controlen en la práctica la aplicación de las normas relativas a la protección de datos ([1]). La propuesta debería modificarse en este sentido.

Artículo 10: costes

67. Como se ha dicho en la sección II, hay una relación directa entre la adecuación de las medidas de seguridad y los costes de estas medidas, es decir, entre la seguridad y los costes. El SEPD considera por lo tanto el artículo 10, que prevé el reembolso de los costes adicionales comprobados, como una disposición importante que podría servir de incentivo para que los proveedores inviertan en la infraestructura técnica.

68. Según las estimaciones de la evaluación de impacto trasmitida por la Comisión al SEPD, los costes de la retención de los datos son considerables. Para una red y un proveedor de servicios de grandes dimensiones, los costes ascenderían a más de 150 millones EUR para un plazo de retención de doce meses, con costes de funcionamiento anuales de alrededor de 50 millones EUR ([2]). Por el contrario, no existen cifras en lo que se refiere a costes de medidas de seguridad adicionales, tales como motores de búsqueda costosos (véase el comentario sobre el artículo 6), ni sobre las consecuencias financieras (estimadas) del reembolso total de los costes adicionales de los proveedores.

69. Según el SEPD son necesarias cifras más precisas para poder juzgar la propuesta en toda su extensión. Sugiere que se aclaren las consecuencias financieras de la propuesta en la exposición de motivos.

70. En lo que se refiere a lo dispuesto en el propio artículo 10, la relación entre la adecuación de las medidas de seguridad y los costes debe precisarse en el texto de la disposición. Por otra parte, la propuesta debe establecer normas mínimas para las medidas de seguridad que deben ser tomadas por los proveedores, a fin de tener derecho a un reembolso por un Estado miembro. A juicio del SEPD, la determinación de estas normas no podría dejarse completa-

([1]) Véase, en el mismo sentido, el Dictamen del SEPD de 23 de marzo de 2005 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el sistema de información de visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros (punto 3.9).

([2]) La Comisión se refiere a cifras de la ETNO (Asociación europea de operadores de telecomunicaciones) y a un informe del diputado europeo Alvaro sobre el proyecto de Decisión marco.

mente a los Estados miembros. Esto podría perjudicar el grado de armonización previsto por la Directiva. Además, debe tenerse en cuenta que los Estados miembros cargan con las consecuencias financieras del reembolso.

Artículo 11: modificación de la Directiva 2002/58/CE

71. Debe aclararse la relación con el artículo 15, apartado 1, de la Directiva 2002/58/CE, ya que esta propuesta priva a la disposición mencionada de una buena parte de su contenido. Deben suprimirse las referencias en el artículo 15, apartado 1, de la Directiva 2002/58/CE al artículo 6 y al artículo 9 (de esa misma Directiva), o por lo menos modificarse para aclarar que los Estados miembros ya no son competentes para adoptar legislación en relación con infracciones penales, adicional a la propuesta actual. Es preciso eliminar toda ambigüedad en sus competencias restantes, por ejemplo por lo que se refiere a la retención de datos a efectos de infracciones penales «no graves».

Artículo 12: evaluación

72. El SEPD acoge con satisfacción que la propuesta contenga un artículo sobre la evaluación de la Directiva, en un plazo de tres años tras su entrada en vigor. Una evaluación reviste la mayor importancia en la perspectiva de las dudas sobre la necesidad de la propuesta y de su proporcionalidad.

73. En esta perspectiva, el SEPD aconseja que se prevea una obligación aún más estricta, que contenga los siguientes elementos:

— la evaluación debería comprender un diagnóstico de la eficacia de la aplicación de la Directiva, desde la perspectiva de los servicios policiales, así como un diagnóstico del impacto en los derechos fundamentales de las personas a las que se refieren los datos. La Comisión debe incluir cualquier prueba que pueda afectar a la evaluación,

— la evaluación debería tener lugar periódicamente (por lo menos cada dos años),

— la Comisión debería tener la obligación de presentar modificaciones a la propuesta, siempre que resulte conveniente (como en el artículo 18 de la Directiva 2002/58/CE).

VI. **Conclusiones**

Condiciones previas

74. Es esencial para el SEPD que la propuesta respete los derechos fundamentales. Una medida legislativa que perjudique la protección garantizada por el Derecho comunitario y, más en especial, por la jurisprudencia del Tribunal de Justicia y del Tribunal Europeo de Derechos Humanos no sólo es inaceptable, sino que también es ilegal.

75. Se debe demostrar la necesidad y la proporcionalidad de la obligación de retener datos en toda su extensión.

76. En lo que se refiere a la necesidad: el SEPD reconoce los cambios de circunstancias, pero no está convencido, por el momento, de la necesidad de la retención de los datos de tráfico y de localización a efectos de los servicios policiales, según lo establecido en la propuesta.

77. Sin embargo, el SEPD presenta en el presente Dictamen su punto de vista sobre la proporcionalidad de la propuesta. Esto significa, en primer lugar, que la mera retención de datos de tráfico y de localización no constituye por sí misma una respuesta adecuada o eficaz. Se requieren medidas adicionales, a fin de asegurarse de que las autoridades tengan un acceso directo y rápido a los datos necesarios en un caso específico. En segundo lugar, la propuesta debe:

— limitar los plazos de retención. Los plazos deben reflejar las necesidades de los servicios policiales,

— limitar el volumen de datos que deben almacenarse. Este volumen debe reflejar las necesidades de los servicios policiales y asegurarse de que no sea posible acceder a datos de contenido,

— contener las medidas de seguridad adecuadas.

Valoración general

78. El SEPD subraya la importancia del hecho de que el actual texto de la propuesta prevea una armonización completa de los principales elementos de la propuesta, en especial los tipos de datos que deben retenerse, los plazos de tiempo durante los cuales los datos deben retenerse, así como (las finalidades de) el acceso y la utilización posterior de los datos.

79. En algunos puntos son necesarias otras clarificaciones, por ejemplo para asegurar que se borren adecuadamente los datos al final de un plazo de retención y para prevenir eficazmente el acceso y el uso por diversos grupos de interesados.

80. El SEPD considera esenciales los siguientes puntos, para que la propuesta sea aceptable desde la perspectiva de la protección de datos:

— la adición a la propuesta de disposiciones específicas sobre el acceso a los datos de tráfico y de localización de las autoridades competentes y sobre la utilización posterior de los datos, como parte esencial e inseparable del asunto,

— la adición a la propuesta de otras salvaguardias adicionales para la protección de datos (por oposición a una simple referencia a salvaguardias en la legislación vigente, más en particular en las Directivas 95/46/CE y 2002/58/CE), entre otras cosas para garantizar el ejercicio de los derechos de las personas a las que se refieren los datos,

— la adición a la propuesta de otros incentivos a los proveedores que inviertan en una infraestructura técnica adecuada, incluidos incentivos financieros. Esta infraestructura sólo puede ser adecuada si existen motores de búsqueda eficaces.

Recomendaciones para modificaciones de la propuesta

81. En lo que se refiere al artículo 3, apartado 2:

— adición de una disposición para asegurarse de que los individuos distintos de las autoridades competentes no tengan acceso a los datos. Esta disposición podría formularse del siguiente modo: «solamente se podrá tener acceso a los datos y/o a su tratamiento para los fines mencionados en el artículo 3, apartado 2» o «los proveedores garantizarán efectivamente que el acceso sólo se conceda a las autoridades competentes»,

— especificación de que los datos solamente pueden proporcionarse cuando sea necesario en relación con una infracción penal específica,

— limitación de la disposición a *determinadas* infracciones penales graves,

— adición a la propuesta de uno o más artículos sobre el acceso a los datos de tráfico y de localización de las autoridades competentes y sobre la posterior utilización de los mismos, así como de una disposición en el sentido de que el acceso en casos específicos debe estar supeditado al control judicial en los Estados miembros,

— inclusión de un apartado relativo a la protección de datos.

82. En lo que se refiere a los artículos 4 y 5:

— adición al artículo 4, segundo párrafo, de la siguiente frase: «El anexo no podrá incluir datos que revelen el contenido de una comunicación.»,

— especificación de que las revisiones del anexo con un impacto sustancial en la protección de datos deben hacerse de preferencia mediante una Directiva, de conformidad con el procedimiento de codecisión.

83. En lo que se refiere al artículo 7, una especificación en el texto de que:

— los plazos de retención de seis meses y de un año son plazos máximos de retención,

— los datos se borran al final del plazo de retención. El texto debería aclarar también cómo deben borrarse los datos, a saber, por el proveedor, a través de medios automatizados, por lo menos a diario.

84. En cuanto al artículo 8, una especificación en el texto de que:

— los datos requeridos son transmitidos por los proveedores a las autoridades,

— los proveedores deben instalar el entramado técnico necesario, incluidos los motores de búsqueda, para facilitar el acceso directo a los datos específicos,

— los proveedores deben asegurarse de que solamente los miembros de su personal con responsabilidades técnicas específicas tienen acceso a las bases de datos por razones técnicas, y de que esos miembros del personal son conscientes del carácter sensible de los datos y trabajan supeditados a normas internas estrictas de confidencialidad,

— la transmisión de los datos no sólo debe efectuarse sin retraso injustificado, sino también sin revelar otros datos de tráfico y de localización distintos de los datos necesarios a efectos de la solicitud.

85. En lo que se refiere al artículo 9:

— la adición de una disposición que obligue al proveedor a seguir manteniendo listas de enlaces y a llevar a cabo auditorías (internas) sistemáticas, para permitir que las autoridades nacionales de protección de datos controlen en la práctica la aplicación de las normas relativas a la protección de datos.

86. En lo que se refiere al artículo 10:

— debe aclararse en el texto de la disposición la relación entre la adecuación de las medidas de seguridad y los costes,

— adición de normas mínimas para que sean tomadas por los proveedores las medidas de seguridad a fin de tener derecho a un reembolso por un Estado miembro,

— clarificación de las consecuencias financieras de la propuesta en la exposición de motivos.

87. En lo que se refiere al artículo 11:

— modificación del artículo 15, apartado 1, de la Directiva 2002/58/CE para suprimir las referencias al artículo 6 y al artículo 9 (de esa misma Directiva), o por lo menos modificarlas para aclarar que los Estados miembros ya no son competentes para adoptar legislación en relación con infracciones penales, adicional a la propuesta actual.

88. En lo que se refiere al artículo 12, modificación de la disposición relativa a la evaluación:

— debería incluir un diagnóstico de la eficacia de la aplicación de la Directiva,

— debería tener lugar periódicamente (por lo menos cada dos años)

— la Comisión debería tener la obligación de presentar modificaciones a la propuesta, siempre que lo considere oportuno (como prevé el artículo 18 de la Directiva 2002/58/CE).

Hecho en Bruselas, el 26 de septiembre de 2005.

Peter HUSTINX

Supervisor Europeo de Protección de Datos