

I

(Resoluciones, recomendaciones y dictámenes)

DICTÁMENES

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Dictamen del Supervisor Europeo de Protección de Datos sobre la iniciativa del Reino de Bélgica, la República de Bulgaria, la República de Estonia, el Reino de España, la República Francesa, la República Italiana, la República de Hungría, la República de Polonia, la República Portuguesa, Rumanía, la República de Finlandia y el Reino de Suecia con vistas a la adopción de la Directiva del Parlamento Europeo y del Consejo sobre la orden europea de protección, y sobre la iniciativa del Reino de Bélgica, la República de Bulgaria, la República de Estonia, el Reino de España, la República de Austria, la República de Eslovenia y el Reino de Suecia para una Directiva del Parlamento Europeo y del Consejo relativa al exhorto europeo de investigación en materia penal

(2010/C 355/01)

EL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS,

HA ADOPTADO EL SIGUIENTE DICTAMEN:

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, su artículo 16,

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

Vista la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos ⁽¹⁾,

Visto el Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos y, en particular, su artículo 41 ⁽²⁾,

Vista la Decisión marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal ⁽³⁾,

⁽¹⁾ DO L 281 de 23.11.1995, p. 31.

⁽²⁾ DO L 8 de 12.1.2001, p. 1.

⁽³⁾ DO L 350 de 30.12.2008, p. 60.

I. INTRODUCCIÓN

1. En los últimos años se han redoblado los esfuerzos para mejorar la cooperación judicial en materia penal. Esta materia, que actualmente ocupa una posición clave en el Programa de Estocolmo ⁽⁴⁾, se caracteriza por la especial protección de los datos personales afectados y los efectos que el correspondiente tratamiento de datos pueda tener en los titulares de los datos.
2. Por este motivo, el Supervisor Europeo de Protección de Datos (SEPD) ha prestado una especial atención sobre esta materia ⁽⁵⁾ y, mediante el presente dictamen, pretende una vez más poner énfasis en la necesidad de proteger los derechos fundamentales como piedra angular del Espacio de Libertad, Seguridad y Justicia (ELSJ), de conformidad con lo establecido en el Programa de Estocolmo.
3. El presente dictamen trata sobre dos iniciativas para una Directiva de una serie de Estados miembros, de conformidad con lo previsto en el artículo 76 del Tratado de Funcionamiento de la Unión Europea (TFUE), en particular:

⁽⁴⁾ Consejo Europeo, Programa de Estocolmo — Una Europa abierta y segura que sirva y proteja al ciudadano (2010/C 115/01), Capítulo 3, «Facilitar la vida a las personas: Una Europa de la ley y la justicia», DO C 115 de 4.5.2010, p. 1; véase también el Dictamen del Supervisor Europeo de Protección de Datos sobre la comunicación de la Comisión al Parlamento Europeo y al Consejo relativa a un espacio de libertad, seguridad y justicia al servicio de los ciudadanos, DO C 276 de 17.11.2009, p. 8.

⁽⁵⁾ El SEPD ha adoptado en los últimos años un gran número de dictámenes y observaciones acerca de iniciativas en el espacio de libertad, seguridad y justicia que pueden encontrarse en el sitio web del SEPD.

- a) la iniciativa de doce Estados miembros para una Directiva del Parlamento Europeo y del Consejo sobre la orden europea de protección («iniciativa OEP»), presentada en enero de 2010 ⁽⁶⁾, y
- b) la iniciativa de siete Estados miembros para una Directiva del Parlamento Europeo y del Consejo relativa al exhorto europeo de investigación en materia penal («iniciativa EEL»), presentada en abril de 2010 ⁽⁷⁾.
4. El asesoramiento en relación con estas iniciativas está comprendido en la responsabilidad atribuida por el artículo 41 del Reglamento (CE) n° 45/2001 al SEPD de asesorar a las instituciones y a los organismos de la Unión Europea en todas las cuestiones relacionadas con el tratamiento de datos personales. Por tanto, el presente dictamen emite observaciones sobre las iniciativas en lo que respecta al tratamiento de datos personales. Dado que en esta ocasión no ha sido solicitada la opinión del SEPD, el presente dictamen se emite por iniciativa propia ⁽⁸⁾.
5. El SEPD recuerda que en virtud del artículo 28, apartado 2, del Reglamento (CE) n° 45/2001, la Comisión está obligada a consultar al SEPD al adoptar una propuesta legislativa relativa a la protección de los derechos y libertades de las personas en relación con el tratamiento de datos personales. En el caso de una iniciativa de los Estados miembros esta obligación no se aplica de manera estricta. Sin embargo, desde la entrada en vigor del Tratado de Lisboa, el procedimiento legislativo ordinario también se aplica a la cooperación policial y judicial, con una única excepción específica prevista en el artículo 76 TFUE, a saber, que un cuarto de los Estados miembros adopte una iniciativa para establecer medidas en el ámbito de la Unión. Con arreglo al Tratado de Lisboa, estas iniciativas se acomodarán, tanto como sea posible, a las propuestas de la Comisión y deberán utilizarse, cuando sea posible, las garantías procedimentales. Por este motivo, dichas iniciativas van acompañadas de una evaluación del impacto.
6. En este contexto, el SEPD no sólo lamenta no haber sido consultado en el momento en que se emitieron las iniciativas, sino que recomienda al Consejo que establezca un procedimiento en el que se consulte al SEPD en los casos en que una iniciativa de los Estados miembros esté relacionada con el tratamiento de datos personales.
7. Aunque estas dos iniciativas tienen objetivos diferentes —es decir, mejorar la protección de las víctimas y la cooperación transfronteriza en materia penal a través de la obtención transfronteriza de pruebas— ambas tienen importantes similitudes:
- a) están basadas en el principio de reconocimiento mutuo de sentencias y resoluciones judiciales ⁽⁹⁾;
- b) se basan en el Programa de Estocolmo ⁽¹⁰⁾, y
- c) prevén el intercambio de datos personales entre los Estados miembros (véanse los puntos 10 y 13 y la sección II.4).
- Por todo lo anterior, el SEPD considera apropiado examinar estas iniciativas de manera conjunta.
8. En este contexto, debe indicarse que también la Comisión Europea ha tratado recientemente la cuestión de la obtención de pruebas para presentarlas a las autoridades competentes en otros Estados miembros (objeto específico de la iniciativa OEP). De hecho, a finales de 2009 se publicó un *Libro Verde* ⁽¹¹⁾ —cuyo período de consulta ya ha sido cerrado ⁽¹²⁾— con el objetivo por parte de la Comisión [derivado del «Plan de acción por el que se aplica el Programa de Estocolmo» ⁽¹³⁾] de presentar en 2011 una propuesta legislativa para obtener un régimen general relativo a las pruebas en materia penal, basado en el principio de reconocimiento mutuo y que abarque todo tipo de pruebas ⁽¹⁴⁾.

⁽⁶⁾ DO C 69 de 18.3.2010, p. 5.

⁽⁷⁾ DO C 165 de 24.6.2010, p. 22.

⁽⁸⁾ Asimismo, el SEPD ha adoptado en el pasado dictámenes sobre iniciativas de los Estados miembros: véase por ejemplo el Dictamen del Supervisor Europeo de Protección de Datos sobre la iniciativa de 15 Estados miembros con vistas a la adopción de la Decisión del Consejo sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza (DO C 169 de 21.7.2007, p. 2) y el Dictamen del Supervisor Europeo de Protección de Datos, de 25 de abril de 2008, sobre la iniciativa de 14 Estados miembros con vistas a la adopción de una Decisión del Consejo por la que se refuerza Eurojust y se modifica la Decisión 2002/187/JAI (DO C 310 de 5.12.2008, p. 1).

⁽⁹⁾ Este principio, introducido en el Plan de Acción de Viena [Plan de acción del Consejo y de la Comisión sobre la mejor manera de aplicar las disposiciones del Tratado de Amsterdam relativas a la creación de un espacio de libertad, seguridad y justicia. Texto adoptado por el Consejo de Justicia y Asuntos de Interior de 3 de diciembre de 1998, DO C 19 de 23.1.1999, p. 1, punto 45, letra f)], ha sido formulado con toda claridad en las conclusiones del Consejo Europeo de Tampere de 15 y 16 de octubre de 1999, puntos 33 y 35 a 37.

⁽¹⁰⁾ Una tercera iniciativa (para una Directiva del Parlamento Europeo y del Consejo relativa al derecho a interpretación y a traducción en los procesos penales, 22 de enero de 2010, 2010/0801) tiene el mismo origen, pero no ha sido tenida en cuenta en el presente dictamen, ya que no trata cuestiones relacionadas con la protección de datos personales. Sobre el mismo tema, véase también la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa al derecho a interpretación y a traducción en los procesos penales, 9.3.2010, COM(2010) 82 final.

⁽¹¹⁾ Libro verde sobre la obtención de pruebas en materia penal en otro Estado miembro y sobre la garantía de su admisibilidad, COM(2009) 624 final, 11.11.2009.

⁽¹²⁾ Las distintas y, en ocasiones contradictorias, respuestas están siendo consideradas por la Comisión Europea y pueden consultarse en la página web: http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0004_en.htm

⁽¹³⁾ Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Garantizar el espacio de libertad, seguridad y justicia para los ciudadanos europeos. Plan de acción por el que se aplica el programa de Estocolmo, Bruselas, 20.4.2010, COM(2010) 171 final, p. 18.

⁽¹⁴⁾ No está claro, de momento, el modo en que un posible futuro instrumento se interrelacionará con la iniciativa EEL.

II. COOPERACIÓN JUDICIAL EN MATERIA PENAL Y TRATAMIENTO DE DATOS PERSONALES EN EL MARCO DE LAS INICIATIVAS OEP Y EEI

II.1. Contexto de las iniciativas

9. Las iniciativas arriba mencionadas se inscriben en la tendencia de las acciones de la UE y del ELSJ de los últimos años. Desde septiembre de 2001, ha habido un aumento significativo en la obtención y el intercambio de información en la Unión Europea (y con terceros países), gracias asimismo a los desarrollos de las TIC y a la ayuda de una serie de instrumentos legales europeos. Asimismo, las iniciativas OEP y EEI tienen como fin mejorar el intercambio de información en lo que respecta a las personas físicas en el ELSJ).

II.2. Iniciativa OEP

10. La iniciativa OEP —basada en el artículo 82, apartado 1, letra d), del TFUE— se centra en la protección de las víctimas de actos delictivos, en especial de las mujeres, y tiene como fin garantizarles una protección efectiva en toda la Unión. Para lograr este objetivo, la iniciativa OEP permite ampliar la protección de las medidas contempladas en su artículo 2, apartado 2, y que han sido adoptadas de conformidad con la legislación de un Estado miembro («el Estado de emisión») a otro Estado miembro al que se traslade la persona objeto de protección («el Estado de ejecución»), sin que la víctima tenga necesidad de incoar nuevos procedimientos o de presentar las pruebas nuevamente en el Estado de ejecución.

11. Las medidas de protección impuestas (a instancia de la víctima) sobre la persona causante del peligro tienen, por tanto, el fin de proteger la vida, la integridad física y psicológica, la libertad o la integridad sexual de la víctima en toda la Unión, con independencia de las fronteras nacionales, e intentan evitar nuevos delitos contra la misma víctima.

12. La OEP deberá ser emitida, a instancia de la víctima, en el «Estado (miembro) de emisión», por una autoridad judicial (o equivalente). El proceso se compone de los siguientes pasos:

- a) el «Estado de emisión» formula una solicitud de OEP;
- b) cuando se recibe la OEP, el «Estado de ejecución» adopta una resolución con arreglo a la legislación nacional para continuar protegiendo a la persona afectada.

13. Para lograr este objetivo, deberán adoptarse medidas administrativas. Dichas medidas abarcarán en parte el intercam-

bio de información personal entre los Estados miembros «de emisión» y «de ejecución» relativa a la persona en cuestión (la «víctima») y a la persona causante del peligro. El intercambio de datos personales está previsto en las siguientes disposiciones:

- a) en el artículo 6 se establece que la propia OEP contiene muchos elementos de información personal, especificados en las letras a), e), f), g) y h), y en el anexo I;
- b) las obligaciones de la autoridad competente del Estado de ejecución del artículo 8, apartado 1, requieren el tratamiento de datos personales, en particular, la obligación de notificar todo quebrantamiento de la medida de protección [artículo 8, apartado 1, letra d), y el anexo II];
- c) las obligaciones de la autoridad competente de los Estados miembros de ejecución y de emisión en caso de modificación, expiración o revocación de la orden de protección o de las medidas de protección (artículo 14).

14. La información mencionada en el apartado anterior se encuadra claramente dentro del ámbito de aplicación de los datos personales, definida en sentido amplio en la legislación de protección de datos como «toda información sobre una persona física identificada o identificable»⁽¹⁵⁾, y que el Grupo de Trabajo del Artículo 29 explica con más detalle. La iniciativa OEP trata de la información relacionada con una persona (la víctima o la persona causante del peligro) o sobre la información que se utiliza o que se puede utilizar para evaluar, tratar de determinada manera o influir en la situación de una persona (en particular, en relación con la persona causante del peligro)⁽¹⁶⁾.

II.3. Iniciativa OEP

15. La iniciativa OEP —basada en el artículo 82, apartado 1, letra a), del TFUE— requiere a los Estados miembros que obtengan, almacenen y transmitan pruebas, aún cuando no estén disponibles en la jurisdicción nacional. Por tanto, la iniciativa excede el principio de disponibilidad, el cual se presentó en el Programa de La Haya de 2004 como un

⁽¹⁵⁾ Véase el artículo 2, letra a), de la Decisión marco 2008/977/JAI del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, así como el artículo 2, letra a), de la Directiva 95/46/CE y el artículo 2, letra a), del Reglamento (CE) n° 45/2001.

⁽¹⁶⁾ Véase el Grupo de Trabajo del Artículo 29, Dictamen 4/2007 sobre el concepto de datos personales, WP 136, adoptado el 20 de junio de 2007, p. 10.

enfoque innovador del intercambio transfronterizo de información policial⁽¹⁷⁾. Excede asimismo lo establecido en la Decisión marco 2008/978/JAI del Consejo, de 18 de diciembre de 2008, relativa al exhorto europeo de obtención de pruebas, que resulta únicamente de aplicación a las pruebas (proporcionadas) que ya existan⁽¹⁸⁾.

16. Un EEI se expedirá a efectos de obtener una o varias medidas de investigación específicas que se llevarán a cabo en el Estado de ejecución, con vistas a la obtención de pruebas (potencialmente no existentes al emitir la orden) y a su traslado (artículo 12). Se aplica a casi todas las medidas de investigación (véanse los considerandos 6 y 7 de la iniciativa).
17. El objetivo de la iniciativa EEI es crear un único instrumento eficaz y flexible para obtener pruebas localizadas en otro Estado miembro en el marco de los procedimientos penales, en lugar de los actuales instrumentos legales utilizados por las autoridades judiciales (basados, por un lado, en la asistencia judicial, y por otro, en el reconocimiento mutuo)⁽¹⁹⁾.
18. Evidentemente, las pruebas obtenidas mediante un EEI (véase asimismo el anexo A de la iniciativa) pueden contener datos personales, como en el caso de la información sobre cuentas bancarias (artículo 23), la información sobre transacciones bancarias (artículo 24) y el control de las transacciones bancarias (artículo 25) o puede cubrir la comunicación de datos personales (como en el caso de las videoconferencias o las conferencias por teléfono, establecidas en los artículos 21 y 22).
19. Por ello, la iniciativa EEI tiene un impacto significativo sobre el derecho de protección de los datos personales. Asimismo, considerando que todavía no ha expirado la fecha de la aplicación de la Decisión marco 2008/978/JAI (y que, por tanto, resulta difícil valorar la eficacia del ins-

⁽¹⁷⁾ El principio se consagró en el Programa de La Haya. Consolidación de la libertad, la seguridad y la justicia en la Unión Europea, punto 2.1, y significa «que, en todo el territorio de la Unión, un funcionario de policía de un Estado miembro que necesite información para llevar a cabo sus obligaciones pueda obtenerla de otro Estado miembro y el que organismo policial del otro Estado miembro que posea dicha información la facilitará para el propósito indicado, teniendo en cuenta el requisito de las investigaciones en curso en dicho Estado». En relación con este tema, véase el 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], DO C 116 de 17.5.2006, p. 8.

⁽¹⁸⁾ Decisión marco 2008/978/JAI del Consejo, de 18 de diciembre de 2008, relativa al exhorto europeo de obtención de pruebas para recabar objetos, documentos y datos destinados a procedimientos en materia penal, DO L 350 de 30.12.2008, p. 72.

⁽¹⁹⁾ Actualmente existen dos instrumentos de reconocimiento mutuo aplicables a la obtención de pruebas: Decisión marco 2003/577/JAI del Consejo, de 22 de julio de 2003, relativa a la ejecución en la Unión Europea de las resoluciones de embargo preventivo de bienes y de aseguramiento de pruebas (DO L 196 de 2.8.2003, p. 45) y la Decisión marco 2008/978/JAI, citada en la nota a pie de página 18.

trumento y la necesidad de medidas legales adicionales)⁽²⁰⁾, el SEPD recuerda la necesidad de verificar periódicamente, a la luz de los principios de protección de datos, la eficacia y la proporcionalidad de las medidas legales adoptadas en el ELSJ⁽²¹⁾. Por tanto, el SEPD recomienda añadir una cláusula de evaluación a la iniciativa OEP, que exija a los Estados miembros que emitan periódicamente informes en relación con la aplicación del instrumento y que la Comisión sintetice dichos informes y, cuando resulte apropiado, emita las pertinentes propuestas de modificación.

II.4. Tratamiento de los datos personales previsto en las iniciativas OEP y EEI

20. Tal como se ha indicado en los puntos 13, 14 y 18, resulta claro que, de conformidad con las Directivas propuestas, las autoridades competentes de los diversos Estados miembros tratarán e intercambiarán datos personales. Teniendo en cuenta estas circunstancias, la información queda protegida por el derecho fundamental de protección de datos, reconocido en el artículo 16 del TFUE y el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea.
21. A pesar de lo anterior, en la «Declaración detallada» aneja a la iniciativa OEP el «Riesgo de menoscabo de derechos fundamentales» se ha identificado con un «0» (cero)⁽²²⁾, y en el análisis del impacto incluido en la «Declaración detallada» aneja a la iniciativa OEP las cuestiones de protección de datos no se han tenido en cuenta⁽²³⁾.
22. El SEPD lamenta estas conclusiones y pone énfasis en la importancia de proteger los datos en el contexto particular en que se tratan los datos personales, a saber:
 - a) en el amplio ámbito de la cooperación judicial en materia penal;
 - b) los datos suelen tener un carácter especialmente protegido y son obtenidos por las autoridades policiales y judiciales como resultado de una investigación;
 - c) el posible contenido de los datos, en particular en relación con la iniciativa EEI, lo cual se extiende a cualquier tipo de prueba, y

⁽²⁰⁾ El artículo 23, apartado 1, de la Decisión marco 2008/978/JAI establece que «los Estados miembros tomarán las medidas necesarias para dar cumplimiento a lo dispuesto en la presente Decisión marco antes del 19 de enero de 2011».

⁽²¹⁾ Asimismo, el apartado 1.2.3 del Programa de Estocolmo pide que las nuevas iniciativas legislativas sólo deberían presentarse tras la comprobación del respeto del principio de proporcionalidad.

⁽²²⁾ La Declaración detallada que permite evaluar el cumplimiento de los principios de subsidiariedad y de proporcionalidad, de conformidad con el artículo 5 del Protocolo (nº 2) del Tratado de Lisboa de 6 de enero de 2010.

⁽²³⁾ La Declaración detallada de 23 de junio de 2010, Expediente interinstitucional: 2010/0817 (COD) únicamente hace referencia de manera explícita al derecho de libertad y seguridad y al derecho de buena administración (véanse las pp. 25 y 41).

- d) la posible comunicación de pruebas fuera de la Unión Europea, de conformidad con el artículo 13 de la Decisión marco 2008/977/JAI relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal ⁽²⁴⁾.
23. Este contexto proporciona a las operaciones de tratamiento de datos un particular impacto y podrá afectar de manera significativa a los derechos fundamentales en materia de datos, incluido el derecho de la protección de datos personales.
24. Debido a las anteriores consideraciones, el SEPD se pregunta el motivo por el que las iniciativas no tratan la protección de los datos personales (aparte de referirse, en el artículo 18 de la iniciativa EEI, a las obligaciones de confidencialidad impuestas a los actores implicados en una investigación) ni hacen referencia de manera explícita a la Decisión marco 2008/977/JAI. De hecho, la Decisión marco sería aplicable a las operaciones de tratamiento previstas por ambas iniciativas [véase el artículo 1, apartado 2, letra a)].
25. Por este motivo, el SEPD considera una buena noticia el que durante los trabajos preparatorios en el Consejo relativos a la iniciativa OEP, se haya introducido ⁽²⁵⁾ una referencia a la Decisión marco 2008/977/JAI y confía que el Parlamento Europeo confirme este cambio en las iniciativas originales ⁽²⁶⁾.
26. El SEPD lamenta de que todavía no se haya introducido un considerando similar en la iniciativa EEI, la cual implica un intercambio de datos personales mucho más amplio. El SEPD recibe con agrado que, en este contexto, la Comisión Europea, al comentar la iniciativa EEI, sugiera que debe introducirse una referencia (ya sea en un considerando o en la parte dispositiva) a la aplicabilidad de la Decisión marco 2008/977/JAI ⁽²⁷⁾.

⁽²⁴⁾ Para más información: Decisión marco 2008/977/JAI.

⁽²⁵⁾ Véase el considerando 27 de la última versión de la iniciativa OEP (28 de mayo de 2010, doc. n.º 10384/2010 del Consejo): «Los datos de carácter personal tratados en el contexto de la aplicación de la presente Decisión marco deben estar protegidos conforme a la Decisión marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal y con arreglo a los principios del Convenio del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, ratificado por todos los Estados miembros».

⁽²⁶⁾ En este sentido, véase la Enmienda 21 incluida en el Proyecto de informe sobre la iniciativa con vistas a la adopción de la Directiva del Parlamento y del Consejo sobre la orden europea de protección [00002/2010 — C7-0006/2010 — 2010/0802(COD)], 20.5.2010, Comisión de Libertades Civiles, Justicia y Asuntos de Interior — Comisión de Derechos de la Mujer e Igualdad de Género, Ponente: Teresa Jiménez-Becerril Barrio, Carmen Romero López, en http://www.europarl.europa.eu/meetdocs/2009_2014/documents/femm/pr/817/817530/817530es.pdf

⁽²⁷⁾ Véanse las observaciones de la Comisión sobre el exhorto europeo de investigación en materia penal, 24.8.2010, JUST/B/1/AA-et D(2010) 6815, p. 9 y 38, en http://ec.europa.eu/justice/news/intro/doc/comment_2010_08_24_en.pdf

27. Por tanto, sin perjuicio de lo dispuesto en la sección III, ambas iniciativas deberían incluir una disposición específica que aclare que la Decisión marco 2008/977/JAI resulta de aplicación a los tratamientos de datos previstos por dichas iniciativas.

III. NORMAS ESPECÍFICAS NECESARIAS ADEMÁS DEL MARCO JURÍDICO DE PROTECCIÓN EXISTENTE PARA LA COOPERACIÓN JUDICIAL EN MATERIA PENAL

28. Una vez más, las dos iniciativas plantean la cuestión esencial de una aplicación incompleta e incoherente de los principios de protección de datos personales en el ámbito de la cooperación judicial en materia penal ⁽²⁸⁾.
29. El SEPD es consciente de la importancia de mejorar la eficacia de la cooperación judicial entre los Estados miembros, también en los ámbitos cubiertos por las iniciativas OEP y EEI ⁽²⁹⁾. Por otra parte, reconoce las ventajas y la necesidad de intercambiar información, pero desea subrayar que el tratamiento de datos debe respetar —entre otras ⁽³⁰⁾— las normas de la Unión Europea en materia de protección de datos. Esto resulta aún más evidente en vistas de que el Tratado de Lisboa introduce el artículo 16 del TFUE y dota de carácter vinculante al artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea.
30. Las situaciones que impliquen un intercambio transfronterizo de información en el territorio de la Unión merecen una especial atención, ya que el tratamiento de datos personales en más de una jurisdicción aumenta los riesgos contra los derechos y los intereses de las personas físicas implicadas. En esos casos, los datos personales se procesan en múltiples jurisdicciones que poseen distintas exigencias legales y en las que el marco técnico no es necesariamente idéntico.
31. Por otra parte, esta situación conduce a una inseguridad jurídica para los titulares de los datos, ya que pueden verse implicadas partes de otros Estados miembros, resultar aplicables las legislaciones nacionales de varios Estados miembros y pueden ser distintas de las leyes a las que están habituados o puede resultar aplicable un sistema jurídico al que no están habituados. Esto exige que se lleven a cabo mayores esfuerzos para garantizar que se cumplen los requisitos que emanan de la legislación de la Unión Europea en materia de protección de datos ⁽³¹⁾.

⁽²⁸⁾ Véase asimismo la sección V del dictamen.

⁽²⁹⁾ Véase, entre otros, su coincidencia en la necesidad de mejorar el acceso a la justicia, la cooperación entre las autoridades judiciales europeas y la eficacia del propio sistema de justicia en el Dictamen del Supervisor Europeo de Protección de Datos relativo a la estrategia en materia de e-Justicia (Justicia en línea), DO C 128 de 6.6.2009, p. 13, puntos 9 y 21.

⁽³⁰⁾ En relación con el aspecto referente al respeto de las normas de procedimiento penal en los Estados miembros, especialmente en el ámbito de la propuesta EEI, puede hacerse referencia a las consideraciones y problemas incluidos en las respuestas enviadas a la Comisión Europea durante la consulta pública relativa al Libro Verde (véanse las notas a pie de página 11 y 12).

⁽³¹⁾ Véase también el documento del Consejo, Programa de La Haya: Consolidación de la libertad, la seguridad y la justicia en la Unión Europea (2005/C 53/01), DO C 53 de 3.3.2005, p. 1, 7 y ss.

32. En opinión del SEPD, la aclaración de la aplicabilidad de la Decisión marco 2008/977/JAI, tal como se contempla en el punto 27, no es más que un primer paso.
33. Los desafíos específicos para una tutela efectiva en el ámbito de la cooperación judicial en materia penal, junto con la Decisión marco 2008/977/JAI (véanse los puntos 52-56) que no resulta del todo satisfactoria, pueden requerir que se adopten disposiciones específicas en materia de protección de datos, cuando los actos jurídicos específicos de la Unión Europea impliquen el intercambio de datos personales.

IV. DESAFÍOS PARA UNA PROTECCIÓN DE DATOS EFECTIVA EN LA COOPERACIÓN PENAL: RECOMENDACIONES ACERCA DE LAS INICIATIVAS OEP Y EEI

IV.1. Consideraciones previas

34. La tutela efectiva de los datos personales (tal como se ha resaltado en el punto 29) no sólo es importante para los interesados sino que también contribuye a que la propia cooperación judicial tenga éxito. De hecho, la voluntad de intercambio de estos datos con autoridades de otros Estados miembros se ve incrementada si se garantiza un nivel de protección, exactitud y fiabilidad de los datos personales en el otro Estado miembro⁽³²⁾. En resumen, el establecimiento de un (elevado) nivel común en este delicado ámbito promovería la confianza mutua entre los Estados miembros y reforzaría la cooperación judicial basada en el reconocimiento mutuo, mejorando así la calidad de los datos sometidos a un intercambio de información.
35. En este concreto contexto, el SEPD recomienda incluir en las iniciativas OEP y EEI garantías específicas para la protección de datos, además de una referencia general a la Decisión marco 2008/977/JAI (tal como se ha propuesto en el punto 27).
36. Algunas de estas garantías son más de carácter general y están destinadas a ser incluidas en ambas iniciativas, en especial las garantías que tienen como fin mejorar la exactitud de los datos, así como la seguridad y la confidencialidad. En cambio, otras garantías se refieren a disposiciones específicas de la iniciativa OEP o de la iniciativa EEI.

IV.2. Garantías de carácter más general

Exactitud

37. En las situaciones previstas en las iniciativas en que los Estados miembros intercambian datos debe ponerse espe-

⁽³²⁾ Véase el Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Decisión marco del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal [COM(2005) 475 final], DO C 47 de 25.2.2006, p. 27, puntos 5 a 7.

cial énfasis en garantizar que la información sea exacta. A este respecto, el SEPD recibe con satisfacción que la iniciativa OEP incluya en su artículo 14 una obligación clara de la autoridad competente del Estado de emisión de informar a la autoridad competente del Estado de ejecución de toda modificación, expiración o revocación de la orden de protección.

38. Asimismo, el SEPD también destaca que la necesidad de traducción podría afectar a la exactitud de la información, en especial dado que las iniciativas hacen referencia a instrumentos jurídicos específicos que podrían tener un significado distinto en diversas lenguas y en los distintos sistemas jurídicos. En este contexto, el SEPD además de recibir con agrado el hecho de que la iniciativa OEP trate la cuestión de las traducciones (artículo 16), sugiere asimismo que se incluya una disposición similar en la iniciativa EEI.

Seguridad, conocimiento y responsabilidad

39. El aumento de la cooperación transfronteriza que podría resultar de la adopción de estas dos iniciativas exige una atenta consideración de los aspectos de seguridad de la transmisión transfronteriza de los datos personales relacionados con la aplicación de los órdenes europeos de protección y de los exhortos europeos de investigación⁽³³⁾. Esto es necesario, no sólo para cumplir los niveles de seguridad del tratamiento de los datos personales establecidos en el artículo 22 de la Decisión marco 2008/977/JAI, sino también para garantizar el secreto de las investigaciones y la confidencialidad de los procedimientos penales, regulada en el artículo 18 de la iniciativa EEI y, como norma general, para los datos personales derivados del intercambio transfronterizo, en virtud del artículo 21 de la Decisión marco 2008/977/JAI.
40. El SEPD pone énfasis en la necesidad de contar con sistemas de telecomunicaciones seguros en los procedimientos de transmisión. Por tanto, recibe con satisfacción la disposición para el uso de la Red Judicial Europea⁽³⁴⁾ como medio para garantizar que la OEP y el EEI se envíen correctamente a las autoridades nacionales competentes, minimizando o reduciendo el riesgo de que resulten implicadas autoridades inadecuadas en el intercambio de datos personales (véase el artículo 7, apartados 2 y 3, de la iniciativa OEP y el artículo 6, apartados 3 y 4, de la iniciativa EEI).

41. Por ello, las iniciativas deberían incluir disposiciones que exijan a los Estados miembros que garanticen que:

⁽³³⁾ En términos generales, véase la Comunicación de la Comisión al Consejo, al Parlamento Europeo y al Comité Económico y Social, Hacia una estrategia europea en materia de e-Justicia (Justicia en línea), Bruselas, 30.5.2008, COM(2008) 329 final, p. 8: «Las autoridades judiciales deben poder intercambiar con toda confianza datos confidenciales».

⁽³⁴⁾ Decisión 2008/976/JAI del Consejo, de 16 de diciembre de 2008, sobre la Red Judicial Europea (DO L 348 de 24.12.2008, p. 130).

- a) las autoridades competentes disponen de los recursos adecuados para aplicar las directivas propuestas;
- b) los agentes competentes observan normas profesionales y están sujetos a los correspondientes procedimientos internos que aseguren, en particular, la protección de las personas en relación con el tratamiento de datos personales, y la observancia adecuada de las disposiciones de confidencialidad y de secreto profesional (como se establece en el artículo 18 de la iniciativa EEI).
42. Asimismo, el SEPD recomienda la introducción de disposiciones que garanticen que se observan los principios sustantivos de protección de datos al procesar datos personales y que se dispone de los mecanismos internos necesarios para demostrar su cumplimiento a las partes interesadas externas. Dichas disposiciones serían instrumentos para responsabilizar a las personas que se encargan de controlar los datos [de conformidad con el «principio de responsabilización» que se discute en el contexto de la actual revisión del marco de protección de datos ⁽³⁵⁾]. Esto les exige que adopten las medidas necesarias para garantizar el cumplimiento. Dichas disposiciones deberán incluir:
- a) sistemas de autenticación que permitan sólo a las personas autorizadas el acceso a ambas bases de datos que contienen datos personales o a las instalaciones en que se guardan las pruebas;
- b) el seguimiento de los accesos a los datos personales y a las operaciones realizadas en los mismos;
- c) la aplicación de un control de auditoría.

IV.3. Garantías en la iniciativa EEI

43. Teniendo en cuenta las características especialmente intrusivas de determinadas medidas de investigación, el SEPD invita a que se haga una reflexión general sobre la admisibilidad de las pruebas obtenidas para fines distintos de los de la prevención, la investigación, la detección o el enjuiciamiento de delitos, o para la aplicación de sanciones penales y el ejercicio del derecho de defensa. En particular, debe considerarse detenidamente el uso de las pruebas obtenidas en virtud del artículo 11, apartado 1, letra d), de la Decisión marco 2008/977/JAI ⁽³⁶⁾.

⁽³⁵⁾ Véase Grupo de Trabajo de Protección de Datos del Artículo 29 y del Grupo de Trabajo sobre Policía y Justicia, El futuro de la protección de la vida privada, p. 20 y ss.

⁽³⁶⁾ Esta disposición permite utilizar las pruebas también para «cualquier otro fin, solo con el previo consentimiento del Estado miembro transmisor o con el consentimiento del interesado, otorgados de acuerdo con el Derecho nacional».

44. Por tanto, debe incluirse en la iniciativa EEI una excepción a lo dispuesto en el artículo 11, apartado 1, letra d), que indique que las pruebas obtenidas mediante un EEI no podrán ser utilizadas para fines distintos de los de la prevención, la investigación, la detección o el enjuiciamiento de delitos, o la aplicación de sanciones penales y el ejercicio del derecho de defensa.

IV.4. Garantías en la iniciativa OEP

45. En lo que respecta a la iniciativa OEP, el SEPD reconoce que los datos personales intercambiados entre las autoridades competentes y que se contemplan en el anexo I de la iniciativa (relativos tanto a la víctima como a la persona causante del peligro) son adecuados, relevantes y no excesivos en relación con los fines para los que han sido obtenidos y posteriormente tratados.
46. Sin embargo, lo que no queda suficientemente claro en la iniciativa —especialmente en el artículo 8, apartado 1, letra b)— es cuáles son los datos personales relacionados con la víctima que la autoridad competente del Estado de ejecución comunicará a la persona causante del peligro.
47. El SEPD estima que es adecuado tener en cuenta las circunstancias y el contenido de las medidas de protección dictadas por el Estado miembro de emisión antes de informar a la persona causante del peligro. Por tanto, esta última deberá conocer únicamente aquellos datos personales de la víctima (que, en algunos casos, podrá incluir datos de contacto) que sean estrictamente relevantes para la plena ejecución de la medida de protección.
48. El SEPD es consciente de que facilitar información de contacto (por ejemplo, números de teléfono, la dirección de la víctima así como otros lugares que frecuente, como el lugar de trabajo o la escuela de sus hijos) puede, de hecho, poner en peligro el bienestar físico y psicológico de la víctima, así como afectar a su derecho a la intimidad y a la protección de los datos personales. Por otro lado, en algunos casos es necesario indicar las direcciones pertinentes para advertir a la persona causante del peligro de los lugares a los que tiene prohibido ir, y facilitar de este modo que cumpla con la orden y evitar las eventuales sanciones por un posible incumplimiento. Asimismo, dependiendo de las circunstancias, puede ser necesaria la identificación del lugar al que la persona causante del peligro tiene prohibido ir, con el fin de no limitar de manera innecesaria su libre circulación.
49. Teniendo en cuenta estas consideraciones, el SEPD destaca la importancia de esta cuestión y recomienda que la iniciativa OEP establezca claramente que, en función de las circunstancias del caso, la persona causante del peligro pueda únicamente conocer aquellos datos personales de la víctima

(que en algunos casos pueden incluir los datos de contacto) que sean estrictamente necesarios para la plena ejecución de la medida de protección ⁽³⁷⁾.

50. Por último, el SEPD pide que se aclare la expresión «medios electrónicos» incluida en el considerando 10 de la iniciativa OEP. En particular, debe explicarse si los datos personales se tratan usando «medios electrónicos» y, en ese caso, las garantías que se proporcionan.

V. NORMAS DE PROTECCIÓN DE DATOS Y COOPERACIÓN JUDICIAL EN MATERIA PENAL: PROBLEMAS RELACIONADOS CON LAS INICIATIVAS OEP Y EEI

51. La Decisión marco 2008/977/JAI se aplicará a todos los intercambios de datos personales en virtud de las iniciativas OEP y EEI.
52. El SEPD, aunque reconoce que la Decisión marco 2008/977/JAI (cuando son los Estados miembros quienes la aplican) constituye un importante paso adelante para la protección de datos en la cooperación policial y judicial ⁽³⁸⁾, opina que la propia Decisión marco no es del todo satisfactoria ⁽³⁹⁾. La principal cuestión sin resolver está relacionada con su restringido ámbito de aplicación. La Decisión marco se limita a los intercambios de datos personales en el ámbito policial y judicial entre las autoridades y los sistemas de los distintos Estados miembros y a nivel de la Unión ⁽⁴⁰⁾.
53. Aunque esta cuestión no puede solucionarse en el contexto de las iniciativas OEP y EEI, el SEPD insiste en resaltar que la falta de un (elevado) nivel común de protección de datos en la cooperación judicial podría implicar que cuando una autoridad judicial a nivel nacional o de la Unión se ocupe de un expediente penal que incluya información que tiene origen en otros Estados miembros (incluida, por ejemplo,

las pruebas obtenidas sobre la base de un EEI) deba aplicar distintas normas de tratamiento de datos: régimen autónomo nacional (que deberá cumplir con el Convenio del Consejo de Europa n° 108) para datos procedentes del propio Estado miembro y las normas de desarrollo de la Decisión marco 2008/977/JAI para los datos procedentes de otros Estados miembros. Por ello, distintos «elementos de información» pueden estar incluidos en sistemas jurídicos diferentes.

54. Las consecuencias de la aplicación de este «doble» nivel de protección de datos a cada expediente penal con elementos transfronterizos son importantes en la práctica diaria (por ejemplo, conservación de la información establecida por las leyes aplicables a cada organismo transmisor; en caso de solicitud de un tercer país, cada organismo transmisor dará su consentimiento de acuerdo con su propia evaluación de la adecuación o de los compromisos internacionales; y las diferencias de las normativas sobre el derecho de acceso de los interesados). Además, la protección de los ciudadanos y sus derechos podrían variar enormemente y estarían sujetos a diversas excepciones generales dependiendo del Estado miembro en que tenga lugar el tratamiento ⁽⁴¹⁾.
55. Por tanto, el SEPD desea aprovechar esta ocasión para reiterar su opinión en relación con la necesidad de un marco jurídico de protección de datos general que cubra todos los ámbitos de competencia de la Unión Europea, incluidos el ámbito policial y judicial, que se aplique tanto a los datos personales transmitidos o puestos a disposición por las autoridades competentes de otros Estados miembros como al tratamiento nacional en el ELSJ ⁽⁴²⁾.
56. Por último, el SEPD observa que las normas de protección de datos deberían aplicarse a todos los sectores y al uso de los datos para todos los fines ⁽⁴³⁾. Por supuesto, son posibles las excepciones debidamente justificadas y redactadas con claridad, en especial respecto de los datos personales tratados a efectos represivos ⁽⁴⁴⁾. Las diferencias en el nivel de protección de los datos personales son contrarias al

⁽³⁷⁾ Este parece ser el sentido de las Enmiendas 13 y 55 del Proyecto de informe sobre la iniciativa con vistas a la adopción de la Directiva del Parlamento y del Consejo sobre la orden europea de protección [00002/2010 — C7-0006/2010 — 2010/0802 (COD)], 20.5.2010, Comisión de Libertades Civiles, Justicia y Asuntos de Interior — Comisión de Derechos de la Mujer e Igualdad de Género.

⁽³⁸⁾ Véase el Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión al Consejo, al Parlamento Europeo y al Comité Económico y Social, Hacia una estrategia europea en materia de e-Justicia (Justicia en línea) (2009/C 128/02), DO C 128 de 6.6.2009, p. 13, punto 17.

⁽³⁹⁾ Véanse los tres Dictámenes del Supervisor Europeo de Protección de Datos sobre la propuesta de Decisión marco relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, [COM (2005) 475 final]], DO C 47 de 25.2.2006, p. 27, DO C 91 de 26.4.2007, p. 9, DO C 139 de 23.6.2007, p. 1. Véase también el Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo relativa a un espacio de libertad, seguridad y justicia al servicio de los ciudadanos, DO C 276 de 17.11.2009, p. 8, puntos 19, 29 y 30.

⁽⁴⁰⁾ Véase el artículo 2 de la Decisión marco 2008/977/JAI.

⁽⁴¹⁾ Véase el Tercer Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Decisión marco del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, DO C 139 de 23.6.2007, p. 41, mencionado en la nota a pie de página n° 39, punto 46.

⁽⁴²⁾ La posición del SEPD ha sido claramente apoyada por el Grupo de Trabajo de Protección de Datos del Artículo 29 y el Grupo de Trabajo sobre Policía y Justicia, El futuro de la protección de la vida privada: contribución conjunta a la consulta de la Comisión Europea sobre el marco jurídico del derecho fundamental a la protección de los datos personales, WP 168, adoptado el 1 de diciembre de 2009, p. 4, 7 y ss. y 24 y ss.

⁽⁴³⁾ Véase la Comunicación de la Comisión al Parlamento Europeo y del Consejo, Un espacio de libertad, seguridad y justicia al servicio de los ciudadanos, Bruselas, 10.6.2009, COM(2009) 262 final, p. 30: «La Unión debe dotarse de un régimen único de protección de los datos personales que cubra el conjunto de las competencias de la Unión».

⁽⁴⁴⁾ Dicho enfoque también cumpliría con el objetivo de la Declaración 21 aneja al Tratado de Lisboa relativa a la protección de datos de carácter personal en el ámbito de la cooperación judicial en materia penal y de la cooperación policial.

actual marco jurídico (renovado) de la Unión Europea. El artículo 3, apartado 2, de la Directiva 95/46/CE —con excepción del ámbito de aplicación de la Directiva en el ámbito policial y judicial— no es conforme con la filosofía que dimana del artículo 16 del TFUE. Asimismo, estas diferencias tampoco están lo suficientemente cubiertas por el Convenio n.º 108 del Consejo de Europa ⁽⁴⁵⁾, que obliga a todos los Estados miembros.

VI. CONCLUSIONES Y RECOMENDACIONES

57. El SEPD recomienda en relación tanto con la iniciativa OEP como con la iniciativa EEI:

- incluir disposiciones específicas que establezcan que los instrumentos se aplican sin perjuicio de lo dispuesto en la Decisión marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal,
- incluir disposiciones que exijan a los Estados miembros que garanticen que:
 - las autoridades competentes disponen de los recursos necesarios para aplicar las directivas propuestas,
 - los agentes competentes observan normas profesionales y están sujetos a los correspondientes procedimientos internos que aseguren, en particular, la protección de las personas en relación con el tratamiento de datos personales, y la observancia adecuada de las disposiciones de confidencialidad y secreto profesional,
 - los sistemas de autenticación sólo permiten a las personas autorizadas el acceso a ambas bases de datos que contienen datos personales o a las instalaciones en que se guardan las pruebas,
 - el seguimiento de los accesos y de las operaciones efectuadas,
 - se implantan controles de auditoría.

58. En relación con la iniciativa OEP, el SEPD recomienda:

- que establezca claramente que, en función de las circunstancias del caso, la persona causante del peligro

pueda únicamente conocer aquellos datos personales de la víctima (que en algunos casos pueden incluir los datos de contacto) que sean estrictamente necesarios para la plena ejecución de la medida de protección,

- que aclare la expresión «medios electrónicos» incluida en el considerando 10 de la iniciativa OEP.

59. En relación con la iniciativa EEI, el SEPD recomienda:

- que incluya una disposición sobre las traducciones, similar al artículo 16 de la iniciativa EEI,
- que incluya una disposición que evite el uso de pruebas para fines distintos de los de la prevención, la investigación, la detección o el enjuiciamiento de delitos o la aplicación de sanciones penales, así como para el ejercicio del derecho de defensa, como excepción del artículo 11, apartado 1, letra d), de la Decisión marco 2008/977/JAI,
- que añada una cláusula de evaluación a la iniciativa EEI, que exija a los Estados miembros que emitan periódicamente informes en relación con la aplicación del instrumento y que la Comisión sintetice dichos informes y, cuando resulte apropiado, emita las pertinentes propuestas de modificación.

60. Por otro lado, de manera más general, el SEPD:

- recomienda al Consejo que establezca un procedimiento en el que deba consultarse al SEPD, en los casos en que una iniciativa presentada por los Estados miembros esté relacionada con el tratamiento de datos personales,
- reitera la necesidad de la existencia de un marco jurídico de protección de datos general que cubra todos los ámbitos de competencia de la Unión Europea, incluidos el ámbito policial y judicial, que se aplique tanto a los datos personales transmitidos o puestos a disposición por las autoridades competentes de otros Estados miembros como al tratamiento nacional en el ELSJ.

Hecho en Bruselas, el 5 de octubre de 2010.

Peter HUSTINX

Supervisor Europeo de Protección de Datos

⁽⁴⁵⁾ Convenio n.º 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencias de datos, de 28 de enero de 1981.