

I

(Resoluciones, recomendaciones y dictámenes)

DICTÁMENES

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta modificada de Reglamento del Parlamento Europeo y del Consejo relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento (CE) n° [...] (por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida) y sobre la propuesta de Decisión del Consejo relativa a las solicitudes de comparación con datos Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de la aplicación de la ley

(2010/C 92/01)

EL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS,

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

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

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

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

Vista la solicitud de dictamen, hecha de conformidad con el artículo 28, apartado 2, del Reglamento (CE) n° 45/2001, y recibida el 15 de septiembre de 2009 de la Comisión Europea.

HA ADOPTADO EL SIGUIENTE DICTAMEN:

I. INTRODUCCIÓN

1. El 10 de septiembre de 2009 la Comisión adoptó dos propuestas, a saber, la propuesta modificada de Reglamento del Parlamento Europeo y del Consejo relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento (CE) n° [...] (por el que se establecen los criterios y

mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida) ⁽³⁾ y la propuesta de Decisión del Consejo relativa a las solicitudes de comparación con datos Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de la aplicación de la ley ⁽⁴⁾. La Comisión remitió ambas propuestas al Supervisor Europeo de Protección de Datos (SEPD) consultándole al respecto, de conformidad con el artículo 28, apartado 2, del Reglamento (CE) n° 45/2001. El SEPD recibió las propuestas el 15 de septiembre de 2009 (en lo sucesivo, las propuestas en cuestión se denominarán «las propuestas» o «el Reglamento propuesto» y «la Decisión propuesta»). El SEPD recibió también la correspondiente evaluación de impacto.

2. El SEPD muestra su satisfacción por el hecho de que se le haya consultado y recomienda que se haga referencia a esta consulta en los considerandos de la propuesta, al igual que se hizo en otros textos legislativos sobre los que se ha consultado al SEPD de conformidad con el Reglamento (CE) n° 45/2001.

3. El SEPD muestra un interés particular por estas propuestas también en vista de las competencias de supervisión que ejerce respecto de la Unidad Central de la base de datos Eurodac y de la supervisión coordinada que debe ejercer respecto del sistema Eurodac en su conjunto con las autoridades nacionales responsables de la protección de datos.

⁽¹⁾ DO L 281 de 23.11.1995, p. 31.

⁽²⁾ DO L 8, de 12.1.2001, p. 1.

⁽³⁾ COM(2009) 342 final.

⁽⁴⁾ COM(2009) 344 final.

4. El SEPD ya ha tratado la cuestión de facilitar el acceso a sistemas informáticos a gran escala con fines de aplicación de la ley en el contexto del acceso al Sistema de Información de Visados por parte de las fuerzas de seguridad y Europol⁽⁵⁾. El objeto de las propuestas está también estrechamente relacionado con la refundición de los Reglamentos «Eurodac» y «Dublín», sobre los cuales el SEPD emitió dos dictámenes el 18 de febrero de 2009⁽⁶⁾.

II. CONTENIDO Y ANTECEDENTES DE LAS PROPUESTAS

5. Las propuestas fundamentan el derecho de las autoridades designadas por los Estados miembros y Europol a pedir una comparación de las impresiones dactilares o de una copia latente con los datos Eurodac. Una comparación positiva que origine una respuesta positiva de Eurodac irá acompañada de todos los datos que figuren en Eurodac sobre la impresión dactilar. Las solicitudes de información adicional a raíz de una respuesta positiva no están reguladas en las propuestas, pero están cubiertas por los instrumentos existentes relativos al intercambio de información en el ámbito de la aplicación de la ley. El ámbito de aplicación de las propuestas cubre la lucha contra los delitos de terrorismo y otros delitos graves, como el tráfico de seres humanos y de drogas⁽⁷⁾.

6. El artículo 7 de la Decisión propuesta fija las condiciones de acceso a Eurodac por parte de las autoridades designadas. Sólo se permitirá el acceso cuando se hayan obtenido resultados negativos de las comparaciones con las bases de datos dactiloscópicas nacionales y las bases de datos automatizadas dactiloscópicas en virtud de la Decisión 2008/615/JAI del Consejo sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza⁽⁸⁾ y cuando la comparación sea necesaria para luchar contra los delitos de terrorismo u otros delitos graves o en un caso concreto y existan motivos fundados para considerar que dicha comparación contribuirá sustancialmente a la lucha contra cualquiera de los delitos en cuestión. El SEPD observa que el artículo 7 no exige que el titular de los datos cuyas impresiones dactilares sean objeto de la solicitud sea sospechoso de cualquiera de los delitos antes mencionados.

⁽⁵⁾ Dictamen de 20 de enero de 2006 sobre la propuesta de Decisión del Consejo sobre el acceso para consultar el Sistema de Información de Visados (VIS) por las autoridades de los Estados miembros responsables de la seguridad interior y por Europol, con fines de prevención, detección e investigación de los delitos de terrorismo y otros delitos graves [COM(2005) 600 final], DO C 97 de 25.4.2006, p. 6.

⁽⁶⁾ Dictamen de 18 de febrero de 2009 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento (CE) n° [...] (por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida) [COM(2008) 825] y dictamen de 18 de febrero de 2009 propuesta relativo a la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida [COM(2008) 820 final].

⁽⁷⁾ Véase, en particular, el artículo 1 de la Decisión propuesta.

⁽⁸⁾ DO L 210 de 6.8.2008, p. 1; en lo sucesivo: Decisión «Prüm».

7. Debe recordarse que el objetivo de la creación del sistema Eurodac era facilitar la aplicación del Reglamento «Dublín», que permite determinar al Estado miembro responsable del examen de una solicitud de asilo mediante una comparación de las impresiones dactilares de los solicitantes de asilo y de los inmigrantes ilegales. El sistema Eurodac permite a los Estados miembros identificar a los solicitantes de asilo y a las personas que sean detenidas al cruzar de forma ilegal una frontera exterior de la Comunidad. Mediante la comparación de las impresiones dactilares, los Estados miembros pueden determinar si un solicitante de asilo o un nacional extranjero que se encuentre de forma ilegal en un Estado miembro ha solicitado asilo previamente en otro Estado miembro, o si un solicitante de asilo ha entrado de forma ilegal en el territorio de la Unión. En el momento de su adopción, el Reglamento por el que se creó Eurodac no contemplaba el acceso de la policía a este sistema; las impresiones dactilares se recogían para la finalidad muy concreta que se indica en el artículo 1.1 del Reglamento Eurodac.

8. El artículo 1.2 del Reglamento propuesto amplía ahora la finalidad del sistema Eurodac y añade los fines de prevención, detección e investigación de delitos de terrorismo y otros delitos graves, en las condiciones establecidas en las propuestas. Este cambio de finalidad se explica en el considerando 6 de la Decisión propuesta, que estipula lo siguiente: «Puesto que el sistema Eurodac se creó para facilitar la aplicación del Reglamento de Dublín, el acceso a Eurodac con fines de prevención, detección e investigación de los delitos de terrorismo y otros delitos graves constituye un cambio en el propósito original de Eurodac, que interfiere con el derecho al respeto de la vida privada de aquellos individuos cuyos datos personales se hayan procesado en el sistema Eurodac».

9. El acceso a Eurodac por parte de las fuerzas de seguridad ya se había anunciado en el pasado, algunos años después de la adopción del Reglamento Eurodac. Ello se menciona en documentos tales como el Programa de La Haya, las conclusiones del Comité Mixto del Consejo JAI de los días 12 y 13 de junio de 2007 y la comunicación de la Comisión al Consejo y al Parlamento Europeo sobre una mayor eficacia, interoperabilidad y sinergia entre las bases de datos europeas en el ámbito de la Justicia y los Asuntos de Interior, del 24 de noviembre de 2005⁽⁹⁾: «Por lo que se refiere al objetivo de luchar contra el terrorismo y la delincuencia, el Consejo considera ahora como una deficiencia la falta de acceso de las autoridades responsables de la seguridad interior a los datos del VIS. Se podría hacer la misma observación con respecto a los datos de inmigración contenidos en el SIS II y a los datos Eurodac».

10. Tal como se reconoce tanto en la evaluación de impacto como en la exposición de motivos, las propuestas de hacer Eurodac accesible a los servicios de seguridad han provocado críticas considerables por parte de varias partes interesadas.

⁽⁹⁾ COM(2005) 597 final, punto 4.6.

III. OBJETO DEL DICTAMEN

11. En el presente dictamen el SEPD analizará la legitimidad de las propuestas. Este análisis llevará a la conclusión de que el SEPD alberga serias dudas acerca de si estas propuestas son legítimas y de si deben adoptarse instrumentos legislativos basados en ellas.
12. El análisis se llevará a cabo con arreglo a las etapas siguientes:
 - a) punto de partida: determinar cómo se puede encontrar un justo equilibrio entre la necesidad de seguridad pública y el derecho a la protección de los datos;
 - b) las propuestas como continuación de dos tendencias más generales:
 - i) a los servicios de seguridad se les facilita cada vez más la utilización de datos correspondientes a personas que no guardan una relación directa con un delito determinado y que fueron recogidos para otros fines;
 - ii) se han propuesto nuevos instrumentos jurídicos, junto a los instrumentos ya existentes, que todavía no se han aplicado plenamente. Ello plantea una serie de cuestiones sobre la necesidad de contar con esos nuevos instrumentos;
 - c) las circunstancias concretas del presente caso. Se encuentra disponible un gran volumen de información en este ámbito para las fuerzas de seguridad;
 - d) la propuesta incidirá principalmente en un grupo social especialmente vulnerable, a saber, los solicitantes de asilo, con el riesgo de estigmatizar aún más a dicho grupo;
 - e) el calendario de las propuestas. Las propuestas se adoptan sin esperar dos importantes cambios de contexto que podrían tener una incidencia significativa, a saber, el Programa de Estocolmo y la (posible) entrada en vigor del Tratado de Lisboa. Además, cada propuesta se hace independientemente de la refundición general de los Reglamentos «Eurodac» y «Dublín», que aún son objeto de debate en el Consejo y el Parlamento Europeo;
 - f) la compatibilidad con el artículo 8 del Convenio Europeo de Derechos Humanos.
13. En el presente dictamen no se analizarán en detalle las disposiciones materiales de las propuestas. En general, la calidad legislativa de las propuestas es buena. Las propuestas están bien redactadas y garantizan unas condiciones estrictas con arreglo a las cuales las autoridades de los Estados miembros y Europol puedan solicitar la comparación de los datos relativos a las impresiones dactilares con los datos almacenados en la base de datos central de

Eurodac. No obstante, en los puntos 49 y 50 del presente dictamen se harán algunas observaciones sobre el aspecto material.

IV. EL PUNTO DE PARTIDA

14. El SEPD desea poner de relieve que un mejor intercambio de información es un objetivo político fundamental para la Unión Europea. Este énfasis en el intercambio de información es más lógico aún si se tiene en cuenta la ausencia de una fuerza policial europea, un sistema judicial europeo en el ámbito penal y un control europeo de las fronteras totalmente armonizado. Las medidas relativas a la información son, por tanto, una contribución fundamental de la Unión Europea que permite a las autoridades nacionales de los Estados miembros abordar la delincuencia transfronteriza de manera eficaz y proteger de forma efectiva las fronteras exteriores. No obstante, dichas medidas deberían contribuir no sólo a la seguridad de los ciudadanos, sino también a la protección de sus libertades fundamentales.
15. Dicho de otro modo, los gobiernos necesitan instrumentos adecuados para garantizar la seguridad del ciudadano, pero dentro de nuestra sociedad europea deben respetar plenamente los derechos fundamentales del mismo ciudadano. Corresponde al legislador de la UE garantizar ese equilibrio. La necesidad de ese equilibrio se destaca explícitamente en la comunicación de la Comisión de 10 de junio de 2009 sobre un espacio de libertad, seguridad y justicia al servicio de los ciudadanos⁽¹⁰⁾. Asimismo, ese equilibrio desempeña un papel importante en los debates en torno a un nuevo programa plurianual en el espacio de la libertad, la seguridad y la justicia (el «Programa de Estocolmo»).
16. En este contexto conviene destacar que la legislación en materia de protección de datos no perjudica en modo alguno los intereses legítimos de los gobiernos de proteger la seguridad pública. Podrán utilizarse los datos que resulten necesarios para alcanzar un fin específico y legítimo, si procede recurriendo a medidas adicionales que proporcionen las garantías adecuadas. También es fundamental que la información sea recogida, compartida y tratada únicamente en función de necesidades concretas en materia de seguridad y teniendo en cuenta los principios de la protección de datos.
17. La lucha contra los delitos terroristas y otros delitos graves⁽¹¹⁾ puede ser ciertamente un motivo legítimo para permitir el tratamiento de datos personales, de conformidad con los derechos fundamentales a la intimidad y la protección de datos. No obstante, para ser válida, la necesidad de dicha intervención debe basarse en elementos claros e innegables, y la proporcionalidad del tratamiento debe quedar demostrada. Ello resulta aún más necesario en caso de que se produzca una amplia intermisión en los derechos de las personas que constituyen un grupo vulnerable necesitado de protección, tal como se prevé en las propuestas.

⁽¹⁰⁾ COM(2009) 262 final. Véase también el punto 22 del dictamen del SEPD de 10 de julio de 2009 sobre dicha comunicación.

⁽¹¹⁾ Se trata de los fines previstos en el artículo 1 de la Decisión propuesta para permitir la comparación de impresiones dactilares.

V. LA CONTINUACIÓN DE TENDENCIAS MÁS GENERALES

Tendencia a proporcionar a las fuerzas de seguridad un mayor acceso a los datos

18. Debe destacarse que las propuestas no sólo siguen la tendencia general de garantizar a las fuerzas de seguridad el acceso a varios sistemas de información e identificación de largo alcance, sino que también dan un paso más dentro de la tendencia a proporcionar a las fuerzas de seguridad el acceso a datos de personas que, en principio, no son sospechosas de haber cometido un delito. Ello afecta, además, a los datos que se han recogido para fines que no guardan relación con la lucha contra la delincuencia. Ejemplos recientes de ello son:

— la Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE ⁽¹²⁾.

— decisión 2008/633/JAI del Consejo de 23 de junio de 2008 sobre el acceso para consultar el Sistema de Información de Visados (VIS) por las autoridades designadas de los Estados miembros y por Europol, con fines de prevención, detección e investigación de delitos de terrorismo y otros delitos graves ⁽¹³⁾,

— la Propuesta de Decisión marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros (Passenger Name Record – PNR) con fines policiales ⁽¹⁴⁾.

19. En sus dictámenes sobre dichas iniciativas, el SEPD ha adoptado un enfoque crítico en lo que se refiere a facilitar el acceso de las fuerzas de seguridad a datos correspondientes a personas que no sean sospechosas de haber cometido ningún delito y que se hayan recogido para otros fines. El SEPD destaca la necesidad de dar una justificación adecuada y superar las pruebas de necesidad y proporcionalidad. En su dictamen sobre los PNR, el SEPD previno contra la tendencia hacia una sociedad sometida a una vigilancia total.

20. Este enfoque se especificó en el dictamen del SEPD sobre la comunicación de la Comisión de 10 de junio de 2009 relativa a un espacio de libertad, seguridad y justicia al

servicio de los ciudadanos ⁽¹⁵⁾. En este dictamen se invita a abordar específicamente en el Programa de Estocolmo la tendencia a utilizar información recogida para otros fines. Es necesario fijar condiciones estrictas, como la condición de que las solicitudes de datos sean proporcionadas, tengan una finalidad bien precisa y, en principio, se basen en sospechas relativas a personas concretas.

Necesidad de un debate general sobre el acceso por parte de las fuerzas de seguridad

21. El presente dictamen debe considerarse en el contexto de un debate más amplio sobre el futuro del intercambio de información en la UE y la tendencia creciente a facilitar a las fuerzas de seguridad el acceso a bases de datos de un volumen considerable. EL SEPD aprovecha esta ocasión para destacar la necesidad de llevar a cabo una evaluación concreta de cada propuesta de este tipo y de tener una visión coherente, global y orientada al futuro acerca de esta materia, si es posible en relación con el Programa de Estocolmo.

22. Actualmente se ve más claramente que nunca la necesidad de reflexionar en profundidad sobre la manera en que debería configurarse el intercambio de información y los sistemas informáticos de gran escala en la UE. En esta reflexión deberán tenerse debidamente en cuenta tanto los costes que se derivarán para la intimidad como la eficacia en la aplicación de la ley, en primer lugar cuando se propongan y debatan nuevos instrumentos, pero también después de haberse aplicado dichos instrumentos, para lo cual deberán realizarse las oportunas revisiones periódicas. Ello es también un asunto que requiere garantías adaptadas a cada caso y una mayor atención al principio de limitación de la finalidad. Esta visión debe dar cabida a una reflexión sobre la (posible) entrada en vigor del Tratado de Lisboa y sus repercusiones en los sistemas que se apoyan en una base jurídica del Primer y Tercer Pilar.

Evaluación de los instrumentos existentes

23. Las actuales propuestas se adoptaron como complemento de los instrumentos jurídicos existentes utilizados para la consulta de impresiones dactilares, que todavía no se han aplicado plenamente. En este contexto, el SEPD remite en particular a la Decisión «Prüm» ⁽¹⁶⁾, que los Estados miembros deberán aplicar para junio de 2011. Sobre la base de esta Decisión, los Estados miembros se conceden acceso automatizado mutuo, por ejemplo, a los Sistemas Automáticos de Identificación Dactilar (AFIS) nacionales, utilizando un sistema para saber si el dato buscado está o no en la base consultada. Si una consulta efectuada sobre la base de la Decisión «Prüm» tiene un resultado positivo, puede obtenerse información suplementaria, incluidos los datos personales, en el Estado miembro que registró la impresión dactilar en su sistema automatizado nacional de identificación dactiloscópica de conformidad con el Derecho interno, incluidas las normas sobre asistencia judicial mutua.

⁽¹²⁾ DO L 105 de 13.4.2006, p. 54. Dictamen del SEPD de 26 de septiembre de 2005, DO C 298 de 29.11.2005, p. 1.

⁽¹³⁾ DO L 218 de 13.8.2008, p. 129.

⁽¹⁴⁾ Aún no adoptada por el Consejo; el último texto disponible en el registro del Consejo es el documento 5618/2/09, de 29 de junio de 2009. Dictamen del SEPD de 20 de diciembre de 2007, DO C 110 de 1.5.2008, p. 1.

⁽¹⁵⁾ Véase la nota 8.

⁽¹⁶⁾ Véanse también el punto 6 y la nota 6.

24. Otro instrumento que podría utilizarse en este contexto es la Decisión marco 2006/960/JAI sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea ⁽¹⁷⁾. Este instrumento facilita el intercambio de la información (es decir, las impresiones dactilares, así como la información suplementaria) que poseen tienen los servicios de seguridad de los Estados miembros o que está puesta a su disposición. Este instrumento es operativo desde el 18 de diciembre de 2008.
25. El único instrumento que está a disposición de los Estados miembros desde hace más tiempo es el instrumento tradicional de asistencia judicial mutua, en virtud de la cual la cual las autoridades judiciales de los Estados miembros pueden solicitar acceso a las bases de impresiones dactilares de carácter penal y no penal, incluso respecto de los solicitantes de asilo, sobre la base del Convenio relativo a la asistencia judicial en materia penal.
26. El SEPD considera esencial que, en primer lugar, se lleve a cabo y evalúe la aplicación de los nuevos instrumentos de la UE que permiten a un Estado miembro consultar impresiones dactilares y otros datos de carácter policial que estén en posesión de otro Estado miembro como parte de la evaluación de la necesidad de acceder a Eurodac.
27. El cumplimiento del principio de proporcionalidad no sólo implica que la medida propuesta sea efectiva, sino también que la finalidad prevista por la propuesta no puede alcanzarse recurriendo a los instrumentos existentes. Dichos instrumentos deben evaluarse cuidadosamente antes de que se establezcan medidas adicionales o nuevas para tratar la información personal. En opinión del SEPD, dicha evaluación no ha tenido lugar.

VI. LAS CIRCUNSTANCIAS ESPECÍFICAS DEL PRESENTE CASO

28. En primer lugar, el SEPD observa que la Comisión, en su comunicación de 24 de noviembre de 2005, recordaba que «la solicitud de asilo o de visado no indica en modo alguno que una persona hasta ahora inocente vaya a cometer una infracción penal o un acto terrorista» ⁽¹⁸⁾.
29. Las propuestas afectan al acceso a los datos correspondientes a personas que, en principio, no sólo no son sospechosas de ningún delito, sino que necesitan una mayor protección debido a que huyen de una persecución. Estas personas representan una población especialmente vulnerable y la precariedad de su situación debe tomarse en consideración al evaluar la necesidad y proporcionalidad de la medida propuesta.
30. En la exposición de motivos de la decisión propuesta se señala que existe una carencia estructural de información y

verificación, al no haber en la actualidad ningún sistema individual accesible a los servicios de seguridad que les permita determinar el Estado miembro que posee información sobre un solicitante de asilo.

31. Aunque ello pueda ser cierto, no responde a la cuestión de por qué se requiere dicha información respecto de solicitantes de asilo que constituyen, como ya se señaló anteriormente, un grupo vulnerable y, en principio, no son sospechosos, mientras que una información similar sobre impresiones dactilares no está disponible en relación con cualquier otro grupo social. Puede haber buenas razones para ello, pero la Comisión no las da.
32. El SEPD llama también la atención sobre una justificación adicional de las propuestas. En la exposición de motivos de la Decisión propuesta se menciona que, en caso de que una consulta efectuada sobre la base de la Decisión «Prüm» tenga un resultado positivo, puede obtenerse información suplementaria, incluidos los datos personales, en el Estado miembro que registró la impresión dactilar en su sistema automatizado nacional de identificación dactiloscópica de conformidad con el Derecho interno, incluidas las normas sobre asistencia judicial mutua. Dicho esto, la Comisión parece utilizar como argumento para justificar la propuesta aludiendo a que «si bien este procedimiento puede ser útil cuando los Estados almacenen impresiones dactilares de solicitantes de asilo junto con las otras impresiones dactilares recogidas por los servicios de seguridad en un sistema automatizado nacional de identificación dactiloscópica, no dará frutos cuando los sistemas automatizados nacionales de identificación dactiloscópica no almacenen impresiones dactilares de solicitantes de asilo a menos que estén relacionadas con la delincuencia». Este argumento también se hace valer en la evaluación de impacto que acompaña a las propuestas.
33. El SEPD considera que dicho argumento no tiene ningún peso. El almacenamiento sistemático de las impresiones dactilares de los solicitantes de asilo que no guarden relación con ningún delito en la misma base de datos que contenga otras impresiones dactilares (de solicitantes de asilo y otras personas sospechosas o culpables de la comisión de un delito) recogidas por las autoridades policiales plantea en sí mismo graves problemas en lo que se refiere al principio de limitación de la finalidad y a la legitimidad del tratamiento de datos. En lugar de recurrir a este argumento, la Comisión debe examinar si dicho almacenamiento sistemático respeta la legislación de la UE en materia de protección de datos.

VII. CALENDARIO DE LAS PROPUESTAS

34. La adopción de las propuestas por la Comisión tiene lugar en un momento en que el contexto está cambiando.

⁽¹⁷⁾ DO L 386 de 29.12.2006, p. 89.

⁽¹⁸⁾ Comunicación mencionada en el punto 9 del presente dictamen.

35. En primer lugar, la adopción del Programa de Estocolmo se espera para diciembre de 2009. En estos meses se están manteniendo intensos debates sobre la redacción de este programa plurianual en el ámbito de la libertad, la seguridad y la justicia. El uso e intercambio de información será un punto importante del Programa de Estocolmo, que incluye la creación de un modelo europeo de información⁽¹⁹⁾ o una estrategia europea de gestión de la información para la seguridad⁽²⁰⁾. En este contexto, el SEPD aboga por un planteamiento equilibrado según el cual las garantías relativas a la intimidad y la protección de datos ya estén incluidas lo antes posible en los sistemas de información. Las actividades del Grupo *ad hoc* «Intercambio de Información» del Consejo están estrechamente relacionadas con el Programa de Estocolmo. Es sumamente probable que el asunto de que tratan las actuales propuestas sea objeto de dichas actividades.
36. En segundo lugar, el SEPD llama la atención sobre la necesidad de reflexionar sobre las consecuencias que tendrá la entrada en vigor del Tratado de Lisboa en la futura legislación relativa a las actividades de las fuerzas de seguridad. La primera consecuencia sería que cualquier propuesta de este tipo estaría sujeta en el futuro al procedimiento legislativo ordinario, lo cual implicaría una implicación por igual del Consejo y del Parlamento Europeo. La segunda consecuencia guarda relación con la supresión de la estructuración en pilares del Tratado de la UE. El Tratado de Lisboa podría hacer necesario que la Comisión presente una nueva propuesta fundamentada en la nueva base jurídica, posiblemente fusionando incluso las propuestas de Reglamento y Decisión en un único instrumento jurídico, lo cual, en cualquier caso, contribuiría a la claridad jurídica.
37. En tercer lugar, el SEPD cuestiona también la necesidad de adoptar la presente propuesta siguiendo un procedimiento distinto de la refundición general de los Reglamentos Eurodac y «Dublín», que todavía se están debatiendo en el Parlamento y el Consejo. La consecuencia de las presentes propuestas es que, aunque no hayan finalizado los debates fundamentales en torno a la modificación del sistema Eurodac, se modificará la finalidad del sistema, lo cual significa también otra modificación fundamental del mismo. Se hubiera garantizado mejor la coherencia si estas propuestas hubieran sido objeto de la refundición general⁽²¹⁾ o se hubieran aplazado hasta que se haya adoptado la primera modificación.
38. En vista de las circunstancias, es mejor aplazar la adopción de la propuesta para evitar la inseguridad jurídica. La Comisión no pretende que las propuestas se adopten urgentemente, y ciertamente ninguna circunstancia justifica dicha urgencia.

VIII. COMPATIBILIDAD CON EL ARTÍCULO 8 DEL CONVENIO EUROPEO DE DERECHOS HUMANOS (CEDH)

39. En la exposición de motivos del Reglamento propuesto se trata explícitamente del cumplimiento de los derechos fun-

damentales, y en particular del artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, sobre la protección de datos de carácter personal. En dicha exposición de motivos se indica que, según la Comisión, para garantizar que el tratamiento de datos personales con fines policiales no lesione el derecho fundamental a la protección de datos personales y, en particular, los principios de necesidad y proporcionalidad, la propuesta impone a los servicios de seguridad unas condiciones estrictas.

40. Al SEPD no le convence esta afirmación de la Comisión. El SEPD señala que es fundamental comprobar que las propuestas superan la prueba de la legitimidad con arreglo al artículo 8 del Convenio Europeo de Derechos Humanos, según la interpretación del Tribunal de Justicia y del Tribunal Europeo de Derechos Humanos. Las propuestas deben cumplir los principios de necesidad y proporcionalidad, teniendo en cuenta el contexto de los instrumentos de que ya se dispone. La Comisión debe demostrar de forma fehaciente esa cuestión en la propuesta o en la exposición de motivos. El asunto de referencia a este respecto es *S. y Marper contra el Reino Unido*⁽²²⁾.
41. En el considerando 6 de la decisión propuesta se afirma que «cualquier interferencia de este tipo debe llevarse a cabo de conformidad con la ley, la cual ha de formularse con la suficiente precisión como para que los particulares puedan adaptar su conducta, debe proteger a las personas de la arbitrariedad e indicar con suficiente claridad el alcance del poder discrecional conferido a los servicios competentes y el modo de su ejercicio. En una sociedad democrática cualquier interferencia de este tipo ha de ser necesaria para satisfacer un interés legítimo y proporcional y ha de ser proporcional al objetivo legítimo que pretende alcanzar». No obstante, los considerandos no muestran por qué es necesario el actual instrumento propuesto.
42. Una jurisprudencia bien sentada del Tribunal europeo de Derechos Humanos muestra que una injerencia se considerará necesaria en una sociedad democrática para un fin legítimo, tal como lo requiere el artículo 8.2 del CEDH, si responde a una «necesidad social imperiosa» y, en particular, si guarda proporción con el fin legítimo que se persigue y las razones que aduzcan las autoridades nacionales para su justificación, son pertinentes y suficientes⁽²³⁾. Las autoridades nacionales disfrutaban también de un margen de apreciación cuyo alcance dependerá no sólo de la naturaleza del fin legítimo que se persiga, sino también de la índole particular de la injerencia de que se trate⁽²⁴⁾. El margen tenderá a disminuir cuando el derecho que esté en juego sea crucial para el disfrute efectivo por cada persona de derechos íntimos o básicos⁽²⁵⁾.

⁽²²⁾ Demandas acumuladas 30562/04 y 30566/04, *S. y Marper contra el Reino Unido*, sentencia del 4 de diciembre de 2008, TEDH, pendiente de publicación.

⁽²³⁾ Véase, por ejemplo, la sentencia correspondiente al asunto *Gillow contra el Reino Unido*, del 24 de noviembre de 1986, serie A, n° 109, apartado 55.

⁽²⁴⁾ Véase la sentencia correspondiente al asunto *Leander contra Suecia*, del 26 de marzo de 1987, serie A, n° 116, apartado 59. Véase también la sentencia del Tribunal de Justicia del 20 de mayo de 2003, *Österreichische Rundfunk y otros*, asuntos acumulados C-465/2000, C-138/01 y C-139/01, Rec. [2003], p. I-4989, apartado 83.

⁽²⁵⁾ *Connors contra el Reino Unido*, sentencia del 27 de mayo de 2004, n° 66746/01, apartado 82.

⁽¹⁹⁾ Expresión utilizada por la Comisión en su comunicación de 10 de junio de 2009, mencionada en la nota 8.

⁽²⁰⁾ Expresión utilizada por la presidencia sueca.

⁽²¹⁾ Véase el punto 4.

43. En este contexto, es necesario ante todo evaluar la finalidad del tratamiento de datos personal que se pretenda llevar a cabo: ¿se ha determinado claramente dicha finalidad? ¿demuestra esta finalidad su necesidad y proporcionalidad? También debe probarse que no se dispone de otros medios menos invasivos para alcanzar la finalidad propuesta.
44. En la propuesta se mantiene que la finalidad de Eurodac se ha modificado con respecto a la finalidad inicial, tal como se explica en el considerando 6 de la Decisión propuesta⁽²⁶⁾. No obstante, un simple cambio en un texto legislativo no se traducirá en una medida que sea compatible con el artículo 8 del CEDH. Se puede incluso sostener que el cambio legislativo no se traduce en absoluto en un cambio de finalidad. Los datos también serán almacenados en el futuro en el sistema Eurodac con la única finalidad de facilitar la aplicación del Reglamento «Dublín». Sólo en situaciones excepcionales, tal como se expuso en el presente dictamen, las autoridades policiales nacionales tendrán acceso a dichos datos. Así, pues, las propuestas, aunque no cambian la finalidad, deben considerarse como excepciones del principio de limitación de la finalidad, que pueden aceptarse con arreglo al artículo 13 de la Directiva 95/46/CVE, bajo ciertas condiciones. No obstante, el SEPD no está convencido de que en el presente caso se den dichas condiciones.
45. En este contexto, el SEPD hace hincapié en que declarar simplemente un cambio de finalidad de la propuesta legislativa no hace aceptable dicho cambio. Un cambio legislativo no conduce por sí mismo a una apreciación diferente acerca de si las propuestas son necesarias en una sociedad democrática, son proporcionadas y resultan por lo demás aceptables con arreglo a las disposiciones mencionadas en el punto anterior.
46. El carácter invasivo de los instrumentos propuestos por la Comisión resulta evidente. No obstante, su utilidad y necesidad distan mucho de quedar demostradas en las propuestas. Su necesidad debe demostrarse aportando pruebas concluyentes de que existe un vínculo entre los solicitantes de asilo y el terrorismo o la delincuencia grave. Las propuestas no aportan esas pruebas. Aunque es cierto que pueden haber entrado sospechosos en el territorio de la UE presentando una solicitud de asilo falsificada, el hecho de que dicho caso sea posible no debe hacer que se presente como un modelo general que justifique la adopción de los instrumentos de que se trata.
47. Otra cuestión que también resulta particularmente preocupante en el presente contexto es el riesgo de estigmatización debido al hecho de que las personas que se encuentren en la situación de solicitantes, no hayan sido condenadas por ningún delito y gocen de la presunción de inocencia sean tratadas del mismo modo que los sospechosos *a priori*⁽²⁷⁾. A este respecto, el Tribunal Europeo de Derechos Humanos tiene presente que el derecho a la presunción de inocencia que el Convenio otorga a cada persona incluye la norma general de que ninguna sospecha relativa a la in-

ciencia de una persona puede ser expresada después de su absolución⁽²⁸⁾.

48. Por otra parte, el SEPD considera que el posible argumento de que el acceso directo a Eurodac por parte de las autoridades policiales es conveniente, fácil y rápido no debe ser suficiente para que la propuesta supere la prueba de la necesidad. La demostración de la necesidad no puede basarse en la mera utilidad del acceso incluso en el marco de salvaguardias estrictas de protección de datos. En resumen, el SEPD duda seriamente de la legitimidad de las propuestas en relación con el artículo 8 del CEDH.

IX. ALGUNAS OBSERVACIONES SOBRE EL ASPECTO MATERIAL

49. Dicho sea de paso, el SEPD recomienda que en el texto del artículo 2 *bis* del Reglamento propuesto se haga una especificación, o, como alternativa al respecto, se añada en la Decisión propuesta que el acceso a Eurodac podrá garantizarse a las autoridades policiales cuando éstas tengan una razón específica para creer que un sospechoso ha solicitado asilo previamente. Ello se sugiere en la exposición de motivos, pero no figura en el texto de la propia propuesta. El SEPD cree que dicha salvaguardia comportaría un importante valor añadido. No obstante, esta sugerencia no significa en sí misma que el SEPD acepte el principio del acceso de las fuerzas de seguridad a Eurodac. Ello debe entenderse como una recomendación subsidiaria.
50. El SEPD observa también que los estrictos criterios para el acceso a Eurodac por parte de las autoridades designadas⁽²⁹⁾ no se aplican al acceso a los datos de Eurodac por parte de Europol. Las solicitudes de comparación por parte de Europol son permitidas a efectos de la realización de un análisis específico o de un análisis de carácter general y de tipo estratégico. El SEPD se pregunta cómo las mayores facilidades que se conceden a Europol pueden ajustarse al razonamiento que hace la Comisión, a saber, que el acceso sólo es necesario en casos y circunstancias específicos y bajo ciertas condiciones.

X. CONCLUSIÓN

51. El SEPD duda seriamente de la legitimidad de las actuales propuestas y de la necesidad de adoptar instrumentos legislativos basados en las mismas. Las dudas se basan en las consideraciones expresadas en el presente dictamen, y que pueden resumirse como sigue:
52. El SEPD desea poner de relieve que un mejor intercambio de información es un objetivo político fundamental para la Unión Europea. Los gobiernos necesitan instrumentos adecuados para garantizar la seguridad del ciudadano, pero en el marco de nuestra sociedad europea deben respetar plenamente los derechos fundamentales de los ciudadanos. Corresponde al legislador de la UE garantizar ese equilibrio.

⁽²⁶⁾ Véase al punto 8 del presente dictamen.

⁽²⁷⁾ S. y Marper.

⁽²⁸⁾ *Asan Rushiti* contra Austria, nº 28389/95, apartado 31, 21 de marzo de 2000, con otras referencias, 33º Repertorio de Jurisprudencia del Tribunal Europeo de Derechos Humanos, p. 56.

⁽²⁹⁾ Artículo 7 de la decisión propuesta; véase el punto 6 del presente dictamen.

53. Las medidas para combatir los delitos terroristas y otros delitos graves pueden ser una razón válida para permitir el tratamiento de datos personales, siempre que la necesidad de la intervención se base en elementos claros e innegables y quede demostrada la proporcionalidad del tratamiento. Ello resulta aún más necesario debido a que las propuestas afectan a un grupo vulnerable necesitado de un alto grado de protección, ya que está constituido de personas que huyen de una persecución. Su situación de precariedad debe tenerse en cuenta al evaluar la necesidad y proporcionalidad de la acción propuesta. El SEPD llama también la atención sobre el riesgo de estigmatización.
54. El SEPD recomienda que se evalúe la legitimidad de las propuestas en un contexto más amplio, a saber:
- a) la tendencia a garantizar el acceso de las fuerzas de seguridad a los datos personales de las personas no sospechosas de haber cometido un delito y que han sido recogidos para otros fines;
 - b) la necesidad de llevar a cabo una evaluación puntual de cada propuesta de este tipo y de tener una visión coherente, global y orientada al futuro, si es posible en relación con el Programa de Estocolmo;
 - c) la necesidad de llevar a cabo y evaluar en primer lugar la aplicación de otros instrumentos de la UE que permiten a un Estado miembro consultar impresiones dactilares y otros datos de carácter policial que estén en posesión de otro Estado miembro;
- d) el carácter urgente de la propuesta, en relación con un entorno jurídico y político cambiante.
55. Por lo que respecta a la compatibilidad de las propuestas con el artículo 8 del CEDH, el SEPD cuestiona el cambio de finalidad del sistema y hace hincapié en que declarar simplemente el cambio de finalidad de una propuesta no constituye realmente un cambio. Además, un cambio legislativo no conduce por sí mismo a una apreciación diferente acerca de si las propuestas son necesarias en una sociedad democrática, son proporcionadas y resultan por lo demás aceptables, especialmente teniendo en cuenta las normas relativas a la limitación de la finalidad que se recogen en la Directiva 95/46/CE.
56. El SEPD pone de relieve que la necesidad debe demostrarse aportando pruebas concluyentes de que existe un vínculo entre los solicitantes de asilo y el terrorismo o la delincuencia grave. Las propuestas no aportan esas pruebas.
57. Por último, el SEPD muestra su satisfacción por el hecho de que se le haya consultado y de que se haga referencia a esta consulta en el preámbulo de la propuesta, al igual que se hizo en otros textos legislativos sobre los que se ha consultado al SEPD de conformidad con el Reglamento (CE) n° 45/2001. Asimismo, el SEPD hace algunas observaciones sobre el texto material de las propuestas.

Hecho en Bruselas el 7 de octubre de 2009.

Peter HUSTINX
Supervisor Europeo de Protección de Datos