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

(2009/C 276/02)

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,

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, y en particular su artículo 41.

HA ADOPTADO EL SIGUIENTE DICTAMEN:

I. **INTRODUCCIÓN:**

1. El 10 de junio de 2009 la Comisión adoptó su comunicación al Parlamento Europeo y al Consejo relativa a un espacio de libertad, seguridad y justicia al servicio de los ciudadanos ([1]). El SEPD presenta su dictamen con arreglo al artículo 41 del Reglamento (CE) nº 45/2001.

2. Antes de la adopción de la comunicación, la Comisión, mediante carta fechada el 19 de mayo de 2009, consultó de modo informal al SEPD sobre la misma. El SEPD respondió a esta consulta el 20 de mayo de 2009 enviando observaciones informales destinadas a mejorar el texto de la comunicación. Además, el SEPD contribuyó activamente a la redacción de la carta del Grupo «Policía y Justicia» , fechada el 14 de enero de 2009, sobre el programa plurianual en el espacio de libertad, seguridad y justicia ([2]).

3. En la comunicación (apartado 1) se destaca que «la Unión debe dotarse de un nuevo programa plurianual que, a partir de los progresos logrados y de las enseñanzas extraídas de las deficiencias actuales, tenga una ambiciosa proyección de futuro. Este nuevo programa debería definir las prioridades para los cinco próximos años». Este programa plurianual (que ya se conoce bajo el nombre de «programa de Estocolmo») supondrá la continuidad de los programas de Tampere y La Haya, que proporcionaron un gran impulso político al espacio de libertad, seguridad y justicia.

4. Se considera que la comunicación constituye la base de este nuevo programa plurianual. En este contexto, el SEPD observa que, si bien los programas plurianuales no son en sí instrumentos vinculantes, influyen considerablemente en la política que las instituciones van a desarrollar en el ámbito de que se trate, dado que muchas de las medidas legislativas y no legislativas se derivarán de un programa determinado.

5. La propia comunicación debe verse desde este punto de vista. Constituye la próxima fase en un debate que comenzó aproximadamente con los dos informes presentados en junio de 2008 por los denominados Grupos «Futuro», que fueron creados por la Presidencia del Consejo para aportar ideas, y que llevan los siguientes títulos: «Libertad, seguridad e intimidad: los asuntos de interior europeos en un mundo abierto» ([3]) y «Propuestas de solución para el futuro programa de justicia de la UE» ([4]).

II. **CONTENIDO BÁSICO DEL DICTAMEN**

6. El presente dictamen no sólo representa una reacción frente a la comunicación, sino que es también una contribución del SEPD a un debate más general sobre el futuro del espacio de libertad, seguridad y justicia, que deberá dar lugar a un nuevo programa de trabajo estratégico (el programa de Estocolmo), tal como lo anunció la Presidencia sueca de la UE ([5]). En el dictamen se examinarán también algunas consecuencias de la posible entrada en vigor del Tratado de Lisboa.

7. Tras especificarse en la parte III las principales perspectivas del dictamen, en la parte IV se hace una evaluación general de la comunicación.

8. En la parte V se trata la cuestión de cómo responder a la necesidad de respetar continuamente la protección de la intimidad y de los datos personales en un contexto de creciente intercambio de dichos datos. La atención se centrará en el apartado 2.3 de la comunicación, que trata de la protección de los datos personales y de la intimidad, y, de manera más general, en las necesidades de nuevas medidas legislativas y no legislativas destinadas a mejorar el marco de la protección de datos.

([1]) COM(2009) 262 final («la comunicación»)

([2]) Sin publicar. El Grupo «Policía y Justicia» fue creado por la Conferencia Europea de Comisarios encargados de la protección de datos para definir sus posiciones en el ámbito de la aplicación de la ley y actuar en su nombre en casos urgentes.

([3]) Doc. nº 11657/08. Denominado en lo sucesivo «el informe sobre Asuntos de Interior».

([4]) Doc. nº 11549/08 (en lo sucesivo, «el informe sobre la justicia»)

([5]) Programa de trabajo del Gobierno sobre la UE, http://www.regeringen.se

9. En la parte VI se debaten las necesidades y posibilidades de almacenamiento, acceso e intercambio de información como instrumentos para la aplicación de la ley, o, en palabras de la comunicación, para «una Europa que protege». El apartado 4 de la comunicación recoge una serie de objetivos relativos al flujo de información y a las herramientas tecnológicas, concretamente en los apartados 4.1.2 (Controlar la información), 4.1.3 (Movilizar las herramientas tecnológicas necesarias) y 4.2.3.2 (Los sistemas de información). El desarrollo de un modelo europeo de información (en el apartado 4.1.2) puede considerarse como la propuesta que representa mayores retos en este contexto. En el dictamen del SEPD se analiza en detalle esta propuesta.

10. En la parte VII se aborda brevemente un asunto específico dentro del espacio de libertad, seguridad y justicia, de importancia para la protección de datos, a saber, el acceso a la justicia y a la justicia electrónica.

III. **PERSPECTIVAS DEL DICTAMEN**

11. En el presente dictamen se parte de la necesidad de proteger los derechos fundamentales como el prisma fundamental para el análisis de la comunicación y, de manera más general, el futuro del espacio de libertad, seguridad y justicia, tal como queda configurado en el nuevo programa plurianual. También se basará en las contribuciones del SEPD al desarrollo de la política de la UE en este ámbito, principalmente en lo que se refiere a su función asesora. Hasta ahora, el SEPD ha adoptado más de treinta dictámenes y observaciones sobre iniciativas derivadas del programa de La Haya, que pueden consultarse en su sitio web.

12. En su evaluación de la comunicación, el SEPD tendrá en cuenta, en particular, las cuatro perspectivas que se indican a continuación y que son pertinentes para el futuro del espacio de libertad, seguridad y justicia. Todas estas perspectivas también ocupan un lugar destacado en la comunicación.

13. La primera perspectiva es el crecimiento exponencial de la información digital relativa a los ciudadanos como resultado de la evolución de las tecnologías de la información y la comunicación ([6]). La sociedad se está desplazando hacia lo que a menudo se llama una «sociedad de la vigilancia», en la que cada transacción y casi cada movimiento de los ciudadanos puede dar lugar a un registro digital. La llamada «internet de las cosas» y la «inteligencia ambiental» se están desarrollando rápidamente mediante el empleo de etiquetas de identificación por radiofrecuencia (RFID). Las características digitales del cuerpo humano (datos biométricos) se utilizan cada vez más. Ello conduce a un mundo cada vez más interconectado en el que las organizaciones de seguridad pública podrán tener acceso a un gran volumen de información potencialmente útil, lo cual puede afectar directamente a la vida de las personas afectadas.

14. La segunda perspectiva es la internacionalización. Por una parte, en la era digital el intercambio de datos no está limitado por las fronteras exteriores de la Unión Europea, mientras que, por otra parte, cada vez es más necesaria la cooperación internacional en todas las actividades de la UE en el espacio de libertad, seguridad y justicia. La lucha contra el terrorismo, la cooperación policial y judicial, la justicia civil y el control de las fronteras constituyen sólo algunos ejemplos de ello.

15. La tercera perspectiva es la utilización de datos a efectos de aplicación de la ley. Amenazas recientes a la sociedad, relacionadas o no con el terrorismo, han dado lugar a (peticiones de) mayores posibilidades para las fuerzas y cuerpos de seguridad de recabar, almacenar e intercambiar datos personales. En muchos casos, los particulares están activamente implicados, como lo muestra, entre otras cosas, la Directiva sobre la conservación de datos ([7]) y los diversos instrumentos relativos al registro de nombres de los pasajeros (PNR) ([8]).

16. La cuarta perspectiva es la libre circulación. El desarrollo gradual de un espacio de libertad, seguridad y justicia requiere que se sigan suprimiendo las fronteras interiores y las posibles barreras a la libre circulación dentro de dicho Espacio. Los nuevos instrumentos en este ámbito no deberían en ningún caso volver a crear barreras. En el presente, la libre circulación incluye, por una parte, la libre circulación de personas y, por otra parte, la libre circulación de datos (personales).

17. Estas cuatro perspectivas muestran que el contexto en el que se utiliza la información está cambiando rápidamente. En dicho contexto, no cabe dudar de la importancia que tiene contar con un mecanismo vigoroso para proteger los derechos fundamentales de los ciudadanos, y en particular la intimidad y la protección de datos. Por los motivos antes expuestos, el SEPD ha elegido la necesidad de la protección como el prisma fundamental de su análisis, tal como se ha señalado en el Punto 11.

([6]) En este contexto, el «informe sobre Asuntos de Interior» habla de un «tsunami digital».

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

([8]) Véase, por ejemplo, el Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (Acuerdo PNR 2007), DO L 204 de 4.8.2007, p. 18, y la propuesta de Decisión marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros (Passenger Name Record — PNR) con fines represivos, doc. COM(2007) 654 final.

IV. **EVALUACIÓN GENERAL**

18. La comunicación y el programa de Estocolmo tienen por objeto especificar las intenciones de la UE en los próximos cinco años, con efectos posiblemente en un plazo incluso más dilatado. El SEPD observa que la comunicación está redactada en una manera que puede denominarse «neutra» con respecto a Lisboa. El SEPD entiende perfectamente por qué la Comisión ha adoptado este enfoque, pero lamenta que la comunicación no haya podido aprovechar plenamente las posibilidades adicionales que brinda el Tratado de Lisboa. En el presente dictamen se insistirá más en la perspectiva del Tratado de Lisboa.

19. La comunicación se basa en los resultados obtenidos con las medidas adoptadas en los últimos años en el espacio de libertad, seguridad y justicia. Dichos resultados pueden caracterizarse como orientados a los hechos, insistiéndose en las medidas que amplían los poderes de las autoridades encargadas de la aplicación de la ley y que resultan intrusivas para el ciudadano. Este es ciertamente el caso en aquellos ámbitos en que los datos personales son utilizados e intercambiados de manera intensiva y que son, por tanto, cruciales para la protección de datos. Los resultados están orientados a los hechos, ya que sucesos exteriores, como los del 11 de septiembre y los atentados de Madrid y Londres, dieron un fuerte impulso a la actividad legislativa. Por ejemplo, la transferencia de datos de pasajeros a los Estados Unidos puede considerarse una consecuencia de los acontecimientos del 11 de septiembre ([9]), mientras que los atentados de Londres condujeron a la Directiva 2006/24/CE sobre la retención de datos ([10]). Se insistió en la adopción de medidas más intrusivas, ya que el legislador de la UE se centró en las medidas que facilitan la utilización y el intercambio de datos, mientras que las medidas que garantizan la protección de los datos personales fueron examinadas con menos urgencia. La principal medida protectora adoptada fue 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 ([11]), tras tres años de debates en el Consejo. El resultado fue una Decisión del Consejo que no es totalmente satisfactoria (véanse los puntos 29 y 30).

20. La experiencia de los últimos años muestra que, antes de adoptar nuevos instrumentos, es necesario reflexionar sobre las consecuencias que estos instrumentos tendrán para las autoridades encargadas de la aplicación de la ley y para los ciudadanos europeos. En esta reflexión deberán tenerse debidamente en cuenta los costes que se derivarán para la intimidad y la eficacia en la aplicación de la ley, en primer lugar cuando se propongan y debatan nuevos instrumentos, pero también después de la aplicación de dichos instrumentos, para lo que deberán realizarse las oportunas revisiones periódicas. Esta reflexión es también fundamental antes de que un nuevo programa plurianual llegue a establecer las principales iniciativas para un futuro próximo.

21. EL SEPD se congratula de que en la comunicación se reconozca la protección de los derechos fundamentales, y en particular la protección de los datos personales, como uno de los aspectos clave del futuro del espacio de libertad, seguridad y justicia. En el apartado 2 de la comunicación se califica a la UE como un espacio único para la protección de los derechos fundamentales sobre la base de valores comunes. También merece beneplácito que en la comunicación se mencione la adhesión al Convenio Europeo de Derechos Humanos como cuestión prioritaria, incluso como la primera cuestión prioritaria. Esta adhesión es un importante paso adelante para garantizar un sistema coherente y armónico para la protección de los derechos fundamentales. Por último, también cabe destacar que en la comunicación se haya concedido un lugar eminente a la protección de datos.

22. La especial atención que la comunicación dedica a dicha cuestión muestra una firme intención de garantizar la protección de los derechos del ciudadano y, por ende, de adoptar un enfoque más equilibrado. Los gobiernos necesitan instrumentos adecuados para garantizar la seguridad del ciudadano, pero dentro de nuestra sociedad europea deben respetar plenamente los derechos fundamentales de los ciudadanos. El servicio a los ciudadanos ([12]) requiere que la Unión Europea mantenga ese equilibrio.

23. En opinión del SEPD, en la comunicación se tiene muy en cuenta la necesidad de dicho equilibrio, así como la necesidad de proteger los datos personales. También se reconoce la necesidad de modificar el énfasis. Ello es importante, ya que las políticas en el espacio de libertad, seguridad y justicia no deberían fomentar un desplazamiento gradual hacia una sociedad de la vigilancia. El SEPD espera que el Consejo adopte el mismo enfoque en el programa de Estocolmo, también mediante el reconocimiento de las orientaciones que se exponen en el punto 25 *infra*.

24. Esto último es tanto más importante por cuanto el espacio de libertad, seguridad y justicia es un ámbito que, como ha destacado recientemente el Tribunal Constitucional alemán en su sentencia de 30 de junio de 2009 sobre el Tratado de Lisboa, modela las circunstancias vitales del ciudadano, y en particular la esfera privada de su propia responsabilidad y de la seguridad personal y social, que está protegida por los derechos fundamentales ([13]).

([9]) Véase el Acuerdo PNR de 2007 mencionado en la nota anterior y otros acuerdos previos.

([10]) Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, DO L 105 de 13.4.2006, p. 54. Aunque la base jurídica es el artículo 95 del TCE, se trató de una reacción inmediata a los atentados de Londres.

([11]) 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, DO L 350 de 30.12.2008, p. 60.

([12]) Véase el título de la comunicación.

([13]) Comunicado de prensa nº 72/2009, de 30 de junio de 2009, del Tribunal Constitucional alemán, apartado 2 c).

25. El SEPD destaca que, en dicho espacio:

— debería intercambiarse la información entre las autoridades de los Estados miembros, incluyendo, si procede, organismos o bases de datos europeos, sobre la base de mecanismos adecuados y efectivos que respeten plenamente los derechos fundamentales del ciudadano y garanticen la confianza mutua,

— ello requiere no sólo la disponibilidad de la información, combinada con el reconocimiento mutuo de los sistemas jurídicos de los Estados miembros (y de la UE), sino también una armonización de las normas de protección de la información, por ejemplo, aunque no exclusivamente, a través de un marco común de protección de datos,

— estas normas comunes no deberían aplicarse únicamente a situaciones con una dimensión transfronteriza. La confianza mutua sólo puede existir cuando las normas son firmes y respetadas, sin riesgo de que no lleguen a aplicarse cuando la dimensión transfronteriza no sea evidente o deje de serlo. Aparte de esto, especialmente cuando se trata del uso de la información, las diferencias entre datos «internos» y «transfronterizos» no pueden funcionar en la práctica ([14]).

V. INSTRUMENTOS PARA LA PROTECCIÓN DE DATOS

V.1. Hacia un régimen único de protección de datos

26. El SEPD apoya el enfoque estratégico de otorgar a la protección de datos un lugar eminente en la comunicación. En efecto, muchas iniciativas del espacio de libertad, seguridad y justicia se basan en la utilización de datos personales, y una buena protección de datos es crucial para que esas iniciativas tengan éxito. El respeto de la intimidad y de la protección de datos no es sólo una obligación jurídica cada vez más reconocida a escala de la UE, sino también una cuestión fundamental para los ciudadanos europeos, tal como lo muestran los resultados del eurobarómetro ([15]). Por otra parte, la restricción del acceso a los datos personales es también fundamental para garantizar la confianza por parte de los organismos encargados de la aplicación de la ley.

27. En el apartado 2.3 de la comunicación se afirma la necesidad de un régimen único de protección de datos que cubra el conjunto de las competencias de la Unión ([16]). El SEPD apoya plenamente este objetivo, independientemente de la entrada en vigor del Tratado de Lisboa. También observa que dicho régimen no significa necesariamente que se trate de un marco jurídico que se aplique a todo tratamiento de datos. Según los tratados en vigor, las posibilidades de adoptar un marco jurídico único que se aplique a todo tratamiento de datos son limitadas debido a la estructura en pilares y al hecho de que (al menos en el primer pilar) la protección de los datos tratados por las instituciones europeas se realiza apoyándose en una base jurídica independiente (el artículo 286 del TCE). No obstante, el SEPD señala que pueden llevarse a cabo algunas mejoras si se aprovechan plenamente las posibilidades que brindan los tratados en vigor, como ya lo destacó la Comisión en su comunicación titulada «Ejecución del Programa de La Haya: el camino a seguir» ([17]). Tras la entrada en vigor del Tratado de Lisboa, el artículo 16 del Tratado de funcionamiento de la Unión Europea proporcionará la base jurídica necesaria para un marco jurídico único que se aplique a todo tratamiento de datos.

28. El SEPD observa que, en cualquier caso, es fundamental garantizar la coherencia del marco jurídico de la protección de datos, si es preciso mediante la armonización y consolidación de los diversos instrumentos jurídicos aplicables en el espacio de libertad, seguridad y justicia.

Con arreglo a los tratados vigentes

29. Recientemente se ha dado un primer paso con la adopción de la Decisión marco 2008/977/JAI del Consejo ([18]). No obstante, este instrumento jurídico no puede considerarse un marco único, debido fundamentalmente a que sus disposiciones no son de aplicación general. En efecto, sus disposiciones no se aplican a situaciones internas, cuando los datos personales tienen su origen en el Estado miembro que los utiliza. Esta limitación reducirá sin duda el valor añadido que brinda la Decisión marco del Consejo, a menos que todos los Estados miembros decidan incorporar las situaciones internas en la legislación nacional de aplicación, lo cual no es probable que tenga lugar.

30. Otra razón por la que el SEPD considera que, a largo plazo, la Decisión marco 2008/977/JAI del Consejo no ofrece un marco jurídico satisfactorio para la protección de datos en un espacio de libertad, seguridad y justicia reside en que varias de sus disposiciones fundamentales no están en consonancia con la Directiva 95/46/CE. Según los tratados vigentes, podría darse un segundo paso ampliando el ámbito de aplicación de la decisión marco del Consejo y adaptándola a la Directiva 95/46/CE.

31. Otro impulso a la puesta en práctica de un régimen único para la protección de datos podría darse facilitando una visión clara y a largo plazo. Esta visión podría incluir un enfoque global y coherente para definir la recogida y el intercambio de datos, así como la explotación de las bases de datos existentes, y al mismo tiempo garantías para la protección de datos. Asimismo, esta visión debería evitar

([14]) El SEPD ha desarrollado este punto en su Dictamen del 19 de diciembre de 2005 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, apartados 30-32.

([15]) Data Protection in the European Union — Citizens' perceptions — Analytical report, Flash Eurobarometer Series 225, enero de 2008, http://www.ec.europa.eu/public_opinion/flash/fl_225_en.pdf (sólo en inglés).

([16]) Véanse también las orientaciones prioritarias de la comunicación.

([17]) COM(2006) 331 final, de 28 de junio de 2006.

([18]) Véase la nota nº 11.

un solapamiento y una duplicación inútiles de los instrumentos (y, por ende, del tratamiento de los datos personales). También debería fomentarse la coherencia de las políticas de la UE en este ámbito, así como la confianza en la forma que las autoridades públicas tratan los datos de los ciudadanos. El SEPD recomienda al Consejo que señale la necesidad de disponer de una visión clara y a largo plazo en el programa de Estocolmo.

32. El SEPD recomienda también que se evalúen y se pongan en la perspectiva adecuada las medidas ya adoptadas en este ámbito, así como su aplicación concreta y su eficacia. Esta evaluación debería tener en cuenta debidamente los costes de la intimidad y la eficacia de la aplicación de la ley. En caso de que la evaluación muestre que algunas medidas no producen los resultados previstos o no guardan proporción con los objetivos buscados, deberían tomarse en consideración las siguientes medidas:

— en primer lugar, modificar o derogar las medidas cuando no parezcan estar suficientemente justificadas para generar un valor añadido concreto para las autoridades encargadas de la aplicación de la ley y para los ciudadanos europeos,

— en segundo lugar, estudiar las posibilidades de mejorar la aplicación de las medidas existentes,

— sólo en tercer lugar, proponer nuevas medidas legislativas cuando sea probable su necesidad para alcanzar los objetivos buscados. Sólo deberían adoptarse nuevos instrumentos cuando ofrezcan un valor añadido claro y concreto para las autoridades encargadas de la aplicación de la ley y para los ciudadanos europeos.

El SEPD recomienda que en el programa de Estocolmo se haga referencia a un sistema de evaluación de las medidas existentes.

33. Por último aunque ello no sea menos importante, debe insistirse especialmente en que se apliquen mejor las garantías existentes, en consonancia con la comunicación de la Comisión sobre el seguimiento del programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos ([19]) y las sugerencias formuladas por el SEPD en su dictamen sobre dicha comunicación ([20]). Por desgracia, en el tercer pilar la Comisión no tiene la posibilidad de incoar procedimientos de infracción.

El Tratado de Lisboa

34. El Tratado de Lisboa abre la vía a un auténtico marco único para la protección de datos. El artículo 16.2 del Tratado sobre el funcionamiento de la Unión Europea obliga al Consejo y al Parlamento Europeo a establecer las normas sobre protección de datos por las instituciones, órganos y organismos de la Unión, por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y por los particulares.

35. El SEPD comprende el énfasis que pone la comunicación en un régimen único de protección de datos que refleja la ambición de la Comisión de proponer un marco jurídico que se aplique a todas las actividades de tratamiento de datos. El SEPD comparte plenamente esta ambición, que incrementa la coherencia del sistema, garantiza la seguridad jurídica y, de este modo, mejora la protección. En particular, con ello se evitarían en el futuro las dificultades de trazar una línea divisoria entre los diferentes pilares cuando los datos recogidos en el sector privado con fines comerciales son utilizados posteriormente a efectos de la aplicación de la ley. Esta línea divisoria entre los diferentes pilares no refleja totalmente la realidad, tal como lo demuestran las importantes sentencias del Tribunal de Justicia en relación con el registro de nombres de los pasajeros (PNR) ([21]) y la conservación de datos ([22]).

36. El SEPD propone que en el programa de Estocolmo se ponga de relieve esta motivación de un régimen único de protección de datos. Resulta patente que dicho régimen no es sólo una simple preferencia, sino también una necesidad, debido a los cambios que se observan en las prácticas de utilización de datos. El SEPD recomienda que en el programa de Estocolmo se incluya de forma prioritaria la necesidad de disponer de un nuevo marco legislativo, entre otras cosas sustituyendo la Decisión marco 2008/977/JAI del Consejo.

37. El SEPD pone de relieve que la noción de un régimen único de protección de datos basado en un marco jurídico general no excluye que se adopten normas adicionales de protección de datos para la policía y el sector judicial. En estas normas adicionales podrían tenerse en cuenta las necesidades concretas en el ámbito de la aplicación de la ley, tal como se prevé en la declaración 21, aneja al Tratado de Lisboa ([23]).

V.2. **Reafirmación de los principios de la protección de datos**

38. En la comunicación de la Comisión se señalan los cambios tecnológicos que están transformando la comunicación entre las personas y las organizaciones públicas y privadas. Según la Comisión, ello exige reafirmar una serie de principios básicos de la protección de datos.

([19]) COM(2007) 87 final, de 7 de marzo de 2007.

([20]) Dictamen del 25 de julio de 2007, DO C 255 de 27.10.2007, p. 1, especialmente el punto 30.

([21]) Sentencia del Tribunal de Justicia de 30 de mayo de 2006, Parlamento Europeo contra Consejo de la Unión Europea (C-317/04) y Comisión de las Comunidades Europeas (C-318/04), asuntos acumulados C-317/04 y C-318/04, Rec. 2006, página I-4721.

([22]) Sentencia del Tribunal de 10 de febrero de 2009, Irlanda contra Parlamento Europeo y Consejo de la Unión Europea, Asunto C-301/06, pendiente de publicación.

([23]) Véase la declaración 21 relativa a la protección de datos de carácter personal en el ámbito de la cooperación judicial en materia penal y de la cooperación policial, aneja al Acta Final de la Conferencia intergubernamental que ha adoptado el Tratado de Lisboa, DO C 115, 9.5.2008, p. 345.

39. El SEPD acoge favorablemente los propósitos de la comunicación. Es sumamente útil hacer una evaluación de la eficacia de dichos principios desde el punto de vista de los cambios tecnológicos. En primer lugar, es importante señalar que la reafirmación de los principios de la protección de datos no siempre debe estar directamente relacionada con la evolución tecnológica. También podría ser necesaria a la luz de otras perspectivas, mencionadas en la parte III *supra*, como la internacionalización, la creciente utilización de datos a efectos de aplicación de la ley y la libre circulación.

40. Por otra parte, el SEPD considera que esta evaluación puede formar parte de la consulta pública anunciada por la Comisión en la Conferencia «Personal data — more use, more protection?» que se celebró los días 19 y 20 de mayo de 2009. Esta consulta pública podría constituir una valiosa aportación ([24]). El SEPD sugiere que se ponga de relieve la vinculación entre los propósitos enunciados en el apartado 2.3 de la comunicación y la consulta pública sobre el futuro de la protección de datos, tanto por parte del Consejo en el texto del programa de Estocolmo como por parte de la Comisión en sus declaraciones públicas sobre la consulta.

41. Los siguientes puntos sirven para ilustrar lo que podría cubrir dicha evaluación:

— los datos personales en el espacio de libertad, seguridad y justicia tienen probablemente un carácter especialmente sensible, tal como ocurre con los datos relativos a las condenas penales, los datos policiales y los datos biométricos, como impresiones dactilares y perfiles de ADN,

— su tratamiento puede tener consecuencias negativas para las personas a las que se refieran los datos, especialmente si se tienen en cuenta los poderes coercitivos de las autoridades encargadas de la aplicación de la ley. Además, el control y análisis de los datos cada están más automatizados, y muy a menudo se realizan sin intervención humana. La tecnología permite utilizar bases de datos con datos personales para efectuar búsquedas generales (extracción de datos, realización de perfiles, etc.). Deberían establecerse claramente las obligaciones jurídicas en las que basa el tratamiento de datos,

— un aspecto fundamental de la legislación relativa a la protección de datos reside en que los datos personales deben recogerse para un fin determinado y no ser utilizados de un modo incompatible con ese fin. La utilización para un fin incompatible sólo deberá permitirse cuando la ley así lo determine y sea necesaria por intereses públicos específicos, como los que se enuncian en el artículo 8.2 del Convenio Europeo de Derechos Humanos,

— la necesidad de respetar el principio de limitación de la finalidad podría tener consecuencias para las tendencias actuales en la utilización de los datos. Las autoridades encargadas de la aplicación de la ley utilizan datos que fueron recogidos por empresas privadas con fines comerciales, en las telecomunicaciones, el transporte y los servicios financieros. Además, se han establecido sistemas de información de gran escala, por ejemplo en los ámbitos de la inmigración y del control de las fronteras. Asimismo, se permiten interconexiones y accesos a bases de datos, ampliándose así los fines para los que se habían recogido inicialmente los datos personales. Es necesario reflexionar sobre estas tendencias actuales, sin dejar de lado posibles ajustes o garantías complementarias, si procede,

— además de los principios en materia de protección de datos que se mencionan en la comunicación, en la evaluación debería prestarse atención a la necesidad de transparencia del tratamiento, permitiendo a la persona a que se refieran los datos ejercer sus derechos. La transparencia es una cuestión especialmente dificultosa en el ámbito de la aplicación de la ley, en particular debido a que debería ponderarse en relación con los riesgos que se deriven para las investigaciones,

— deberían hallarse soluciones para los intercambios con terceros países.

42. La evaluación debería centrarse además en la posibilidad de hacer más eficaces los principios de aplicación de la protección de datos. En este contexto, podría ser útil centrarse en instrumentos que puedan reforzar las responsabilidades de las personas que controlan los datos. Estos instrumentos deben permitir determinar la plena responsabilidad de dichas personas en lo que se refiere a la gestión de los datos. En este contexto, resulta útil la noción de «gobernanza de los datos». Esta noción abarca todos los medios jurídicos, técnicos y organizativos con los que las organizaciones garantizan la plena responsabilidad del modo en que se manejan los datos, como la planificación y el control, la utilización de la tecnología correcta, la formación adecuada del personal, las auditorías de conformidad, etc.

V.3. **Tecnologías respetuosas de la intimidad**

43. El SEPD se congratula de que en el apartado 2.3 de la comunicación se mencione la certificación relativa a la privacidad. Además de esto, podría hacerse referencia a la «privacidad desde el diseño» y a la necesidad de determinar las «mejores técnicas disponibles» que respeten el marco de la UE para la protección de datos.

44. En opinión del SEPD, «la privacidad desde el diseño» y las tecnologías respetuosas de la intimidad podría ser instrumentos útiles para lograr una mayor protección, así como una utilización más eficaz de la información. El SEPD sugiere dos vías que no se excluyen entre sí:

— un régimen de certificación para la intimidad y la protección de datos ([25]) como opción para los fabricantes y usuarios de sistemas de información, con o sin el apoyo de la financiación o la legislación de la UE,

([24]) El Grupo del artículo 29 para la protección de datos, en el que participa el SEPD, ha decidido intensificar sus trabajos sobre su contribución a dicha consulta pública.

([25]) un ejemplo de dicho régimen lo constituye el distintivo europeo de protección de la intimidad (EuroPriSe).

— una obligación jurídica, para los fabricantes y usuarios de sistemas de información, de utilizar sistemas acordes con el principio de la privacidad desde el diseño. Ello podría requerir una ampliación del actual ámbito de aplicación de la legislación sobre protección de datos con el fin de que los fabricantes se responsabilicen de los sistemas de información que desarrollen ([26]).

El SEPD sugiere que en el programa de Estocolmo se mencionan estas posibles vías.

V.4. **Aspectos externos**

45. Otro aspecto mencionado en la comunicación es la elaboración y promoción de normas internacionales para la protección de datos. Actualmente se está desarrollando numerosas actividades con miras a establecer normas viables de aplicación a escala mundial, por ejemplo por parte de los comisarios de la Conferencia Internacional de protección de la vida privada y los datos personales. En un próximo futuro, ello podría conducir a un acuerdo internacional. El SEPD sugiere que el programa de Estocolmo apoye dichas actividades.

46. En la comunicación se menciona también la celebración de acuerdos bilaterales, partiendo de los progresos ya realizados, con los Estados Unidos. El SEPD comparte la idea de que es necesario un marco jurídico claro para la transferencia de datos a terceros países y se congratula por consiguiente de la labor conjunta realizada por las autoridades de la UE y EE.UU. en el Grupo de Contacto de Alto Nivel sobre un instrumento transatlántico de protección de datos, a la vez que pide que haya más claridad y se preste más atención a determinadas cuestiones ([27]). Desde esta perspectiva, resulta también interesante tener en cuenta las ideas recogidas en el informe sobre Asuntos de Interior en relación con un espacio euroatlántico de cooperación en el ámbito de la libertad, la seguridad y la justicia, sobre las cuales, según dicho informe, la UE debería tomar una decisión de aquí a 2014. Dicho espacio no sería posible si no se ofrecieran las garantías adecuadas en materia de la protección de datos.

47. El SEPD considera que las normas europeas de protección de datos, que se basan en el Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal ([28]) y en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas y del Tribunal Europeo de Derechos Humanos, deberían determinar el nivel de protección en un acuerdo general con los Estados Unidos sobre protección e intercambio de datos. Este acuerdo general podría basarse en acuerdos específicos de intercambio de datos personales. Ello resulta aún más importante si se tiene en cuenta la intención formulada en el apartado 4.2.1 de la comunicación, según la cual la Unión Europea debe celebrar acuerdos de cooperación policial cuando sea necesario.

48. El SEPD comprende plenamente que es necesario mejorar la cooperación internacional, en algunos casos también con países que no protegen los derechos fundamentales. No obstante ([29]), es fundamental tener en cuenta que esta cooperación internacional puede generar un gran incremento en la recogida y la transferencia internacional de datos. Por consiguiente, resulta indispensable que los principios de tratamiento equitativo y legítimo (así como las garantías procesales en su conjunto) se apliquen a la recogida y transferencia de datos personales más allá de las fronteras de la Unión, y que sólo se transmitan datos personales a terceros países u organizaciones internacionales si esas terceras partes implicadas garantizan un nivel adecuado de protección u ofrecen otras garantías adecuadas.

49. Por último, el SEPD recomienda que en el programa de Estocolmo se insista en la importancia que tienen los acuerdos generales con los Estados Unidos y otros terceros países sobre la protección y el intercambio de datos, basados en el nivel de protección que se garantiza dentro del territorio de la UE. Desde una perspectiva más amplia, el SEPD señala la importancia que tiene fomentar activamente el respeto de los derechos fundamentales, y en particular de la protección de datos, en relación con terceros países y organizaciones internacionales ([30]). Además, en el programa de Estocolmo podría mencionarse el principio general de que el intercambio de datos personales con terceros países requiere un nivel adecuado de protección u otras garantías adecuadas en los terceros países en cuestión.

VI. **LA UTILIZACIÓN DE LA INFORMACIÓN**

VI.1. **Hacia un modelo europeo de información**

50. Un mejor intercambio de la información constituye un objetivo político esencial de la Unión Europea en el espacio de libertad, seguridad y justicia. En el apartado 4.1.2 de la comunicación se pone de relieve que la seguridad de la Unión se basa en potentes mecanismos de intercambio de información entre las autoridades nacionales y los agentes europeos. Este énfasis en el intercambio de información es lógico si se tiene en cuenta la ausencia de una fuerza policial europea, un sistema judicial europeo en el ámbito penal y de un control europeo de las fronteras. Las medidas relativas a la información son, por tanto, una contribución fundamental de la Unión Europea que permite a las autoridades de los Estados miembros abordar la delincuencia

([26]) Los usuarios de la información están cubiertos por la legislación sobre la protección de datos, al igual que las personas que controlan o tratan los datos.

([27]) Véase el dictamen del Supervisor Europeo de Protección de Datos, de 11 de noviembre de 2008, acerca del informe final del Grupo de Contacto de Alto Nivel entre la UE y Estados Unidos sobre el intercambio de información y la protección de la vida privada y los datos personales, DO C 128 de 6.6.2009, p. 1.

([28]) Serie Tratados Europeos (STE) nº 108 de 28.1.1981.

([29]) Véase la carta del SEPD, del 28 de noviembre de 2005, relativa a la comunicación de la Comisión sobre la dimensión exterior del espacio de libertad, seguridad y justicia, disponible en el sitio web del ESDP.

([30]) La jurisprudencia reciente sobre las listas de terroristas confirma la necesidad de contar con garantías (también en las relaciones con las Naciones Unidas) para garantizar que las medidas de lucha contra el terrorismo cumplan las normas de la UE. en materia de derechos fundamentales (asuntos acumulados C-402/05 P y C-415/05 P, Kadi y Al Barakaat Foundation contra Consejo, sentencia del 3 de septiembre de 2008, pendiente de publicación.

transfronteriza de manera eficaz y proteger eficazmente las fronteras exteriores. No obstante, con ello no sólo se contribuye a la seguridad de los ciudadanos, sino también a su libertad (antes se mencionó la libre circulación de personas como una perspectiva del presente dictamen) y a la justicia.

51. Ello explica precisamente que se haya introducido en el Programa de La Haya el principio de disponibilidad. Con arreglo al mismo, la información necesaria para luchar contra la delincuencia debería cruzar las fronteras interiores de la UE sin obstáculos. La experiencia reciente ha mostrado la dificultad de plasmar este principio en medidas legislativas. La propuesta, presentada por la Comisión, de Decisión marco del Consejo sobre el intercambio de información en virtud del principio de disponibilidad, de 12 de octubre de 2005 ([31]), no fue aceptada en el Consejo. Los Estados miembros no estaban dispuestos a aceptar las consecuencias del principio de disponibilidad en toda su amplitud. En su lugar, se adoptaron instrumentos más limitados ([32]), como la Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza (Decisión «Prüm») ([33]).

52. Aunque el principio de disponibilidad estaba en el núcleo del Programa de La Haya, la Comisión parece adoptar ahora un enfoque más modesto, que pretende estimular en mayor medida el intercambio de información entre las autoridades de los Estados miembros mediante la introducción del modelo europeo de información. La Presidencia sueca de la UE piensa en el mismo sentido ([34]). La Presidencia presentará una propuesta de estrategia para el intercambio de información. El Consejo ya ha iniciado sus trabajos en torno a este ambicioso proyecto de estrategia de la UE para la gestión de la información, estrechamente vinculada con el modelo europeo de información. El SEPD observa esta evolución con gran interés e insiste en la atención que debería prestarse en estos proyectos a los aspectos de la protección de datos.

Modelo europeo de información y protección de datos

53. En primer lugar debe destacarse que el futuro del espacio de libertad, seguridad y justicia no debería estar «orientado a la tecnología», en el sentido de que las posibilidades casi ilimitadas que ofrecen las nuevas tecnologías deberían contrastarse siempre con los principios pertinentes de la protección de datos y aprovecharse únicamente en la medida en que cumplan dichos principios.

54. El SEPD observa que en la comunicación se presenta el modelo de información no sólo como un modelo técnico, a saber, con una gran capacidad de análisis estratégico y una mejor recogida y tratamiento de la información operativa. También reconoce que deberían tomarse en cuenta los aspectos relacionados con la política correspondiente, como los criterios para recoger, compartir y tratar la información, sin dejar de cumplir los principios de la protección de datos.

55. La tecnología de la información y las condiciones jurídicas son, y seguirán siendo, fundamentales. El SEPD celebra que en la comunicación se parta del supuesto de que un modelo europeo de información no puede interpretarse sobre la base de consideraciones técnicas. Es fundamental que la información sea recogida, compartida y tratada únicamente sobre la base de necesidades concretas en materia de seguridad y teniendo en cuenta los principios de la protección de datos. El SEPD está también totalmente de acuerdo en que es preciso definir un mecanismo de seguimiento para evaluar cómo se lleva a cabo el intercambio de información, y sugiere al Consejo que desarrolle estos elementos en el programa de Estocolmo.

56. En este contexto, el SEPD destaca que la protección de datos, destinada al proteger al ciudadano, no debe considerarse un obstáculo para una gestión de datos eficaz, ya que proporciona importantes instrumentos para mejorar el almacenamiento de información, el acceso a la misma y su intercambio. El derecho del titular de los datos a ser informado acerca de qué información que le afecta es objeto de tratamiento y a rectificar la información errónea puede reforzar también la exactitud de los datos en los sistemas de gestión de los mismos.

57. La legislación relativa a la protección de datos tiene fundamentalmente como consecuencia que si los datos son necesarios para una finalidad específica y legítima, podrán utilizarse dichos datos, mientras que si no son necesarios para una finalidad bien definida, los datos personales no deberían utilizarse. En el primer caso, pueden adoptarse perfectamente medidas adicionales para ofrecer las garantías adecuadas.

58. No obstante, el SEPD se muestra crítico en la medida en que la comunicación menciona la «identificación de las necesidades futuras» como parte del modelo de información, y pone de relieve que, también en el futuro, el principio de limitación de la finalidad deberá servir de orientación a la hora de construir los sistemas de información ([35]). Una garantía fundamental estriba en que los sistemas de protección de datos deben permitir al ciudadano saber de antemano con qué finalidad se recogen los datos que le afectan y que esos datos se utilizarán únicamente con esa finalidad, especialmente en el futuro. Esta garantía está consagrada incluso en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea. El principio de limitación de la finalidad permite hacer algunas excepciones (que afectan de modo particular al espacio de libertad, seguridad y justicia), pero esas excepciones no deben determinar la construcción del sistema.

([31]) COM(2005) 490 final.

([32]) Desde el punto de vista de la disponibilidad. La Decisión «Prüm» contiene disposiciones de largo alcance para la utilización de datos biométricos (ADN e impresiones dactilares).

([33]) DO L 210 de 6.8.2008, p. 1.

([34]) Véase el programa de trabajo del Gobierno sobre la UE citado en la nota 5, p. 23.

([35]) Véase también el punto 41 *supra*.

Elección de la arquitectura adecuada

59. Lo primero que debe hacerse es elegir la arquitectura adecuada para el intercambio de información. En la comunicación (apartado 4.1.3) se reconoce la importancia que tienen unas arquitecturas de información adecuadas, pero, lamentablemente, sólo en relación con la interoperatividad.

60. El SEPD destaca también que en el modelo europeo de información los requisitos de las protección de datos deberían ser parte integrante de todo desarrollo del sistema y no ser considerados únicamente como una condición necesaria para la legalidad del mismo ([36]). Debería hacerse referencia al concepto de «privacidad desde el diseño» y a la necesidad de determinar las «mejoras técnicas disponibles» ([37]), tal como se ha indicado en el punto 43 *supra*. El modelo europeo de información debería basarse en estos principios. Más concretamente, ello significa que los sistemas de información que sean concebidos con fines de seguridad pública deberían elaborarse siempre de acuerdo con el principio de «privacidad desde el diseño». El SEPD recomienda al Consejo que incluya estos elementos en el programa de Estocolmo.

Interoperatividad de los sistemas

61. El SEPD hace hincapié en que la interoperatividad no es una cuestión meramente técnica, sino que tiene también repercusiones en la protección de los ciudadanos, y en particular en la protección de los datos. Desde el punto de vista de esta última, la interoperatividad de los sistemas, si se realiza correctamente, ofrece claras ventajas en la medida en que evita la duplicación del almacenamiento. No obstante, también es obvio que hacer técnicamente viable el acceso a los datos o el intercambio de los mismos se convierte, en muchos casos, en un poderoso aliciente para acceder *de facto* a dichos datos o proceder a su intercambio. En otras palabras, la interoperatividad presenta riesgos particulares de interconexión de bases de datos que tengan diferentes finalidades ([38]) y puede afectar a la limitación estricta de la finalidad de las bases de datos.

62. En suma, el mero hecho de sea técnicamente posible intercambiar información digital entre bases de datos interoperativas o fusionar estas bases de datos no justifica que se haga una excepción respecto del principio de limitación de la finalidad. En determinados casos, la interoperatividad debería basarse en opciones políticas claras y prudentes. El SEPD sugiere que esta idea se especifique en el programa de Estocolmo.

VI.2. **Utilización de la información recogida para otros fines**

63. En la comunicación no se aborda manera explícita una de las tendencias más importantes de estos últimos años, a saber, la utilización, para fines de aplicación de la ley, de datos recogidos en el sector privado para fines comerciales. Esta tendencia no sólo afecta a los datos relativos al tráfico de comunicaciones electrónicas y a los datos de los pasajeros que vuelen a (determinados) terceros países ([39]), sino también al sector financiero. Un ejemplo de ello lo constituye la Directiva 2005/60/CE del Parlamento Europeo y del Consejo, de 26 de octubre de 2005, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo ([40]). Otro ejemplo bien conocido y muy debatido es el tratamiento por parte de la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT) ([41]) de datos personales que son requeridos para el programa de seguimiento de la financiación del terrorismo del Departamento del Tesoro de EE.UU.

64. El SEPD considera que en el programa de Estocolmo deberá prestarse especial atención a estas tendencias, que pueden considerarse excepciones al principio de limitación de la finalidad y a menudo suponen una importante intrusión en la intimidad, ya que la utilización de estos datos puede revelar muchas cosas del comportamiento de una persona. En los casos en que se propongan dichas medidas, deberá haber pruebas sólidas que avalen la necesidad de recurrir a medidas de ese tipo. Cuando se den esas pruebas, deberá garantizarse la plena protección de los derechos de los individuos.

65. En opinión del SEPD, la utilización, a efectos de la aplicación de de la ley, de datos personales recogidos con fines comerciales sólo debería permitirse bajo condiciones estrictas, como las siguientes:

— los datos sólo se utilizarán para fines definidos de manera específica, como la lucha contra el terrorismo o la delincuencia grave, que deberán determinarse teniendo en cuenta cada caso particular,

— los datos se transferirán mediante un sistema de exportación («push») y no de extracción («pull») ([42]),

([36]) Véanse las «Guidelines and criteria for the development, implementation and use of Privacy Enhancing Security Technologies», elaboradas en el marco del proyecto PRISE (http://www.prise.oeaw.ac.at).

([37]) Las mejores técnicas disponibles representan la fase más efectiva y avanzada en el desarrollo de actividades y sus métodos operativos, que indican la adecuación práctica de técnicas particulares para facilitar, en principio, las bases para que las aplicaciones y sistemas ITS cumplan el requisito de intimidad, protección de datos y seguridad del marco regulador de la UE.

([38]) Véanse las observaciones del SEPD sobre la Comunicación de la Comisión relativa a la interoperabilidad de las bases de datos europeas, de 10 de marzo de 2006, disponibles en http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf

([39]) Véase, por ejemplo, el punto 15 *supra*.

([40]) DO L 309 de 25.11.2005, p. 15.

([41]) Véase el dictamen 10/2006 sobre el tratamiento de datos personales por parte de la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (Worldwide Interbank Financial Telecommunication — SWIFT), del Grupo de Trabajo del Artículo 29.

([42]) Con arreglo al sistema «push», la persona encargada de controlar los datos envía («pushes») al organismo encargado de la aplicación de la ley los datos que hayan sido previamente solicitados. Con arreglo al sistema «pull», el organismo encargado de la aplicación de la ley tiene acceso a la base de datos de la persona encargada de controlar los datos y extrae («pulls») información de dicha base de datos. Según el sistema «pulls», la persona encargada del control tendrá más dificultades para volver a asumir su responsabilidad.

— las solicitudes de datos deberán ser proporcionadas, tener una finalidad bien precisa y, en principio, basarse en sospechas relativas a personas concretas,

— deberían evitarse las consultas rutinarias, la extracción de datos y la realización de perfiles,

— toda utilización de datos a efectos de la aplicación de la ley debería quedar registrada para permitir al titular de los datos en el ejercicio de sus derechos, a las autoridades encargadas de la protección de datos y al poder judicial llevar a cabo un control efectivo de dicha utilización.

VI.3. **Sistemas de información y organismos de la UE**

Sistemas de información con o sin almacenamiento centralizado ([43])

66. En los últimos años, en el espacio de libertad, seguridad y justicia ha aumentado de manera significativa el número de sistemas de información que se basan en la legislación de la UE. En algunos casos se adoptan decisiones para establecer un sistema que implica un almacenamiento centralizado de datos a nivel europeo, mientras que en otros casos la ley sólo prevé el intercambio de información entre bases de datos nacionales. El Sistema de Información de Schengen es probablemente el mejor ejemplo de un sistema con almacenamiento centralizado. Desde el punto de vista de la protección de datos, la Decisión 2008/615/JAI del Consejo (Decisión «Prüm») ([44]) constituye el mejor ejemplo de un sistema sin almacenamiento centralizado, ya que prevé un intercambio masivo de datos biométricos entre las autoridades de los Estados miembros.

67. En la comunicación se ilustra la continuación en el futuro de esta tendencia a crear nuevos sistemas. Un primer ejemplo, tomado del apartado 4.2.2, lo constituye un sistema de información que amplía el Sistema de Información Europeo de Antecedentes Penales (ECRIS) para incluir a nacionales de países que no pertenecen a la UE. La Comisión ya ha encargado un estudio sobre el Índice europeo de nacionales de terceros países condenados (EICTCN), que podría dar lugar a una base de datos centralizada. Un segundo ejemplo lo ofrece el intercambio de información sobre personas que figuran en registros de insolventes en otros Estados miembros, en el marco de la justicia electrónica (apartado 3.4.1 de la comunicación) sin almacenamiento centralizado.

68. Un sistema descentralizado ofrecería algunas ventajas desde el punto de vista de la protección de datos, ya que evita la duplicación del almacenamiento de datos por la autoridad del Estado miembro y por el sistema centralizado, la responsabilidad de los datos queda clara dado que la autoridad del Estado miembro será la encargada de realizar el control, y el control por el poder judicial y las autoridades encargadas de la protección de datos puede tener lugar a nivel de los Estados miembros. No obstante, este sistema muestra también sus puntos débiles cuando se intercambian datos con otros ámbitos de competencia, por ejemplo a la hora de garantizar que la información esté actualizada en el país de origen y en el de destino, y en lo que se refiere a la manera de garantizar un control eficaz por ambas partes. Más complicado aún resulta garantizar la responsabilidad del sistema técnico para el intercambio. Estos puntos débiles pueden superarse mediante la elección de un sistema centralizado con responsabilidad para los organismos europeos, al menos para algunas partes del sistema (como la infraestructura técnica).

69. En este contexto, sería útil formular criterios básicos para elegir entre sistemas centralizados y descentralizados, garantizando unas opciones políticas claras y prudentes en casos concretos. Estos criterios pueden contribuir al funcionamiento de los propios sistemas, así como a la protección de los datos de los ciudadanos. El SEPD sugiere que en el programa de Estocolmo se haga constar la intención de formular dichos criterios.

Sistemas de información de gran escala

70. En el apartado 4.2.3.2 de la comunicación se analiza brevemente el futuro de los sistemas de información de gran escala, destacándose el Sistema de Información de Schengen (SIS) y el Sistema de Información de Visados (VIS).

71. En el mismo apartado se menciona también el establecimiento de un sistema de registro electrónico de las entradas y salidas del territorio de los Estados miembros de la Unión Europea, así como de programas de viajeros registrados. Este sistema ya había sido anunciado por la Comisión como parte del paquete de medidas en materia de fronteras por iniciativa del Vicepresidente Frattini ([45]) En sus observaciones preliminares ([46]), el SEPD se mostró bastante crítico con esta propuesta debido a que no quedaba suficientemente demostrada la necesidad de establecer este intrusivo sistema por añadidura de los sistemas de gran escala existentes. El SEPD no ve ninguna otra prueba de la necesidad de dicho sistema y, por ello, sugiere al Consejo que no aluda a esta idea en el programa de Estocolmo.

72. En este contexto, el SEPD desea remitirse a sus dictámenes sobre diversas iniciativas en el ámbito del intercambio de información de la UE ([47]), en los que hizo numerosas sugerencias y observaciones sobre las implicaciones que tiene, desde al punto de vista de la protección de datos, la utilización de grandes bases de datos a escala de la UE. Entre otras cuestiones, el SEPD dedicó especial atención a la necesidad de establecer unas garantías sólidas y bien adaptadas, así como a la proporcionalidad y a la necesidad de

([43]) En el presente contexto, por almacenamiento centralizado se entiende un almacenamiento a escala europea central, mientras que almacenamiento descentralizado significa un almacenamiento a escala de los Estados miembros.

([44]) Véase la nota nº 33.

([45]) Comunicación de la Comisión «Preparación de los próximos pasos en la gestión de fronteras en la Unión Europea», de 13.2.2008, COM(2008), 69.

([46]) Observaciones preliminares del SEPD sobre tres Comunicaciones de la Comisión relativas a la gestión de fronteras [COM(2008) 69, COM(2008) 68 y COM(2008) 67], de 3 de marzo de 2008. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf

([47]) En particular, dictamen 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, DO C 181 de 23.7.2005, p. 13, y dictamen de 19 de octubre de 2005 sobre tres propuestas relativas al Sistema de Información de Schengen de segunda generación (SIS II), DO C 91 de 19.4.2006, p. 38.

realizar evaluaciones de impacto antes de proponer o emprender medidas en este ámbito. El SEPD siempre ha abogado por una legislación y una protección de datos que respeten el equilibrio entre los requisitos de seguridad y la protección de la intimidad de las personas sometidas a los sistemas. El SEPD había adoptado la misma postura cuando actuó como supervisor de las partes centrales de los sistemas.

73. Además, el SEPD aprovecha esta oportunidad para destacar la necesidad de contar con un enfoque coherente sobre el intercambio de información de la UE tomado en su conjunto, teniendo en cuenta la coherencia jurídica, técnica y en materia de supervisión entre los sistemas ya establecidos y los que se están elaborando. En efecto, hoy día, más que nunca, se percibe claramente la necesidad de tener una visión valiente y global sobre la manera en que debería configurarse el intercambio de información de la UE y el futuro de los sistemas de información de gran escala. Sólo basándose en esa visión cabría reconsiderar un sistema de registro electrónico de las entradas y salidas del territorio de los Estados miembros.

74. El SEPD sugiere que en el programa de Estocolmo se haga constar la intención de desarrollar esa visión, que debería dar cabida a una reflexión sobre la posible entrada en vigor del Tratado de Lisboa y sus implicaciones para los sistemas inspirados en una base jurídica propia del primer y el tercer pilar.

75. Por último, en la comunicación se menciona la creación de una nueva agencia, la cual, con arreglo a la misma comunicación, también debería hacerse competente en lo que se refiere al sistema de registro electrónico de entradas y salidas. Entretanto, la Comisión ha adoptado una propuesta relativa a la creación de dicha agencia ([48]). El SEPD apoya en principio esta propuesta, que podría hacer más eficaz el funcionamiento de los sistemas, incluida la protección de datos, y presentará en su momento un dictamen sobre la misma.

Europol y Eurojust

76. En varios pasajes de la comunicación se habla del cometido de Europol, destacándose como cuestión prioritaria que Europol debe desempeñar un papel central en la coordinación, el intercambio de información y la formación de profesionales. Asimismo, en el apartado 4.2.2 de la comunicación se hace referencia a los recientes cambios que se han producido en el marco jurídico de cooperación entre Eurojust y Europol y se anuncia que proseguirán los trabajos para reforzar Eurojust, especialmente en lo que se refiere a la investigación en el ámbito de la delincuencia organizada transfronteriza. El SEPD apoya plenamente estos objetivos, siempre que se respeten adecuadamente las garantías relativas a la protección de datos.

77. En este contexto, el SEPD se congratula del nuevo proyecto de acuerdo al que han llegado recientemente Europol y Eurojust ([49]), y que tiene como objetivo mejorar e intensificar la cooperación mutua entre ambos organismos e instaurar un intercambio eficaz de información entre ellos. En esta labor desempeña un papel fundamental una protección de datos eficiente y efectiva.

VI.4. **Utilización de datos biométricos**

78. El SEPD observa que en la comunicación no se aborda la cuestión de la creciente utilización de datos biométricos en diferentes instrumentos jurídicos de la Unión Europea relativos al intercambio de información, incluidos los instrumentos que establecen los sistemas de información de gran escala. Ello es de lamentar, toda vez que se trata de una cuestión especialmente importante y sensible desde el punto de vista de la protección de datos y la intimidad.

79. El SEPD, si bien reconoce las ventajas generales que ofrece la utilización de datos biométricos, siempre ha insistido en las importantes repercusiones que dicha utilización tiene sobre los derechos de los individuos y ha sugerido que se instauren garantías rigurosas para la utilización de esos datos en cada uno de los sistemas. En la reciente sentencia del Tribunal Europeo de Derechos Humanos en el asunto *S. y Marper contra el Reino Unido* ([50]) se hacen indicaciones útiles en este contexto, especialmente en lo que se refiere a la justificación y los límites de la utilización de datos biométricos. En particular, la utilización de información relativa al ADN puede revelar información sensible acerca de las personas, máxime si se tiene en cuenta que siguen aumentando las posibilidades técnicas de obtener información a partir del ADN. La utilización a gran escala de datos biométricos en los sistemas de información es también problemática debido a las inexactitudes inherentes a la recogida y comparación de dichos datos. Por estas razones, el legislador de la UE debería mostrarse cauto a la hora de utilizarlos.

80. Otra cuestión planteada repetidas veces en los últimos años ha sido la utilización de impresiones dactilares de niños y personas de edad avanzada, debido a las imperfecciones inherentes que presentan los sistemas biométricos para esos grupos de edad. El SEPD ha pedido que se lleve a cabo un estudio pormenorizado para determinar adecuadamente la exactitud de los diferentes sistemas ([51]). También ha propuesto un límite de edad de 14 años para los niños, a menos que en el citado estudio se demuestre otra cosa. El SEPD recomienda que esta cuestión se mencione en el programa de Estocolmo.

([48]) Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 24 de junio de 2009, por el que se establece una Agencia para la gestión operativa del Sistema de Información de Schengen (SIS II), el Sistema de Información de Visados, (VIS), EURODAC y otros sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia [COM(2009) 293/2].

([49]) Este proyecto de acuerdo, que fue aprobado por el Consejo, deberá aún ser firmado por ambas partes. Véase el Registro del Consejo: http://register.consilium.europa.eu/pdf/en/09/st10/st10019.en09.pdf http://register.consilium.europa.eu/pdf/en/09/st10/st10107.en09.pdf

([50]) 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.

([51]) Dictamen de 26 de marzo de 2008 sobre la propuesta de Reglamento por el que se modifica el Reglamento (CE) nº 2252/2004 del Consejo sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros, DO C 200 de 6.8.2008, p. 1.

81. Dicho esto, el SEPD piensa que sería útil elaborar criterios básicos para la utilización de datos biométricos. Estos criterios deberían garantizar que los datos sólo se utilicen cuando sean necesarios, adecuados y proporcionados y el legislador haya demostrado la existencia de una finalidad explícita, específica y legítima. Más concretamente, los datos biométricos, y en particular los relativos al DNA, no deberían utilizarse cuando se pueda alcanzar el mismo efecto utilizando otra información menos sensible.

VII. **ACCESO A LA JUSTICIA Y A LA JUSTICIA ELECTRÓNICA**

82. La tecnología también se utilizará como instrumento para lograr una mejor cooperación judicial. En el apartado 3.4.1 de la comunicación, se presenta la justicia electrónica como un medio de facilitar a los ciudadanos el acceso a la justicia. La justicia electrónica consiste en un portal que contiene información y el uso de videoconferencias como parte del procedimiento jurídico. Además, abre la vía a procedimientos jurídicos en línea y prevé la interconexión de registros nacionales, como los registros de insolvencia. El SEPD observa que en la comunicación no se alude a nuevas iniciativas en relación con la justicia electrónica, sino que en ella se consolidan las acciones ya emprendidas. El SEPD está implicado en algunas de estas acciones, a raíz del dictamen que emitió el 19 de diciembre de 2008 sobre la comunicación de la Comisión «Hacia una estrategia europea en materia de e-Justicia (Justicia en línea)» ([52]).

83. La justicia electrónica es un proyecto ambicioso que requiere el máximo apoyo. Puede mejorar de modo efectivo el sistema judicial europeo y la protección judicial del ciudadano, y representa un importante paso adelante hacia un Espacio Europeo de Justicia. Teniendo presente esta apreciación positiva, pueden hacerse algunas observaciones:

— los sistemas tecnológicos para la justicia electrónica deberían construirse con arreglo al principio de «privacidad desde el diseño» . Como ya se afirmó anteriormente, en relación con el modelo europeo de información, lo primero que debe hacerse es elegir la arquitectura adecuada,

— la interconexión y la interoperatividad de los sistemas deberían respetar el principio de limitación de la finalidad,

— deberían definirse con precisión las responsabilidades de las diferentes partes implicadas,

— las consecuencias para los individuos y la interconexión de los registros nacionales con datos personales sensibles, como los registros de insolvencia, deberían analizarse previamente.

VIII. **CONCLUSIONES**

84. EL SEPD comparte el énfasis que la comunicación pone en la protección de los derechos fundamentales, y en particular en la protección de los datos personales, como uno de los aspectos clave del futuro del espacio de libertad, seguridad y justicia. En opinión del SEPD, en la comunicación se fomenta con razón un equilibrio entre la necesidad de contar con instrumentos adecuados para garantizar la seguridad del ciudadano y la necesidad de proteger sus derechos fundamentales. El SEPD reconoce que debería insistirse más en la protección de los datos personales.

85. Por otra parte, el SEPD apoya plenamente el apartado 2.3 de la comunicación, donde se hace un llamamiento en favor de un régimen único de protección de datos que cubra todos los ámbitos de competencia de la UE, independientemente de la entrada en vigor del Tratado de Lisboa. En este contexto, el SEPD recomienda:

— proclamar la necesidad de que en el programa de Estocolmo se tenga una visión clara y a largo plazo de dicho régimen único,

— evaluar las medidas que se han adoptado en este ámbito, su aplicación concreta y su eficacia, teniendo en cuenta los costes que se derivan para la privacidad y la eficacia requerida para la aplicación de la ley,

— recoger de forma prioritaria en el programa de Estocolmo la necesidad de disponer de un nuevo marco legislativo, entre otras cosas sustituyendo la Decisión marco 2008/977/JAI del Consejo.

86. El SEPD se congratula de la intención de la Comisión de reafirmar los principios de la protección de datos, que debe estar conectada con la consulta pública anunciada por la Comisión en la Conferencia «Personal data — more use, more protection?», que se celebró los días 19 y 20 de mayo de 2009. Fundamentalmente, el SEPD insiste en la importancia que tiene el principio de limitación de la finalidad como piedra angular de la legislación sobre la protección de datos, así como en la importancia de centrarse en las posibilidades de hacer más eficaz la aplicación de los principios de la protección de datos, mediante instrumentos que puedan reforzar las responsabilidades de las personas encargadas de controlar los datos.

87. La «privacidad desde el diseño» y las tecnologías respetuosas de la intimidad podrían fomentarse mediante;

— un régimen de certificación para la intimidad y la protección de datos como opción para los fabricantes y usuarios de sistemas de información,

— una obligación jurídica, para los fabricantes y usuarios de sistemas de información, de utilizar sistemas que respeten el principio de la intimidad mediante el diseño.

88. Por lo que se refiere a los aspectos externos de la protección de datos, el SEPD recomienda:

— destacar en el programa de Estocolmo la importancia de los acuerdos generales con Estados Unidos y otros terceros países en materia de protección e intercambio de datos,

([52]) Dictamen del SEPD de 19 de diciembre de 2008 sobre la comunicación de la Comisión «Hacia una estrategia europea en materia de e-Justicia (Justicia en línea)», DO C 128 de 6.6.2009, p. 13.

— fomentar activamente el respeto de los derechos fundamentales, y en particular de la protección de datos, en relación con terceros países y organizaciones internacionales,

— mencionar en el programa de Estocolmo que el intercambio de datos personales con terceros países requiere un nivel adecuado de protección u otras garantías adecuadas en los terceros países en cuestión.

89. El SEPD observa con gran interés la evolución hacia una estrategia de la UE de gestión de la información y un modelo europeo de información e insiste en la atención que debe prestarse en estos proyectos a los aspectos de la protección de datos, que deberán desarrollarse en el programa de Estocolmo. La arquitectura para el intercambio de información debería basarse en la «privacidad desde el diseño» y las «mejores técnicas disponibles».

90. El mero hecho de sea técnicamente posible intercambiar información digital entre bases de datos interoperativas o fusionar estas bases de datos no justifica que se haga una excepción respecto del principio de limitación de la finalidad. En determinados casos, la interoperatividad debería basarse en opciones políticas claras y prudentes. El SEPD sugiere que esta idea se recoja en el programa de Estocolmo.

91. En opinión del SEPD, la utilización para fines de aplicación de la ley de datos personales recogidos para fines comerciales sólo debería permitirse bajo condiciones estrictas, que se especifican en el punto 65 del presente dictamen.

92. Otras sugerencias para la utilización de información personal son las siguientes:

— formular criterios básicos para elegir entre sistemas centralizados y descentralizados, haciendo constar en el programa de Estocolmo la intención de formular dichos criterios,

— no mencionar en el programa de Estocolmo el establecimiento de un sistema de registro electrónico de las entradas y salidas del territorio de los Estados miembros, junto con programas de viajeros registrados,

— apoyar el refuerzo de Europol y Eurojust y el nuevo acuerdo acordado recientemente entre ambos organismos,

— elaborar criterios básicos para la utilización de datos biométricos, garantizando que los datos sólo se utilicen cuando sean necesarios, adecuados y proporcionados y el legislador haya demostrado la existencia de una finalidad explícita, específica y legítima. Los datos relativos al ADN no deberían utilizarse cuando se pueda alcanzar el mismo efecto utilizando otra información menos sensible.

93. El SEPD apoya la justicia electrónica y ha hecho algunas observaciones sobre la manera de mejorar el proyecto (véase el punto 83).

Hecho en Bruselas, el 10 de julio de 2009.

Peter HUSTINX

Supervisor Europeo de Protección de Datos