Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo — «La Estrategia de Seguridad Interior de la UE en acción: cinco medidas para una Europa más segura»

(2011/C 101/02)

EL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS,

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

Vista la Carta de los Derechos Fundamentales de la Unión Europea y, en particular, sus artículos 7 y 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 dichos datos ([1]),

Vista la solicitud de un dictamen de conformidad con el Reglamento (CE) nº 45/2001, 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]), en particular, su artículo 41.

ADOPTA EL SIGUIENTE DICTAMEN

I. INTRODUCCIÓN

1. El 22 de noviembre de 2010, la Comisión adoptó una Comunicación bajo el título «La Estrategia de Seguridad Interior de la UE en acción: cinco medidas para una Europa más segura» (en adelante, la «Comunicación») ([3]). La Comunicación fue remitida al SEPD para su consulta.

2. El SEPD acoge con agrado la consulta transmitida por la Comisión. Ya con anterioridad a la Comunicación, el SEPD aportó comentarios no oficiosos sobre el borrador, varios de los cuales se han incorporado a la versión final de la Comunicación.

Contexto de la Comunicación

3. La Estrategia de Seguridad Interior de la UE (en adelante, ESI), abordada en la Comunicación, fue adoptada el 23 de febrero de 2010 durante la Presidencia española ([4]). La estrategia define un modelo de seguridad europeo que comprende, entre otras actuaciones, la cooperación en el ámbito judicial y policial, el fortalecimiento de la gestión en las fronteras exteriores y la protección civil, dentro del debido respeto a los valores europeos compartidos, como es el caso de los derechos fundamentales. Sus objetivos principales consisten en:

   — presentar al público los instrumentos vigentes que contribuyen ya a garantizar la seguridad y libertad de los ciudadanos dentro de la UE y el valor añadido que representa la actividad de la UE en este ámbito,

   — desarrollar nuevos instrumentos y políticas comunes a partir de un planteamiento más integrado que atienda no sólo a los efectos sino también a las causas de la inseguridad,

   — reforzar la cooperación judicial y policial, la gestión de las fronteras exteriores, la protección civil y la gestión en caso de catástrofes.

4. El objetivo que persigue la ESI es responder a las principales amenazas y desafíos que pesan sobre la seguridad de la UE, como es el caso de las formas graves de delincuencia y la delincuencia organizada, el terrorismo y la ciberdelincuencia, la gestión de las fronteras exteriores de la UE, así como potenciar la capacidad de respuesta frente a las catástrofes naturales o provocadas por el hombre. La estrategia sienta las directrices, los principios y las orientaciones que habrá de seguir la UE con el fin de hacer frente a estos problemas, y formula un llamamiento a la Comisión para que planifique un calendario de actuaciones destinadas a llevar a buen término la estrategia.

5. Por otro lado, es importante aludir en este contexto a las recientes Conclusiones adoptadas por el Consejo de Justicia e Interior los días 8 y 9 de noviembre de 2010 ([5]) (en adelante, «Conclusiones de noviembre de 2010») en relación con la creación y la ejecución un ciclo político en el marco de la UE orientado a combatir las formas graves de delincuencia y la delincuencia organizada internacional. El presente documento se atiene a la Conclusión del Consejo relativa a la Arquitectura de Seguridad Interior de 2006 ([6]), e insta al Consejo y a la Comisión a que definan una ESI global basada en los valores y principios comunes de la UE como reafirma la Carta de los Derechos Fundamentales de la Unión Europea ([7]).

([1]) DO L 281 de 23.11.1995, p. 31.
([2]) DO L 8, de 12.1.2001, p. 1.
([3]) COM(2010) 673 final.
([4]) Doc. 5842/2/10.
([5]) 3043ª reunión del Consejo de Justicia e Interior, de los días 8 a 10 de noviembre de 2010 en Bruselas.
([6]) Doc. 7039/2/06 JAI 86 CATS 34.
([7]) El ciclo de elaboración de políticas de la UE para las formas graves de delincuencia y la delincuencia organizada internacionales abordadas en las Conclusiones de noviembre de 2010 consiste en cuatro fases: 1) progresos políticos basados en la Evaluación de la Amenaza de la Delincuencia Organizada de la Unión Europea (UE SOCTA), 2) establecimiento de políticas y toma de decisiones mediante la identificación de un número determinado de prioridades por parte del Consejo, 3) aplicación y seguimiento del Plan de Acción Operativo (PAO), y 4) al concluir el ciclo de elaboración de políticas, una evaluación rigurosa que también servirá como aportación para el futuro ciclo de elaboración de políticas.

6. Entre las directrices y objetivos que habrán de impulsar la aplicación de la ESI, las Conclusiones de noviembre de 2010 señalan la necesidad de reflexionar sobre un enfoque proactivo basado en la información, la cooperación rigurosa entre los organismos de la UE, potenciando los sistemas de intercambio de información, así como al hecho de que los ciudadanos cobren conciencia de la importancia del trabajo desarrollado por la Unión en aras a su protección. Además, las Conclusiones instan a la Comisión a que elabore, conjuntamente con los expertos de los organismos y Estados miembros pertinentes, un Plan Estratégico Plurianual (en adelante, MASP) para cada prioridad, definiendo la estrategia más adecuada con el fin de hacer frente al problema. Las conclusiones instan asimismo a la Comisión a desarrollar, mediante consultas con los Estados miembros y con los expertos de los organismos de la UE, un mecanismo independiente para la evaluación de la aplicación del MASP. El SEPD volverá a analizar estos problemas en un momento posterior del presente Dictamen, debido a la estrecha vinculación que guardan o a su notable impacto sobre la protección de los datos de carácter personal, la intimidad y otros derechos y libertades fundamentales relacionados.

Contenido y objetivo de la Comunicación

7. La Comunicación propone cinco objetivos estratégicos, todos ellos relacionados con la protección de la intimidad y la protección de datos:

   — desarticular las redes de delincuencia internacional,

   — prevenir el terrorismo y combatir la radicalización y la captación de nuevos terroristas,

   — aumentar los niveles de seguridad de los ciudadanos y las empresas en el ciberespacio,

   — potenciar la seguridad a través de la gestión de las fronteras exteriores, y

   — reforzar la capacidad de resistencia de Europa frente a las crisis y las catástrofes.

8. La *ESI en Acción*, de acuerdo con los términos de la Comunicación, propone una agenda compartida para los Estados miembros, el Parlamento Europeo, la Comisión, el Consejo, organismos y otras entidades, así como por la sociedad civil y las autoridades locales, y propone el tipo de colaboración que habrán de mantener entre sí durante los próximos cuatros años con el fin de alcanzar los objetivos de la ESI.

9. La Comunicación se fundamenta en el Tratado de Lisboa y reconoce la importancia de las directrices establecidas en el Programa de Estocolmo (y su plan de actuación), que en el capítulo 4.1 subraya la necesidad de una estrategia detallada en materia de seguridad interior basada en el respeto de los derechos fundamentales, la protección internacional y el Estado de Derecho. Asimismo, a la luz del Programa de Estocolmo, desarrollar, realizar el seguimiento y aplicar la estrategia de seguridad interna debería convertirse en una de las tareas prioritarias del comité de seguridad interna (COSI) constituido en virtud del artículo 71 del Tratado de funcionamiento de la Unión Europea. Con el fin de garantizar la aplicación efectiva de la ESI, el comité deberá asumir también los aspectos relacionados con la seguridad de una gestión de fronteras integrada y, llegado el caso, la cooperación judicial en materias penales que afecten a la cooperación operativa en el ámbito de la seguridad interna. También es importante mencionar en este contexto que el Programa de Estocolmo insta a adoptar un enfoque integrado de la estrategia de seguridad interna que debe tener en cuenta la estrategia de seguridad externa, así como otras políticas de la UE, en particular, aquellas que afectan al mercado interior.

Objetivo del Dictamen

10. La Comunicación hace referencia a diversos ámbitos políticos que forman parte o que afectan al concepto de «seguridad interna», entendido en sentido amplio, dentro de la Unión Europea.

11. El presente Dictamen no tiene por objeto analizar todos los ámbitos políticos y asuntos concretos abordados por la Comunicación, sino:

   — examinar los objetivos que en relación con la estrategia de seguridad interior propone la Comunicación desde una perspectiva específica de protección de la intimidad y de los datos, y, desde este punto de vista, recalcar los vínculos necesarios con otras estrategias actualmente debatidas y adoptadas a nivel de la UE,

   — especificar una serie de nociones y conceptos en materia de protección de datos que habrán de tenerse en cuenta a la hora de diseñar, desarrollar y aplicar la estrategia de seguridad interior en la UE,

   — aportar, cuando resulte útil y apropiado, sugerencias en relación con el procedimiento idóneo que permita tomar en consideración las inquietudes suscitadas por la protección de datos a la hora de llevar a la práctica las acciones propuestas en la Comunicación.

12. El SEPD procederá a ello resaltando, en particular, los vínculos entre la estrategia de seguridad interior y la estrategia de gestión de la información y el trabajo realizado sobre el marco global de protección de datos. Además, el SEPD hará referencia a conceptos tales como: «técnicas idóneas» e «intimidad integrada en el diseño», la evaluación del impacto sobre el derecho a la intimidad y la protección de datos, así como los derechos del interesado, que guardan consecuencia directa sobre el diseño y la aplicación de la estrategia de seguridad interior. El Dictamen también comentará varios ámbitos políticos seleccionados, como la gestión integrada de las fronteras exteriores, incluido EUROSUR y el tratamiento de los datos de carácter personal por parte de FRONTEX, así como otros ámbitos como el ciberespacio y el TFTP (Programa de seguimiento de la financiación del terrorismo).

II. OBSERVACIONES GENERALES

Necesidad de aportar un enfoque más global, integrado y «estratégico» a las estrategias de la UE relacionadas con la ESI

13. En la actualidad, se están debatiendo y proponiendo en el seno de la UE diferentes estrategias que toman como base el Tratado de Lisboa y el Programa de Estocolmo y que comportan un efecto directo o indirecto sobre la protección de datos. La ESI es una de ellas y guarda estrecha relación con otras estrategias (abordadas en recientes Comunicaciones de la Comisión o previstas en un futuro próximo), como la estrategia de gestión de la información de la UE y el modelo de intercambio de información europeo, la estrategia sobre la aplicación de la Carta de los Derechos Fundamentales de la UE, así como la estrategia global relativa a la protección de los datos y la política antiterrorista de la UE. En el presente Dictamen, el SEPD presta especial atención a los vínculos con la estrategia de gestión de la información y el marco global para la protección de datos cuyo fundamento es el artículo 16 del TFEU, que cuentan con vínculos políticos más claros con la ESI desde el punto de visto de la protección de datos.

14. Todas estas estrategias constituyen un complejo «mosaico» de directrices, programas y planes de actuación políticos interrelacionados, que exigen un enfoque global e integrado dentro de la UE.

15. En términos más generales, este planteamiento de «vinculación de estrategias», tomado desde una perspectiva amplia de cara a actuaciones posteriores, mostraría que la UE posee una visión en lo que se refiere a *sus estrategias*, y que éstas y las Comunicaciones recientemente adoptadas y elaboradas en relación con las mismas guardan un vínculo estrecho, como así es en efecto, siendo el Programa de Estocolmo el punto de referencia común para todas ellas. También podría generar sinergias positivas entre las diferentes políticas relacionadas con el espacio de libertad, seguridad y justicia, que evitarían cualquier posible yuxtaposición de trabajos y actuaciones en este ámbito. Igualmente importante es la posibilidad de que el presente enfoque conduzca a aplicaciones más efectivas y coherentes de las normas de protección de datos en el contexto de todas las estrategias interrelacionadas.

16. El SEPD subraya que uno de los pilares de la ESI es la gestión eficiente de la información dentro de la Unión Europea, basada en los principios de necesidad y proporcionalidad que justifiquen la necesidad del intercambio de información.

17. Asimismo, como se mencionaba en el dictamen del SEPD sobre la Comunicación relativa a la gestión de la información ([8]), el SEPD subraya que toda nueva medida legislativa que facilite el almacenamiento e intercambio de datos personales sólo deberá proponerse si se basa en pruebas concretas de su necesidad ([9]). Este requisito jurídico deberá transformarse en un enfoque político proactivo en el momento de llevar a la práctica la ESI. La necesidad de un enfoque global de la ESI inevitablemente lleva aparejada también la necesidad de evaluar todos los instrumentos y herramientas ya vigentes en el ámbito de la seguridad interna antes de proponer otros nuevos.

18. En este contexto, el SEPD propone asimismo servirse más asiduamente de las cláusulas que establecen una evaluación periódica de los instrumentos existentes, como los incluidos en la Directiva sobre Conservación de Datos, que es objeto de evaluación en estos momentos ([10]).

La protección de datos como objetivo de la ESI

19. La Comunicación hace referencia a la protección de datos de carácter personal en el apartado «Políticas de seguridad basadas en valores compartidos», donde señala que las herramientas y actuaciones que se practiquen con el fin de llevar a la práctica la ESI deberán basarse en valores compartidos, incluido el Estado de Derecho y el respeto a los derechos fundamentales, tal como establece la Carta de los Derechos Fundamentales de la UE. En este contexto, estipula que «Aunque el intercambio de información contribuye a aumentar la eficacia de la acción represiva en la UE, debemos también proteger la intimidad de las personas y su derecho fundamental a la protección de datos personales.»

20. Sólo puede acogerse favorablemente dicha disposición. Ahora bien, en sus términos no es posible considerar que abarque suficientemente el problema de la protección de datos en la ESI. La Comunicación tampoco analiza en profundidad los aspectos relativos a la protección de los datos ([11]), ni explica cómo se garantizarán en la práctica el derecho a la intimidad y a la protección de los datos de carácter personal en el momento de llevar a la práctica la ESI.

([8]) Dictamen de 30 de septiembre de 2010 sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo — Panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia.

([9]) Se trata de un requisito legal, véase, en particular, la sentencia del TJCE en los asuntos acumulados C-92/09 y C-93/09 del 2 de noviembre de 2010. En contextos más concretos, el SEPD también recomienda este enfoque en otros dictámenes sobre propuestas legislativas relativas al espacio de libertad, seguridad y justicia: p. ej. Dictamen de 19 de octubre de 2005 sobre tres Propuestas relativas al Sistema de Información Schengen de Segunda Generación (SIS II), el Dictamen de 20 de diciembre de 2007 sobre el borrador de Propuesta de una Decisión Marco del Consejo sobre Utilización de Datos del Registro de Nombres de los Pasajeros (Passenger Name Record — PNR) con Fines Represivos, Dictamen de 18 de febrero de 2009 sobre la Propuesta de Reglamento relativo al establecimiento del «Eurodac» para la comparación de huellas dactilares en la aplicación efectiva del Reglamento (CE) nº [.../...] (que establece los criterios y mecanismos de determinación del Estado miembro responsable de examinar la aplicación de la protección internacional presentada ante uno de los Estados miembros por un nacional de un tercer país o apátrida), y Dictamen de 7 de octubre de 2009 sobre las propuestas relativas al acceso de las fuerzas de seguridad a EURODAC.

([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).

([11]) La protección de datos solo se menciona de forma más específica en el contexto del problema del tratamiento de los datos de carácter personal por parte del FRONTEX.

21. En opinión del SEPD, entre los objetivos de *la ESI en Acción* debería figurar la *protección* entendida en un sentido amplio, que garantice, por un lado, el *correcto* equilibrio entre la protección de los ciudadanos frente a las amenazas existentes, y, por otro, la protección de sus derechos a la intimidad y a la protección de los datos de carácter personal. En otras palabras, la seguridad y la intimidad deben merecer idéntica consideración a la hora de llevar a la práctica la ESI conforme a lo establecido en el Programa de Estocolmo y las Conclusiones del Consejo.

22. En pocas palabras, brindar seguridad a la vez que se respetan íntegramente el derecho a la intimidad y a la protección de los datos debería mencionarse como objetivo específico de la Estrategia de Seguridad Interna de la UE. Dicha circunstancia debería reflejarse en todas las actuaciones practicadas por los Estados miembros y por las instituciones de la UE con el fin de aplicar en la práctica la estrategia.

23. En este contexto, el SEPD hace alusión a la Comunicación (2010) 609 relativa a un enfoque global de la protección de los datos de carácter personal dentro de la Unión Europea. ([12]) El SEPD emitirá en breve un dictamen sobre esta Comunicación, pero en lo que hace aquí hincapié es en que no se puede poner en práctica una ESI eficiente sin el respaldo de un sólido programa de protección de datos que la complemente y proporcione confianza mutua y mayor eficacia.

III. NOCIONES Y CONCEPTOS APLICABLES AL DISEÑO Y LA APLICACIÓN DE LA ESI

24. Es evidente que algunas de las actuaciones que emanan de los objetivos de la ESI pueden incrementar los riesgos para el derecho a la intimidad de los individuos y para el derecho a la protección de datos personales. Para contrarrestar dichos riesgos, el SEPD quiere llamar la atención respecto a conceptos tales como «Intimidad integrada en el diseño», evaluación del impacto de la protección del derecho a la intimidad y la protección de los datos, de los derechos del interesado y de las mejores técnicas disponibles (MTD). Todos estos derechos deberán tomarse en cuenta en el momento de aplicar la ESI, y pueden contribuir de manera útil a la elaboración de políticas mejor orientadas hacia la intimidad y la protección de datos en este ámbito.

Intimidad integrada en el diseño

25. El SEPD ha abogado en diversas ocasiones y en diversos dictámenes por el concepto de intimidad «*integrada*» («Intimidad integrada en el diseño» o «Intimidad por defecto»). El concepto se encuentra actualmente en fase de elaboración tanto en el sector privado como en el sector público, y por tanto, debe desempeñar un papel importante en el contexto de la seguridad interna de la UE y de la actuación policial y judicial ([13]).

26. La Comunicación no alude a este concepto. El SEPD sugiere que se haga referencia a él en las actuaciones que se propondrán y se emprenderán con el fin de llevar a la práctica la ESI, en particular, en el contexto del Objetivo 4 «Reforzar la seguridad a través de la gestión de fronteras», donde se hace una mención explícita a una mayor utilización de las nuevas tecnologías en los controles y vigilancia fronterizos.

Evaluación del impacto de la intimidad y la protección de datos

27. El SEPD alienta a la Comisión a que refleje — como parte de los futuros trabajos sobre el diseño y aplicación de la ESI basados en la Comunicación- lo que debería entenderse por una verdadera «evaluación del impacto de la intimidad y la protección de datos» en el espacio de libertad, seguridad y justicia, y, en particular en la ESI.

28. La Comunicación hace referencia a la evaluación de amenazas y riesgos. Esta mención ha de ser acogida favorablemente. Sin embargo, en ningún momento, hace referencia a la evaluación del impacto sobre el derecho a la intimidad y la protección de datos. El SEPD considera que el trabajo de aplicación de la Comunicación en la ESI ofrece una buena oportunidad para elaborar dichas evaluaciones del impacto sobre la intimidad y la protección de datos en el contexto de la seguridad interior. El SEPD observa que ni la Comunicación ni las directrices sobre evaluación de impacto de la Comisión ([14]) inciden en este aspecto ni lo transforman en un requisito político.

29. Por tanto, el SEPD recomienda que al aplicar futuros instrumentos se realice una evaluación del impacto sobre el derecho a la intimidad y la protección de datos más específica y rigurosa, ya como evaluación independiente, ya como parte de la evaluación general del impacto sobre los derechos fundamentales efectuada por la Comisión. Esta evaluación del impacto no debería limitarse únicamente a declarar los principios generales o a analizar opciones políticas, como ocurre en la actualidad, sino que también debería recomendar salvaguardas específicas y concretas.

30. Por consiguiente, deberán desarrollarse características e indicadores con el fin de velar por que toda propuesta que tenga un impacto sobre la intimidad y la protección de datos sea objeto de consideración en profundidad, incluidos aspectos tales como la proporcionalidad, la necesidad y el principio de limitación.

31. También podría ser útil, en este contexto, aludir al artículo 4 de la Recomendación RFID ([15]), en la que la Comisión instaba a los Estados miembros a garantizar que la industria, en colaboración con las partes interesadas de la sociedad civil, elaborase un marco para la evaluación del impacto sobre la protección de datos y el derecho a la intimidad. Asimismo, la Resolución de Madrid, adoptada en noviembre de 2009 por la Conferencia Internacional

([12]) Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre un enfoque global respecto a la protección de datos en la Unión Europea, COM (2010) 609.

([13]) El SEPD, en su dictamen sobre la Comunicación de la Comisión respecto al Programa de Estocolmo recomendaba que debería existir una obligación legal para los constructores y usuarios de sistemas informáticos de desarrollar y utilizar sistemas que respeten el principio de «intimidad integrada en el diseño».

([14]) SEC(2009) 92, 15.1.2009.

([15]) C(2009) 3200 final, 12.5.2009.

de Autoridades de Protección de Datos y Privacidad, promovía la realización de estudios de impacto sobre la intimidad previos a la aplicación de nuevos sistemas y tecnologías de información destinados al tratamiento de datos de carácter personal o la realización de modificaciones sustanciales en tratamientos ya existentes.

Derechos de los interesados

32. El SEPD observa que la Comunicación no se ocupa específicamente de la cuestión de los derechos de los interesados, lo cual constituye un elemento decisivo de la protección de datos y debería repercutir en el diseño de la ESI. Es esencial asegurar que, en todos los sistemas e instrumentos diferentes que afecten a la seguridad interior de la UE, los ciudadanos disfruten derechos similares en relación con el modo en que se tratan sus datos de carácter personal.

33. Muchos de los sistemas a los que se alude en la Comunicación establecen reglas específicas sobre los derechos de los interesados (dirigidas también a grupos de personas como víctimas, presuntos autores de infracciones penales o inmigrantes), pero hay grandes variaciones, no debidamente justificados, entre los diversos sistemas e instrumentos.

34. Por consiguiente, el SEPD invita a la Comisión a examinar más atentamente la cuestión de la coordinación de los derechos de los interesados dentro de la UE en el contexto de la ESI y de la Estrategia de Gestión de la Información en un futuro próximo.

35. Se deberá prestar especial atención a los mecanismos de recurso. La ESI deberá garantizar que, cuando los derechos de los interesados no sean totalmente respetados, los responsables del tratamiento de los datos brinden procedimientos de reclamación efectivos, asequibles y a los que pueda accederse fácilmente.

Mejores técnicas disponibles

36. La aplicación de la ESI se basará inevitablemente en la utilización de una infraestructura informática que servirá de apoyo a las acciones previstas en la Comunicación. Como mejores técnicas disponibles (MTD) podrán considerarse aquellas que posibilitan el correcto equilibrio entre el logro de los objetivos de la ESI y el respeto de los derechos de los individuos. En el contexto actual, el SEPD quisiera reiterar la recomendación realizada en dictámenes previos ([16]) respecto a la necesidad de que la Comisión defina y promueva en colaboración con partes interesadas del sector medidas concretas para la aplicación de las mejores técnicas disponibles. Dicha aplicación supone la fase más eficaz y avanzada de desarrollo de las actividades y de sus modalidades de explotación, que demuestran la capacidad práctica de determinadas técnicas para proporcionar los resultados previstos de manera eficiente y de conformidad con el marco de protección de la intimidad y de los datos de la UE. Este enfoque coincide plenamente con el de «intimidad integrada en el diseño», mencionado anteriormente.

37. Cuando proceda y resulte factible, se deberán elaborar documentos sobre las mejores técnicas disponibles con el fin de proporcionar directrices y mayor seguridad jurídica en la aplicación real de las medidas formuladas por la ESI. Dicha circunstancia también podría promover la armonización de tales medidas a través de los distintos Estados miembros. Por último, aunque no por ello menos importante, la definición del derecho a la intimidad y de las mejores técnicas disponibles orientadas a la seguridad facilitarán el papel de supervisión de las autoridades de protección de datos, dotándolas de referencias técnicas sobre derecho a la intimidad y protección de datos adoptadas por los responsables del tratamiento de datos.

38. El SEPD también constata la importancia de una coordinación correcta entre la ESI y las actividades ya realizadas dentro del Séptimo Programa Marco para acciones de investigación, desarrollo tecnológico y demostración, así como del Programa Marco de seguridad y defensa de las libertades. Una visión conjunta que tenga por finalidad proporcionar las mejores técnicas disponibles posibilitará la innovación del conocimiento y de las capacidades necesarias para proteger a los ciudadanos a la vez que se respetan los derechos fundamentales.

39. Por último, el SEPD destaca el papel que la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) puede desempeñar en la elaboración de las directrices y la evaluación de las capacidades de seguridad exigidas para garantizar la integridad y disponibilidad de los sistemas informáticos, así como en el fomento de estas mejores técnicas disponibles. A este respecto, el SEPD acoge favorablemente la inclusión de la Agencia desempeñando un papel protagonista en la mejora de las capacidades para hacer frente a ciberataques y a la ciberdelincuencia ([17]).

Aclaraciones sobre los actores y sus papeles

40. En este contexto, son necesarias aclaraciones adicionales respecto a los actores que forman parte o contribuyen a la arquitectura de la ESI. La Comunicación hace referencia a varios actores y partes interesadas, como la ciudadanía, el sistema judicial, los organismos de la UE, las autoridades nacionales, la policía y las empresas. Sería más conveniente

([16]) Dictamen del SEPD sobre sistemas de transporte inteligentes, de julio de 2009 y el Dictamen del SEPD respecto a la comunicación sobre identificación por radiofrecuencia (RFID) de diciembre de 2007, véase también el informe anual 2006 del SEPD página 48.

([17]) El SEPD prevé la adopción de un dictamen sobre el marco legal de ENISA, ya en diciembre de 2010.

que los papeles y competencias específicos de estos actores fueran abordados en las acciones específicas que se propongan para la aplicación de la ESI.

IV. COMENTARIOS ESPECÍFICOS SOBRE LOS ÁMBITOS POLÍTICOS RELACIONADOS CON LA ESI

Gestión integrada de fronteras (IBM)

41. La Comunicación alude al hecho de que, con el Tratado de Lisboa, la UE se encuentra mejor situada para sacar partido a las sinergias entre las políticas de gestión fronteriza en materia de personas y de bienes. En relación con la circulación de personas, menciona que «la UE puede tratar la gestión de la migración y la lucha contra la delincuencia como objetivos idénticos de la estrategia de gestión integrada de las fronteras». En el documento se interpreta la gestión fronteriza como una herramienta potencialmente poderosa para combatir las formas graves de delincuencia y la delincuencia organizada ([18]).

42. El SEPD constata asimismo que en la Comunicación se identifican tres ejes estratégicos: 1) un mayor uso de las nuevas tecnologías para los controles fronterizos (segunda generación del Sistema de Información de Schengen (SIS II), Sistema de Información de Visados (VIS), sistema de entrada/salida y programa de registro de pasajeros), 2) un mayor uso de las nuevas tecnologías de vigilancia fronteriza (Sistema Europeo de Vigilancia de Fronteras, EUROSUR) y 3) una mayor coordinación de los Estados miembros a través de FRONTEX.

43. El SEPD desea aprovechar la oportunidad que brinda el presente Dictamen para recordar las exigencias que planteó en varios dictámenes anteriores respecto a la necesidad de que se establezca una política clara de gestión fronteriza en la UE, respetando plenamente las normas de protección de datos. El SEPD considera que los trabajos actuales sobre la ESI y la Gestión de Información brindan una magnífica oportunidad para dar pasos más concretos hacia un enfoque político coherente en estos ámbitos.

44. El SEPD observa que la Comunicación no solo hace referencia a sistemas existentes a gran escala y a aquellos que deberían ponerse en marcha en un futuro próximo (como SIS, SIS II y VIS), sino también, en la misma línea, a los sistemas que la Comisión pueda proponer en el futuro, pero la decisión aún no ha sido adoptada (p.ej. el programa de viajeros registrados (RTP) y el sistema de entrada/salida). Se ha de recordar en el presente contexto que sigue siendo necesario aclarar y demostrar los objetivos y legitimidad de la introducción de estos sistemas, también a la luz de los resultados de evaluaciones de impacto específicas realizadas por la Comisión. Si no se llevara esto a cabo, cabría interpretar que la Comunicación prevé el proceso de toma de decisiones, y, por consiguiente, que no tiene en consideración el hecho de que aún no se ha adoptado la decisión final sobre si se deberían introducir el RTP y el sistema de entrada/salida en la Unión Europea.

45. El SEPD, por tanto, sugiere que en trabajos futuros sobre la aplicación de la ESI se eviten dichas previsiones. Como se mencionó con anterioridad, cualquier decisión sobre la introducción de nuevos sistemas intrusivos en la intimidad a gran escala solo debería tomarse sobre la base de una evaluación de todos los sistemas existentes, con debida atención a la necesidad y a la proporcionalidad.

EUROSUR

46. La Comunicación menciona que la Comisión presentará una propuesta legislativa para establecer el sistema EUROSUR en 2011 con el fin de contribuir a la seguridad interior y a la lucha contra la delincuencia. La Comunicación menciona asimismo que EUROSUR utilizará las nuevas tecnologías desarrolladas a través de proyectos y actividades de investigación financiados por la UE, como las imágenes obtenidas por satélite, para detectar y rastrear objetivos en la frontera marítima, p. ej. para rastrear embarcaciones que se desplazan a alta velocidad y que transportan drogas a la UE.

47. En este contexto, el SEPD observa que no está claro si la propuesta legislativa en relación con EUROSUR que la Comisión presentará en 2011 contemplará también el tratamiento de los datos de carácter personal recabados en el contexto de EUROSUR y, de ser así, en qué medida. La Comunicación de la Comisión no adopta una posición clara a este respecto. El problema es especialmente relevante si tenemos en cuenta que en la Comunicación se establecen claros vínculos entre EUROSUR y FRONTEX a nivel táctico, operativo y estratégico (véanse los comentarios que se presentan a continuación sobre FRONTEX) y exige una cooperación estrecha entre ambos organismos.

Tratamiento de datos de carácter personal por parte de FRONTEX

48. El SEPD ha emitido un dictamen sobre la revisión del Reglamento FRONTEX de 17 de mayo de 2010 ([19]), en el que invita a un debate auténtico y a una reflexión en profundidad sobre el problema asociado a la protección de datos dentro del marco que contempla el refuerzo de las tareas inherentes a FRONTEX y la atribución a este organismo de nuevas responsabilidades.

49. La Comunicación cita la necesidad de aumentar la contribución de FRONTEX al control de las fronteras exteriores conforme al Objetivo 4 *Reforzar la seguridad a través de la gestión de las fronteras exteriores*. En este contexto, la Comunicación señala que, basándose en la experiencia y en el planteamiento de enfoque conjunto de la UE en relación con la gestión de la información, la Comisión considera que FRONTEX contribuirá significativamente al desmantelamiento de organizaciones delictivas si se le autoriza a tratar y utilizar esta información con un alcance limitado

([18]) Comunicado de prensa sobre la Estrategia de Seguridad Interior de la UE en acción — cinco medidas para una Europa más Segura Memo 10/598.

([19]) Dictamen de 17 de mayo de 2010 sobre la propuesta de un Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (CE) nº 2007/2004 y se crea una Agencia Europea para la gestión de la cooperación operativa en las fronteras exteriores de los Estados miembros de la Unión Europea (FRONTEX).

y conforme a unas normas de gestión de los datos de carácter personal claramente definidas. Se trata de un nuevo enfoque que varía respecto a la propuesta de la Comisión en relación con la revisión del Reglamento FRONTEX, asunto que actualmente es objeto de debate en el Parlamento Europeo y el Consejo, que guardó silencio en relación con el tratamiento de los datos de carácter personal.

50. Contra este telón de fondo, el SEPD acoge favorablemente el hecho de que la Comunicación proporcione indicaciones sobre las circunstancias en las que dicho tratamiento pueda revelarse necesario (p.ej. análisis de riesgos, mejor rendimiento de las operaciones conjuntas o intercambio de información con Europol). Más en concreto, la Comunicación señala que actualmente la información sobre delincuentes involucrados en las redes de tráfico —competencia de FRONTEX—, ya no puede utilizarse para el análisis de riesgos o para orientar mejor futuras operaciones conjuntas. Además, los datos relevantes sobre sospechosos no llegan a las autoridades nacionales competentes o a Europol con el fin de proseguir las investigaciones.

51. Y sin embargo, el SEPD constata que en la Comunicación no se hace referencia al debate actualmente en curso sobre la revisión del marco jurídico de FRONTEX que, como se señaló anteriormente, aborda esta cuestión con el fin de proporcionar soluciones legislativas. Además, el texto de la Comunicación, que acentúa el papel que juega FRONTEX de cara al objetivo de desmantelar organizaciones delictivas, puede interpretarse como una ampliación del mandato de FRONTEX. El SEPD propone que este punto sea tenido en cuenta tanto en lo que se refiere a la revisión del Reglamento FRONTEX como a la aplicación de la ESI.

52. El SEPD también llama la atención sobre la necesidad de evitar toda yuxtaposición de tareas entre Europol y FRONTEX. En este contexto, el SEPD acoge favorablemente el hecho que, de acuerdo con la Comunicación, debe evitarse la yuxtaposición de tareas entre Europol y FRONTEX. No obstante, esta cuestión también deberá abordarse en la revisión del Reglamento FRONTEX y en las actuaciones que lleve a la práctica la ESI, que darán lugar a una cooperación estrecha entre FRONTEX y EUROPOL. Ello resulta especialmente importante a la luz de los principios de limitación de la finalidad y calidad de los datos. Este comentario también es aplicable a la futura cooperación con organismos como la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) o la Oficina Europea de Apoyo al Asilo.

Uso de datos biométricos

53. La Comunicación no aborda específicamente un fenómeno actual, el creciente incremento del uso de datos biométricos en el espacio de libertad, seguridad y justicia, incluidos los sistemas informáticos a gran escala de la UE y otras herramientas de gestión fronteriza.

54. El SEPD, por tanto, aprovecha esta oportunidad para recordar su sugerencia ([20]) en el sentido de que este asunto, altamente sensible desde el punto de visto de la protección de datos, sea tomado seriamente en consideración al aplicar la ESI, en particular, en el contexto de la gestión fronteriza.

55. El SEPD recomienda también el desarrollo de una clara y estricta política en el uso de datos biométricos en el espacio de libertad, seguridad y justicia basada en una evaluación seria y en una apreciación caso por caso de la necesidad de su utilización en el contexto de la ESI, con pleno respeto a los principios fundamentales de protección de datos como son los de proporcionalidad, necesidad y limitación de la finalidad.

Programa de Seguimiento de la Financiación del Terrorismo (TFTP)

56. La Comunicación anuncia que la Comisión elaborará en 2011 una política que permitirá a la UE extraer y analizar los datos de mensajería financiera presentes en su propio territorio. En este contexto, el SEPD hace referencia a su Dictamen de 22 de junio de 2010 sobre tratamiento y transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos, a efectos del Programa de seguimiento de la financiación del terrorismo (TFTP) ([21]). Todos los comentarios críticos en dicho Dictamen son igualmente válidos y aplicables en el contexto del trabajo previsto sobre un marco de la UE en relación con los datos de mensajería financiera. Por tanto, se deberían tener en cuenta en los debates en la materia. Deberá prestarse especial atención a la proporcionalidad en el momento de extraer y tratar cantidades ingentes de datos de personas que no sean sospechosas, así como al problema del control efectivo por parte de autoridades independientes y del sistema judicial.

Seguridad de los ciudadanos y de las empresas en el ciberespacio

57. El SEPD acoge favorablemente la importancia que asigna la Comunicación a las acciones preventivas dentro de la UE, y considera que reforzar la seguridad en las redes informáticas es esencial para el buen funcionamiento de la sociedad de la información. Asimismo, el SEPD apoya las actividades específicas orientadas a mejorar las capacidades para hacer frente a ciberataques, que articulen infraestructuras en los órganos policiales y judiciales, y que instauren asociaciones con la industria a fin de dotar de poderes a los ciudadanos y las empresas. Del mismo modo, se acoge favorablemente el papel de ENISA a la hora de facilitar muchas de las actuaciones contempladas en este objetivo.

([20]) Véase, en particular, el Dictamen del SEPD sobre la Comunicación respecto al panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia, mencionado en la nota 8 al pie de página.

([21]) Dictamen del SEPD de 22 de junio de 2010 sobre la Propuesta de una Decisión del Consejo sobre las conclusiones del Acuerdo entre la Unión Europea y los Estados Unidos de América relativo al tratamiento y la transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos, a efectos del Programa de seguimiento de la financiación del terrorismo (TFTP II).

58. Sin embargo, la *ESI en Acción* no menciona actuaciones policiales previstas en el ciberespacio, de qué manera estas actividades podrían poner en peligro derechos individuales, ni cuales serían las salvaguardas exigibles. El SEPD insta a un enfoque más ambicioso en relación con las garantías adecuadas. Convendría reforzar este enfoque a fin de proteger los derechos fundamentales de todos los individuos, incluidos aquellos que puedan verse afectados por actuaciones concebidas con el fin de contrarrestar cualquier posible actividad delictiva en este ámbito.

V. **CONCLUSIÓN Y RECOMENDACIONES**

59. El SEPD insta a vincular varias estrategias y Comunicaciones de la UE en el proceso de aplicación de la ESI. A este enfoque debería seguirle un plan de acción concreto respaldado por una evaluación real de las necesidades, cuyo resultado debería ser una política sobre la ESI de la UE global, integrada y bien estructurada.

60. La necesidad de un enfoque global respecto a la ESI conduce también de forma ineludible a la necesidad de evaluar todos los instrumentos y herramientas ya existentes en el campo de la seguridad interna antes de proponer otros nuevos. En este contexto, la inclusión de disposiciones que exijan evaluaciones regulares de la eficiencia de los instrumentos pertinentes es altamente recomendable.

61. El SEPD sugiere que al preparar el Plan Estratégico plurianual exigido por las Conclusiones del Consejo de noviembre de 2010, se tenga en consideración el trabajo en curso sobre el marco global de protección de datos basado en el artículo 16 del TFUE, en particular, la Comunicación (2009) 609.

62. El SEPD formula varias sugerencias sobre las nociones y conceptos relevantes desde la perspectiva de la protección de datos que deberán tenerse en cuenta en el ámbito de la ESI, como la Intimidad integrada en el diseño, la evaluación del impacto sobre la protección del derecho a la intimidad y la protección de datos, mejores técnicas disponibles.

63. El SEPD recomienda que al aplicar futuros instrumentos se realice una evaluación del impacto sobre la intimidad y la protección de datos, bien como evaluación por separado o como parte de la evaluación general del impacto sobre los derechos fundamentales efectuada por la Comisión.

64. El SEPD también invita a la Comisión a desarrollar una política más coherente y exhaustiva sobre los requisitos previos de los datos biométricos en el ámbito de la ESI, así como a una mayor coordinación respecto a los derechos de los interesados dentro de la UE.

65. Por último, el SEPD realiza varios comentarios sobre el tratamiento de los datos de carácter personal en el contexto de la gestión fronteriza y, en particular, por parte de FRONTEX, y posiblemente en el contexto de EUROSUR.

Hecho en Bruselas, el 17 de diciembre de 2010.

Peter HUSTINX

Supervisor Europeo de Protección de Datos