DICTÁMENES

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión al Consejo y al Parlamento Europeo — «La política antiterrorista de la UE: logros principales y retos futuros»

(2011/C 56/02)

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 estos datos [1],

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 [2] y, en particular, su artículo 41,

HA ADOPTADO EL SIGUIENTE DICTAMEN:

I. INTRODUCCIÓN

1. El 20 de julio de 2010, la Comisión aprobó una Comunicación titulada «La política antiterrorista de la UE: logros principales y retos futuros» [3]. La Comunicación pretende recoger «los elementos básicos para una evaluación política de la actual estrategia antiterrorista de la UE», y constituye asimismo un componente de la Estrategia de Seguridad Interior [4]. En la Comunicación se evalúan logros del pasado y se exponen los retos futuros y las líneas de actuación en materia de política antiterrorista de la UE.

2. Muchas de las iniciativas mencionadas en la Comunicación han sido objeto ya de dictámenes o comentarios específicos del SEPD. No obstante, la presente Comunicación contempla una perspectiva política y unas formulaciones a largo plazo que, por su amplitud, justifican un dictamen específico del SEPD.

3. En este sentido, el presente dictamen aspira a dotar de un mayor fundamento a las opciones políticas, en un ámbito en el que la utilización de información personal se caracteriza por ser a la vez masiva, esencial y especialmente sensible.

4. El presente dictamen se abstiene de comentar la Comunicación más reciente de la Comisión en la materia, titulada «La Estrategia de Seguridad Interior de la UE en acción: cinco medidas para una Europa más segura», aprobada el 22 de noviembre de 2010 [5]. Ésta será analizada por el SEPD en un dictamen aparte, en el que volverá a abordarse también la necesidad de establecer vínculos claros entre los distintos documentos.

5. En el presente dictamen, el SEPD analiza los diferentes elementos de la Comunicación, a la vez que se aportan diversos consejos y recomendaciones encaminados a garantizar la salvaguarda del derecho fundamental a la protección de los datos personales en el área de la política antiterrorista de la UE, sobre todo en el momento de abordar los retos futuros y desarrollar nuevas orientaciones políticas.

II. ANÁLISIS DE LA COMUNICACIÓN Y CUESTIONES RELEVANTES EN MATERIA DE PROTECCIÓN DE DATOS

6. En la Comunicación se analizan en primer lugar, inspirándose al efecto en la estructura de la estrategia antiterrorista de la UE correspondiente a 2005 [6], los cuatro ejes fundamentales de la política antiterrorista de la Unión: prevenir, proteger, perseguir y responder. A continuación, y en un capítulo específico, se abordan ciertas cuestiones horizontales, a saber, el respeto de los derechos fundamentales, la cooperación internacional y la financiación.

[1] DO L 281 de 23.11.1995, p. 31.
[2] DO L 8 de 12.1.2001, p. 1.
[3] COM(2010) 386 final.
[4] Véase la página 2 de la Comunicación.
[5] COM(2010) 673 final.
[6] Doc. 14469/4/05 de 30 de noviembre de 2005.

1. **Prevenir, proteger, perseguir, responder y la necesidad de incorporar los principios de la protección de datos**

7. «Prevención» comprende un amplio abanico de actuación, que va desde la lucha contra la radicalización y la captación, hasta cómo hacer frente al modo empleado por los terroristas para servirse de Internet. En este contexto, en la Comunicación se incluyen entre los principales logros en esta materia la Decisión Marco del Consejo relativa a la lucha contra el terrorismo, adoptada en 2002 ([1]) , y modificada en 2008 ([2]).

8. «Proteger» a las personas y a las infraestructuras constituye asimismo un concepto muy ámplio, que incluye las iniciativas en materia de seguridad en las fronteras, seguridad en el transporte, control de precursores de explosivos, protección de infraestructuras críticas y refuerzo de la cadena de suministro.

9. «Perseguir» comprende la recogida de información, la cooperación policial y judicial y la lucha contra las actividades terroristas y su financiación. Entre los futuros retos en este ámbito figuran el establecimiento de un marco para el registro de nombres de pasajeros (PNR) a nivel de la UE ([3]), la utilización del artículo 75 del TFUE con el fin de desarrollar un marco para el bloqueo de fondos y activos financieros, y el reconocimiento mutuo a la hora de obtener pruebas en asuntos penales.

10. «Responder» se refiere a la capacidad para hacer frente a las consecuencias de los atentados terroristas, incluida la asistencia a las víctimas de este tipo de acciones.

11. Todos estos ámbitos presentan estrechos vínculos con distintas iniciativas sobre las que el SEPD ya se ha posicionado: el programa de Estocolmo, medidas restrictivas y de bloqueo de activos, conservación de datos, escáneres de seguridad, precursores de armas, biometría, la Decisión de Prüm, los Registros de Nombres de los Pasajeros, el acuerdo sobre el TFTP, el Sistema de Información de Schengen, el Sistema de Información de Visados, la gestión integrada de las fronteras, la Estrategia de Gestión de la Información de la UE y el intercambio transfronterizo de pruebas.

12. Las áreas de «prevención» y «protección» son las más delicadas desde el punto de vista de la protección de datos, por diferentes motivos.

13. En primer lugar, tales ámbitos se basan, por definición, en evaluaciones de riesgos prospectivas, lo que, en la mayoría de los casos, genera un tratamiento a gran escala y «preventivo» de vastos volúmenes de información personal sobre ciudadanos que no son sospechosos (como es el caso, por ejemplo, de los los sistemas de detección en Internet, las fronteras electrónicas y los escáneres de seguridad).

14. En segundo lugar, en la Comunicación se prevén relaciones más estrechas entre los cuerpos de seguridad del Estado y las empresas privadas (como los proveedores de Internet, las instituciones financieras y las empresas de transporte) con el fin de procurar el intercambio de información relevante y, en ocasiones, «delegar» en ellas cierta parte de las tareas asociadas al cumplimiento de la ley. Esto supone un mayor uso de datos personales, recabados por empresas privadas con fines mercantiles, en actividades orientadas a velar por el cumplimiento de la ley por parte las autoridades públicas.

15. Muchas de estas iniciativas fueron adoptadas con frecuencia como respuesta inmediata a incidentes terroristas, sin analizar en profundidad posibles duplicaciones o yuxtaposiciones con medidas ya en vigor. En algunos casos, incluso después de de varios años desde su entrada en vigor, sigue sin determinarse si la invasión de la privacidad de los ciudadanos resultante de tales medidas era realmente necesaria en todos los casos.

16. Por otra parte, es muy probable que el uso «preventivo» de datos personales genere discriminación. El análisis preventivo de la información implica por lo general la recogida y el tratamiento de datos personales relativos a amplias categorías de individuos (por ejemplo, todos los pasajeros, o todos los usuarios de Internet) sin necesidad de que exista una sospecha específica sobre ellos. El análisis de tales datos, especialmente si se combina con técnicas de minería de datos, puede abocar a que ciudadanos inocentes sean considerados sospechosos únicamente porque su perfil (edad, sexo, religión, etc.) o pautas de comportamiento (p. ej., sus desplazamientos, o el uso de Internet, etc.) coinciden con los de personas en la órbita del terrorismo, o sospechosos de mantener vínculos con el terrorismo. Por tanto, y especialmente en este contexto, un uso ilícito o inexacto de la información personal (en ocasiones, de naturaleza sensible), unido a los amplios poderes coercitivos de las autoridades encargadas de velar por el cumplimiento de la ley, puede llevar a la discriminación y estigmatización de personas y/o colectivos específicos.

17. Desde esta perspectiva, garantizar un elevado nivel de protección de los datos constituye igualmente una herramienta en la lucha contra el racismo, la xenofobia y la discriminación, lo que, de acuerdo con los términos utilizados en la Comunicación, «también puede contribuir a prevenir la radicalización y la captación de terroristas».

2. **Un enfoque coherente basado en el principio de necesidad**

18. Es importante observar la necesidad de garantizar la coherencia y establecimiento de vínculos claros entre todas las Comunicaciones e iniciativas emprendidas en el ámbito de Interior, y en particular, en el ámbito de la Seguridad Interna. Por ejemplo, aunque la estrategia antiterrorista de la UE está estrechamente vinculada con la Estrategia de Gestión de la Información, con la estrategia sobre la Carta de los Derechos Fundamentales y con el Modelo Europeo de Intercambio de Información, no se han abordado ni

([1]) 2002/475/JAI, (DO L 164 de 22.6.2002, p. 3).
([2]) 2008/919/JAI, (DO L 330 de 9.12.2008, p. 21).
([3]) Como anunciado también en el Plan de acción de la Comisión por el que se aplica el programa de Estocolmo, COM(2010) 171 final de 20 de abril de 2010.

explícita ni exhaustivamente las relaciones entre todos estos documentos. La aprobación, el 22 de noviembre de 2010, de la «Estrategia de Seguridad Interior de la UE en acción: cinco medidas para una Europa más segura [1]» no venía sino a subrayar esa deficiencia.

19. Por tanto, el SEPD recomienda a las instituciones de la UE que se aseguren de que las políticas e iniciativas en el terreno de Interior y la SeguridadInterna se formulen y se apliquen de manera que se garantice un enfoque coherente y la existencia de claros vínculos de interrelación, generando así sinergias apropiadas y positivas, y evitando la duplicación de trabajos y de esfuerzos.

20. El SEPD recomienda asimismo que el principio de necesidad sea tenido explícitamente en cuenta en cada propuesta que se plantee en este ámbito. A tal efecto, deberán considerarse posibles yuxtaposiciones con instrumentos preexistentes, y deberá limitarse la recogida y el intercambio de datos personales a lo estrictamente necesario para los fines que se persiguen.

21. Por ejemplo, en el caso del Acuerdo sobre el Programa de Seguimiento de la Financiación del Terrorismo (TFTP II) con los Estados Unidos, el SEPD cuestionó hasta qué punto el acuerdo era realmente necesario para obtener resultados que hubieran podido alcanzarse mediante instrumentos que hubieran supuesto una menor vulneración de la privacidad, como los ya contemplados en el marco de la UE y en el marco internacional vigente [2]. En el mismo dictamen, el SEPD cuestionó la necesidad del envío masivo de datos personales, en lugar de ajustarse en mayor medida al fin perseguido.

22. En la Comunicación se menciona como uno de los retos existentes «velar por que estos instrumentos cubran las necesidades reales (de las autoridades de orden público de los Estados miembros) asegurando al mismo tiempo el pleno respeto del derecho consagrado en las normas sobre protección de la privacidad y de los datos personales». El SEPD acoge favorablemente este reconocimiento explícito, y formula un llamamiento a las instituciones de la UE para que evalúen con detenimiento hasta qué punto los instrumentos existentes, además de los previstos, cubren las necesidades reales en materia de cumplimiento de la ley, y evitan la yuxtaposición con otras medidas y restricciones innecesarias del derecho a la privacidad. En este sentido, los instrumentos existentes deben demostrar a través de revisiones periódicas que constituyen un medio eficaz para combatir el terrorismo.

23. El SEPD ha abogado, en numerosos dictámenes y comentarios, por la necesidad de evaluar todos los instrumentos existentes en materia de intercambio de información antes de proponer otros nuevos, con un énfasis especial en el reciente dictamen sobre el «Panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia» [3]. De hecho, evaluar la eficacia de las medidas vigentes, considerando a la vez la repercusión sobre el derecho a la privacidad de las nuevas medidas previstas, son tareas cruciales, a las que debe otorgarse un papel relevante en las actuaciones de la Unión Europea en este ámbito, con arreglo al planteamiento expuesto en el Programa de Estocolmo.

24. Las yuxtaposiciones y la falta de eficacia deben dar lugar a ajustes en las opciones políticas, o incluso a la consolidación o la retirada de los sistemas de recogida y tratamiento de datos en vigor.

25. El SEPD recomienda que se preste especial atención a aquellas propuestas que den lugar a la recogida generalizada de datos personales de todos los ciudadanos, en lugar de únicamente de los datos de sospechosos. Asimismo, han de considerarse y justificarse de manera específica los casos en los que se prevea el tratamiento de datos personales con fines ajenos a aquellos por los que se recogieron en un principio, como, por ejemplo, en el caso en el que, a efectos de velar por el cumplimiento de la ley, se accede a datos personales almacenados en el sistema Eurodac.

26. La Comunicación subraya también que uno de los retos futuros consistirá en garantizar la adopción de una política eficaz de investigación en materia de seguridad, que contribuirá a alcanzar un elevado nivel de seguridad. El SEPD respalda la afirmación contenida en la Comunicación, en el sentido de que una investigación eficaz en el ámbito de la seguridad reforzará los vínculos entre los diferentes actores. En esta perspectiva, es primordial que los conocimientos técnicos especializados en materia de protección de datos se incorporen a la investigación sobre seguridad en una fase muy temprana, con el fin de guiar las opciones políticas elegidas, y de garantizar que el respeto de la privacidad se incorpore en la mayor medida de lo posible a las nuevas tecnologías orientadas a la seguridad, de conformidad con el principio de «privacy by design».

3. **Con respecto al uso de medidas restrictivas (bloqueo de activos)**

27. Por lo que se refiere al uso de medidas restrictivas (bloqueo de activos) en relación con determinados países y presuntos terroristas, la jurisprudencia del Tribunal de Justicia ha confirmado reiterada y coherentemente que el respeto de los derechos fundamentales en la lucha contra el terrorismo es esencial, con vistas a garantizar tanto la salvaguarda de los derechos de los ciudadanos, como la legalidad de las medidas adoptadas.

28. El SEPD ha aportado ya diversos dictámenes y comentarios en este ámbito [4]; por un lado, subrayando las mejoras registradas en los procedimientos, pero, por el otro, solicitando nuevos avances, especialmente en lo que se refiere al derecho a la información y el acceso a los datos personales,

[1] Véase el apartado 4 del presente dictamen.
[2] Dictamen del SEPD de 22 de junio de 2010.
[3] Dictamen del SEPD de 30 de septiembre de 2010.

[4] Dictamen de 28 de julio de 2009 sobre la propuesta de Reglamento del Consejo por el que se modifica el Reglamento (CE) nº 881/2002 por el que se imponen determinadas medidas restrictivas específicas dirigidas contra determinadas personas y entidades asociadas con Usamah bin Ladin, la red Al-Qaida y los talibanes, (DO C 276 de 17.11.2009, p. 1). Dictamen del 16 de diciembre de 2009 relativo a varias propuestas legislativas que imponen determinadas medidas restrictivas específicas respecto de Somalia, Zimbabue, la República Democrática de Corea y Guinea, (DO C 73 de 23.3.2010, p. 1). Véase asimismo la carta del SEPD de 20 de julio de 2010 sobre tres propuestas legislativas relativas a ciertas medidas restrictivas, en concreto, respecto al Sr. Milosevic y las personas asociadas a él, en apoyo al mandato del Tribunal Internacional para la ex Yugoslavia, y en relación a Eritrea. Todos los dictámenes y comentarios del SEPD se encuentran disponibles en su sitio *web*, en la dirección http://www.edps.europa.eu

la definición clara de las restricciones de tales derechos, y la disponibilidad de recursos judiciales efectivos y de una supervisión independiente.

29. La necesidad de introducir ulteriores mejoras en el procedimiento y las salvaguardas que se encuentran a disposición de las personas objeto de estas medidas ha sido recientemente confirmada por el Tribunal General en el asunto denominado «Kadi II» ([1]). En particular, el Tribunal subrayó la necesidad de que la persona consignada en la lista del bloqueo sea detalladamente informada sobre los motivos de dicha inclusión. Tal garantía colinda estrechamente con los derechos contemplados en virtud de la legislación sobre protección de datos y relativos al acceso a los propios datos personales y a que dichos datos sean rectificados, sobre todo cuando sean incorrectos u obsoletos. Estos derechos, mencionados explícitamente en el artículo 8 de la Carta de los Derechos Fundamentales, constituyen elementos esenciales de la protección de datos, y sólo podrán ser objeto de limitaciones en la medida en que éstas sean necesarias y previsibles, y así lo disponga la legislación.

30. Desde este punto de vista, el SEPD coincide con la Comunicación en que uno de los retos futuros en el ámbito de la política antiterrorista consistirá en cómo se aplique el artículo 75 del TFUE. Este nuevo fundamento jurídico, introducido por el Tratado de Lisboa, permite específicamente la adopción de medidas para el bloqueo de activos contra personas físicas o jurídicas. El SEPD recomienda que este fundamento jurídico se utilice asimismo para establecer un marco para el bloqueo de activos plenamente adecuado al respeto de los derechos fundamentales. El SEPD está dispuesto a seguir contribuyendo al desarrollo de instrumentos y procedimientos legislativos pertinentes, y confía en que se le consulte debida y oportunamente cuando la Comisión (con arreglo a su Programa de trabajo para 2011), desarrolle una normativa específica en esta materia ([2]).

31. Desde una perspectiva más amplia, es necesario establecer un marco de protección de datos aplicable también a la Política Exterior y de Seguridad Común. De hecho, el artículo 16 del TFUE establece el fundamento jurídico para establecer normas de protección de datos en el ámbito de la política exterior y de seguridad común. El fundamento jurídico y procedimiento diferente contemplado en el artículo 39 del TUE se aplicarán únicamente cuando los Estados miembros tramiten datos personales en este ámbito. No obstante, aún cuando en el Tratado de Lisboa se insta a la adopción de estas normas sobre protección de datos, y se brindan las herramientas para su establecimiento, por el momento, en la reciente Comunicación relativa a «Un enfoque global de la protección de los datos personales en la Unión Europea» ([3]) no se ha previsto iniciativa alguna. En este contexto, el SEPD insta a la Comisión a presentar una propuesta para la creación de un marco de protección de datos en el ámbito de la Política Exterior y de Seguridad Común.

([1]) Sentencia de 30 de septiembre de 2010 en el asunto T-85/09 *Kadi* contra la *Comisión*; véanse en particular los apartados 157 y 177.

([2]) El Programa de trabajo 2011 de la Comisión [COM(2010) 623 de 27 de octubre de 2010] menciona en su anexo II (Lista indicativa de posibles iniciativas objeto de consideración) un «Reglamento por el que se establece un procedimiento para el bloqueo de fondos de personas de las que se sospecha la comisión de actividades terroristas en la UE».

([3]) Comunicación de la Comisión (2010) 609 de 4 de noviembre de 2010.

4. **Respeto de los derechos fundamentales y cooperación internacional**

32. En el capítulo dedicado al respeto de los derechos fundamentales se hace hincapié en que la UE debe respetar de manera ejemplar la Carta de los Derechos Fundamentales, que ha de constituirse en «brújula» de todas las políticas de la UE. El SEPD acoge favorablemente dicho planteamiento.

33. El SEPD respalda asimismo la afirmación de que el respeto de los derechos fundamentales constituye no sólo un imperativo jurídico, sino también una condición clave para promover la confianza mutua entre las autoridades nacionales, y la credibilidad entre la ciudadanía en general.

34. En este contexto, el SEPD recomienda la adopción de un enfoque proactivo y acciones concretas con el fin de que dichas aspiraciones se materialicen, también como medio para una aplicación efectiva de la Carta de los Derechos Fundamentales de la UE ([4]).

35. Las evaluaciones del impacto sobre la privacidad (PIAs) y la consulta a las autoridades competentes en materia de protección de datos en una fase inicial deberán ser obligatorias en todas las iniciativas que repercutan en la protección de datos personales, independientemente de quién las emprenda y del ámbito en el que se propongan.

36. En el capítulo sobre cooperación internacional, la Comunicación subraya asimismo la necesidad de crear «el marco de condiciones legales y políticas necesarias para una mayor cooperación con los socios externos de la UE en el ámbito de la lucha contra el terrorismo».

37. A este respecto, el SEPD recuerda la necesidad de asegurar que se establezcan las salvaguardas apropiadas cuando se intercambien datos personales con terceros países y organismos internacionales, a fin de garantizar que los derechos de los ciudadanos a la protección de los datos se respeten adecuadamente asimismo en el contexto de la cooperación internacional.

38. Ello incluye también la promoción de la protección de los datos en colaboración con terceros países y organismos internacionales, con objeto de garantizar el cumplimiento de las normas de la UE. Estos objetivos son conformes además con la intención de la Comisión de elaborar normas jurídicas y técnicas rigurosas en relación con la protección de datos en terceros países y a escala internacional, y potenciando la cooperación con terceros países ([5]).

([4]) Véase la Comunicación de la Comisión (2010) 573 de 19 de octubre de 2010 sobre una Estrategia para la aplicación efectiva de la Carta de los Derechos Fundamentales por la Unión Europea.

([5]) Véase la Comunicación (2010) 609 sobre «Un enfoque global de la protección de los datos personales en la Unión Europea», páginas 16 y 17.

39. Las medidas restrictivas (bloqueo de activos) brindan una clara oportunidad para la actividad de la Unión Europea en este terreno, en el que la intensa cooperación con países terceros y con las Naciones Unidas no debe minar el elevado nivel de protección de los derechos fundamentales que proporciona el régimen jurídico de la UE.

III. **CONCLUSIONES**

40. El SEPD acoge favorablemente la atención que se presta en la Comunicación a los derechos fundamentales y la protección de datos, y recomienda un serie de mejoras concretas en el área de la política antiterrorista.

41. El SEPD recomienda apoyar con iniciativas concretas el respeto de los derechos fundamentales en este ámbito y, en particular, el derecho a la protección de los datos personales, que constituye un aliado necesario a la hora de promover la seguridad jurídica, la confianza y la cooperación en la lucha contra el terrorismo, así como una condición jurídica necesaria para el desarrollo de los sistemas previstos.

42. El SEPD respalda asimismo el planteamiento de que en este ámbito es preferible una formulación sistemática de las políticas, antes que otra basada en la respuesta a los incidentes, sobre todo cuando estos dan lugar a la creación de nuevos sistemas de almacenamiento, recogida e intercambio de datos sin una evaluación adecuada de las alternativas existentes.

43. Desde esta perspectiva, el SEPD recomienda a las instituciones de la UE que velen por que las políticas e iniciativas en materias de interior y de seguridad interna se formulen y se apliquen de modo que garanticen la adopción de un criterio coherente y la existencia de vínculos inequívocos entre las mismas, dando lugar así a la generación de sinergias apropiadas y positivas, y evitando la duplicación de trabajos y de esfuerzos.

44. En este contexto, el SEPD recomienda al legislador de la UE que potencie el papel otorgado a la protección de datos, mediante el compromiso con actuaciones (y plazos) específicos, como:

— evaluar la eficacia de las medidas en vigor, así como considerar su repercusión sobre la protección de la privacidad, son tareas cruciales, a las que debe otorgarse un papel relevante dentro de las actuaciones de la Unión Europea en esta materia,

— en el momento de contemplar la adopción de nuevas medidas, tener en cuenta posibles yuxtaposiciones con instrumentos ya existentes, teniendo en cuenta su eficacia, y limitando la recogida y el intercambio de datos personales a lo realmente necesario para los fines que se persiguen;

— proponer el establecimiento de un marco de protección de datos aplicable asimismo a la Política Exterior y de Seguridad Común;

— proponer un enfoque exhaustivo y global para garantizar, en el ámbito de las medidas restrictivas (bloqueo de activos), tanto la eficacia de las acciones encaminadas a velar por el cumplimiento de la legislación, como el respeto de los derechos fundamentales, con arreglo al artículo 75 del TFUE;

— reservar a la protección de los datos un papel central en el debate sobre las medidas en este ámbito, garantizando, por ejemplo, que se lleven a cabo evaluaciones de impacto sobre la intimidad y la protección de datos, y que las autoridades competentes en materia de protección de datos sean consultadas debidamente cuando se formulen propuestas pertinentes en esta materia;

— garantizar que los conocimientos técnicos especializados en materia de protección de datos se incorporen a la investigación sobre seguridad en una fase inicial, con el fin de guiar las opciones políticas elegidas y garantizar que el respeto de la privacidad se incorpore en la mayor medida posible a las nuevas tecnologías orientadas a la seguridad;

— garantizar la adopción de las salvaguardas adecuadas cuando se procesen datos personales en el contexto de la cooperación internacional, y promover el desarrollo y la aplicación de los principios relativos a la protección de datos por parte de terceros países y organismos internacionales.

Hecho en Bruselas, el 24 de noviembre de 2010.

Peter HUSTINX

Supervisor Europeo de Protección de Datos