ISSN 1830-9429

Informe anual

2010

SUPERVISOR EUROPEO
DE PROTECCIÓN DE DATOS

Informe anual

2010

Europe Direct es un servicio que le ayudará a encontrar respuestas a sus preguntas sobre la Unión Europea

Número de teléfono gratuito (*):

00 800 6 7 8 9 10 11

(*) Algunos operadores de telefonía móvil no autorizan el acceso a los números 00 800 o cobran por ello.

Más información sobre la Unión Europea, en el servidor Europa de Internet (http://europa.eu).

Al final de la obra figura una ficha catalográfica.

Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2011

ISBN 978-92-95073-23-4
doi:10.2804/219

Printed in Luxembourg

IMPRESO EN PAPEL BLANQUEADO SIN CLORO ELEMENTAL (ECF)

Contenidos

GUÍA PARA EL USUARIO

A continuación de la presente guía figuran una declaración de misión y una introducción a cargo de Peter Hustinx, Supervisor Europeo de Protección de Datos (SEPD), y de Giovanni Buttarelli, Supervisor adjunto.

El **capítulo 1** **(Hechos destacados de 2010)** presenta los aspectos más sobresalientes del trabajo del SEPD en 2010 y los resultados alcanzados en los diferentes ámbitos en los que se desarrolla su actividad.

El **capítulo 2** **(Supervisión)** describe las tareas efectuadas para supervisar y asegurar que las instituciones y organismos de la Comunidad cumplen sus obligaciones en materia de protección de datos. Presenta un análisis de los hechos más destacados de 2010 en materia de controles previos, reclamaciones, control del cumplimiento y asesoramiento sobre medidas administrativas. Expone las directrices temáticas adoptadas por el SEPD en los ámbitos de las investigaciones administrativas y los procedimientos disciplinarios, así como las tareas complementarias llevadas a cabo en el campo de las directrices sobre la videovigilancia. Recoge asimismo la nueva política del SEPD en materia de cumplimiento y aplicación.

El **capítulo 3** **(Consulta)** aborda el ejercicio de la función asesora por parte del SEPD, centrándose en los dictámenes y las observaciones emitidos sobre las propuestas legislativas y los documentos relacionados, así como en sus repercusiones sobre una serie de ámbitos cada vez más amplios. Describe asimismo la participación del SEPD en los asuntos pendientes ante el Tribunal de Justicia de la Unión Europea. Incluye además un análisis de temas de carácter horizontal: algunas cuestiones referidas a las nuevas tecnologías y a nuevos hechos de interés en el ámbito político y legislativo.

El **capítulo 4** **(Cooperación)** describe la labor desarrollada en foros importantes, como el Grupo de trabajo sobre protección de datos del artículo 29, y en las conferencias europeas e internacionales dedicadas a la protección de datos. Aborda asimismo la supervisión coordinada (por el SEPD y por las autoridades nacionales de protección de datos) de los sistemas informáticos a gran escala.

El **capítulo 5** **(Comunicación)** expone las actividades y realizaciones del SEPD en materia de información y comunicación, incluyendo la comunicación externa con los medios de comunicación, las actividades de mejora de la sensibilización y las herramientas de información en Internet.

El **capítulo 6** **(Administración, presupuesto y personal)** recoge detalladamente los principales hechos de interés en la organización del SEPD, entre ellos los referidos a las cuestiones presupuestarias, a los recursos humanos y a los acuerdos administrativos.

El **capítulo 7** **(Responsable de la protección de datos (RPD) del SEPD)** presenta el trabajo del nuevo equipo RPD del SEPD. Basándose en el plan de acción del RPD y en las normas de aplicación adoptadas, pone de relieve los progresos realizados en el registro de notificaciones, en la realización del «ejercicio de primavera» y en la atención de la necesidad de información y de mejora de la sensibilización.

El **capítulo 8** **(Principales objetivos para 2011)** hace una breve exposición y examina las principales prioridades para 2011.

Completan el informe una serie de **anexos.** Comprenden una visión general del marco jurídico relevante, algunas disposiciones del Reglamento (CE) n° 45/2001, la lista de autoridades competentes en materia de protección de datos, la relación de los dictámenes de control previo y de los dictámenes consultivos del SEPD, las alocuciones del Supervisor y el Supervisor adjunto y la composición de la secretaría del SEPD.

Existe, por otra parte, un resumen de conclusiones del presente informe, en el que se ofrece una versión resumida de las novedades más importantes referidas a las actividades del SEPD durante 2010.

Quienes deseen más información sobre el SEPD pueden consultar nuestro sitio web en: http://www.edps.europa.eu. El sitio web también dispone de una aplicación que permite suscribirse a nuestro boletín.

Pueden pedirse ejemplares impresos del Informe anual y del Resumen de conclusiones, con carácter gratuito, al servicio EU Bookshop (http://www.bookshop.europa.eu).

DECLARACIÓN DE MISIÓN

La misión del Supervisor Europeo de Protección de Datos (SEPD) consiste en garantizar el respeto de los derechos y libertades fundamentales de las personas (y en especial, el derecho a la intimidad) en el tratamiento de datos personales por parte de las instituciones y organismos de la UE.

Corresponde al SEPD:

- supervisar y garantizar el cumplimiento de las disposiciones del Reglamento (CE) n° 45/2001([1]) y de los demás actos de la UE relativos a la protección de los derechos y las libertades fundamentales con ocasión del tratamiento de datos personales por parte de las instituciones y organismos de la UE (supervisión);

- asesorar a las instituciones y a los organismos comunitarios en todos aquellos asuntos relacionados con el tratamiento de datos personales, incluida la consulta sobre propuestas legislativas y el control de las innovaciones en materia de protección de datos personales (consultoría);

- cooperar con las autoridades nacionales de control y con los organismos de supervisión del antiguo «tercer pilar» de la UE para mejorar la coherencia en la protección de los datos personales (cooperación).

En consonancia con lo anterior, los fines del SEPD consisten en desarrollar una labor estratégica encaminada a:

- propiciar una cultura de la protección de datos en las instituciones y organismos, contribuyendo además a fomentar la buena gobernanza;

- integrar el respeto de los principios de protección de datos en las políticas y en la legislación de la UE, allí donde sea pertinente;

- mejorar la calidad de las políticas de la UE en todos aquellos casos en los que la protección de datos eficaz constituye un requisito esencial para aplicarlas con acierto.

([1]) 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 (DO L 8 de 12.1.2001, p. 1).

INTRODUCCIÓN

Nos complace presentar al Parlamento Europeo, al Consejo y a la Comisión Europea el Informe anual que recoge las actividades del Supervisor Europeo de Protección de Datos (SEPD), de conformidad con el Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo y con el artículo 16 del Tratado de Funcionamiento de la Unión Europea, que sustituye al artículo 286 del Tratado CE.

El informe cubre el año 2010, sexto ejercicio completo del SEPD como nueva institución de supervisión independiente, responsable de garantizar que las instituciones y organismos de la UE respeten los derechos y las libertades fundamentales de las personas físicas y, en particular, su derecho a la vida privada, en relación con el tratamiento de los datos personales. Al mismo tiempo, el informe abarca el segundo año del mandato común quinquenal de los actuales responsables de este organismo.

Este año fue nuevamente de gran importancia para el derecho fundamental de la protección de datos. El impacto del Tratado de Lisboa, que establece un firme fundamento jurídico para una protección de datos exhaustiva en todas las esferas de las políticas comunitarias, es cada vez más visible. El proceso de revisión del marco jurídico de la UE para la protección de datos está avanzando y atrae un interés creciente. Dos iniciativas políticas clave, el Programa de Estocolmo sobre el espacio de libertad, seguridad y justicia, y la Agenda digital – piedras angulares de la estrategia Europa 2020 – ponen de relieve que la protección de los datos personales es un elemento crucial para la legitimidad y eficacia en este terreno.

El SEPD se ha implicado intensamente en estas áreas y está decidido a continuar esta participación en el futuro inmediato. Al mismo tiempo, hemos tratado de cumplir la función que corresponde a un organismo de supervisión independiente como el nuestro en todos los ámbitos principales de su actividad, y de mantener la idoneidad de su organización. Hemos conseguido así avances importantes, tanto en lo que se refiere al control del tratamiento de los datos personales por parte de las instituciones y organismos comunitarios, como a la consulta sobre nuevas políticas y medidas legislativas y a la estrecha cooperación con otras autoridades de control con vistas a garantizar una protección de datos más coherente.

Quisiéramos, por tanto, aprovechar esta oportunidad para expresar nuestro agradecimiento a todos cuantos apoyan nuestra labor en el Parlamento Europeo, el Consejo y la Comisión, así como a los numerosos miembros de las diferentes instituciones y organismos que son responsables de los procedimientos con los que se ejerce, en la práctica, la protección de datos. Quisiéramos, igualmente, enviar un mensaje de estímulo a todos aquellos que deben afrontar los importantes desafíos que tenemos por delante.

Deseamos, por último, expresar también un agradecimiento especial a los miembros de nuestro personal. Se trata de profesionales excepcionalmente cualificados que contribuyen sobremanera a la eficacia de nuestra actuación.

Peter Hustinx
Supervisor Europeo de Protección de Datos

Giovanni Buttarelli
Supervisor adjunto

1 HECHOS DESTACADOS DE 2010

1.1. Elementos esenciales

Una serie de hechos recientes han contribuido a situar los **derechos fundamentales y la protección de datos** en un lugar preferente de la agenda europea. El **Tratado de Lisboa,** vigente desde el 1 de diciembre de 2009, ha consagrado la protección de los derechos fundamentales de la Unión Europea (UE), al asignar a la Carta de los Derechos Fundamentales idéntico valor legal que a los Tratados y obligar a la UE al cumplimiento del **Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales** (CEDH). Por cuanto se refiere específicamente a la protección de datos, el artículo 16 del TFUE ofrece asimismo un fundamento jurídico general para la protección de las personas respecto del tratamiento de los datos de carácter personal por parte de las instituciones y organismos de la UE, así como por los Estados miembros en el ejercicio de las actuaciones comprendidas en el ámbito de aplicación del Derecho de la UE.

La importancia de los derechos fundamentales en general, y de la protección de datos en particular, ha sido destacada ulteriormente en el **Programa de Estocolmo,** el programa político quinquenal actualmente en vigor para el espacio de libertad, seguridad y justicia. Este Programa hace hincapié en la necesidad de asegurar el respeto de los derechos fundamentales y la libertad e integridad de las personas, garantizando a un tiempo su seguridad. Por consiguiente, el respeto de los derechos y dignidad de las personas, y de los restantes derechos contemplados en la Carta y en el CEDH, en particular el derecho a la intimidad y a la protección de los datos, constituyen los valores esenciales de las iniciativas europeas en este terreno. Es significativo que el Consejo Europeo haya invitado a la Comisión a presentar una propuesta sobre la incorporación de la Unión al CEDH «con carácter urgente».

Otras instituciones han dado también su respaldo a estas iniciativas. En relación con el Programa de Estocolmo, el Parlamento Europeo ha destacado la importancia de los derechos fundamentales para la evolución futura en el espacio de libertad, seguridad y justicia[2]. La propia Comisión ha aprobado recientemente una Comunicación por la que establece una estrategia para la aplicación eficaz de la Carta en el nuevo marco jurídico existente desde la entrada en vigor del Tratado de Lisboa.

El **proceso de revisión del marco jurídico de la protección de datos,** iniciado en 2009 y continuado en 2010, constituye un elemento fundamental para una Europa de los derechos fundamentales. En noviembre de 2010, la Comisión publicó una Comunicación relativa a un enfoque global de la protección de los datos personales en la Unión Europea. En ella se define la estrategia de la Comisión relativa a la actualización del marco jurídico de la UE para la protección de los datos personales en todos los ámbitos de las actividades de la Unión. La Comunicación pretende abordar los problemas inherentes a la globalización y a las nuevas tecnologías, de tal forma que quede garantizado en el

[2] Resolución del Parlamento Europeo del 25 de noviembre de 2009 sobre la Comunicación de la Comisión titulada 'Un espacio de libertad, seguridad y justicia al servicio de los ciudadanos – Programa de Estocolmo', P7_TA(2009)0090.

futuro un elevado nivel de protección de los datos personales. El SEPD está siguiendo de cerca el proceso de revisión, habiendo ya contribuido a él en diferentes ocasiones. Este proyecto seguirá siendo una de nuestras principales prioridades durante 2011.

La Comisión Europea dedicó también esfuerzos considerables en 2010 a la puesta en práctica de las diferentes iniciativas relacionadas con el Programa de Estocolmo. Algunas de estas propuestas se basan en un intenso intercambio de datos entre las autoridades policiales o de orden público de los distintos países y tienen, por consiguiente, efectos importantes sobre la intimidad de las personas y la protección de sus datos. En el desarrollo del espacio de **libertad, seguridad y justicia**, los órganos legislativos europeos tienen que mantener constantemente el justo equilibrio entre la seguridad y la libre circulación de los ciudadanos, y la protección de su intimidad y de sus datos de carácter personal. La aplicación del Programa de Estocolmo fue un aspecto fundamental de las actividades del SEPD en 2010, y probablemente también lo seguirá siendo en el futuro.

Otro elemento importante de las actividades del último año se refiere a los aspectos de la protección de datos relacionados con las **nuevas tecnologías.** Las tecnologías actuales permiten intercambiar y tratar los datos a una escala sin precedentes. Al mismo tiempo, ese tratamiento se lleva a cabo de formas más sutiles y menos detectables. Las redes sociales, la computación en la nube, los peajes automáticos, los dispositivos de geolocalización, la publicidad basada en el comportamiento y otros nuevos servicios de tipo similar plantean enormes desafíos para la protección de datos. La revisión del marco jurídico correspondiente deberá abordar estos problemas de manera eficaz, al objeto de garantizar un elevado nivel de protección en un mundo gobernado por la tecnología. Las nuevas tecnologías constituyen igualmente el núcleo de las iniciativas de la Comisión incluidas en la Agenda digital para Europa. El SEPD tendrá en cuenta tales iniciativas y las analizará siempre que planteen posibles problemas para la protección de los datos de las personas.

1.2. Panorámica general del año 2010

Las principales actividades del SEPD durante el año 2010 se basaron en la misma estrategia general seguida anteriormente, si bien a mayor escala y con un alcance mayor. También mejoró la capacidad del SEPD para actuar de manera efectiva y eficaz.

El marco jurídico([3]) en el que opera el SEPD contempla una serie de tareas y competencias que permiten efectuar una primera distinción entre tres funciones principales. Estas funciones siguen constituyendo plataformas estratégicas para las actividades del SEPD y quedan reflejados en su declaración de misión:

- **una función de supervisión**, que consiste en supervisar y asegurar el cumplimiento de las garantías legales existentes por parte de las instituciones y organismos comunitarios([4]) cada vez que efectúan un tratamiento de datos personales;

- **una función de consulta**, que consiste en asesorar a las instituciones y organismos comunitarios en todas las cuestiones pertinentes, y particularmente en relación con las propuestas legislativas que puedan afectar a la protección de datos personales;

- **una función de cooperación**, que consiste en colaborar con las autoridades y organismos nacionales de supervisión en el marco del antiguo «tercer pilar» de la UE, correspondiente a la cooperación policial y judicial en materia penal, con vistas a mejorar la coherencia en la protección de datos personales.

Estas funciones se describen más ampliamente en los capítulos 2, 3 y 4 del presente Informe anual, en los que se exponen las principales actividades del SEPD y los avances alcanzados en 2010. En esta sección se sintetizan algunos de sus elementos esenciales.

La importancia atribuida a la información y comunicación acerca de estas actividades justifica plenamente que se dedique el capítulo 5 exclusivamente a la comunicación. Todas estas actividades se basan en una gestión eficaz de los recursos financieros, humanos o de otro tipo, como se expone en el capítulo 6.

([3]) Véase el resumen del marco jurídico del Anexo A y el extracto del Reglamento (CE) nº 45/2001 del Anexo B.

([4]) A lo largo del presente informe se utilizarán los términos «instituciones» y «organismos» en el sentido del Reglamento (CE) nº 45/2001, es decir, incluyendo igualmente a las agencias de la UE. Para una lista completa, visite el enlace siguiente: http//europa.eu/agencies/community_agencies/index.es.htm

Supervisión

Las tareas de supervisión abarcan desde el asesoramiento y el apoyo a los funcionarios responsables de la protección de datos, mediante el control previo de las operaciones de tratamiento de datos de riesgo, hasta la práctica de investigaciones, incluidas las inspecciones sobre el terreno y la tramitación de las reclamaciones. El asesoramiento adicional prestado a la administración de la UE puede revestir la forma de consultas sobre medidas administrativas o de publicación de directrices temáticas.

Todas las instituciones y organismos de la UE deben contar al menos con un **responsable de la protección de datos** (RPD). En 2010, el número total de RPD se elevaba a 47. La interacción periódica con dichos responsables y con la red que conforman es una condición previa importante para que la supervisión resulte eficaz. Se creó un «cuarteto de RPD» integrado por los cuatro responsables de la protección de datos del Parlamento Europeo, el Consejo de la Unión Europea, la Comisión Europea y el Centro de Traducción de los Órganos de la Unión Europea, con el objetivo de coordinar la red de RPD. El SEPD colaboró estrechamente con dicho cuarteto.

El **control previo** de las operaciones de tratamiento que implican algún riesgo siguió siendo el principal elemento de la supervisión durante 2010. El SEPD emitió 55 dictámenes de control previo relacionados no sólo con procedimientos administrativos ordinarios, como los de evaluación, selección y promoción del personal, sino también con actividades en áreas fundamentales, como el Sistema de Alerta Precoz y Respuesta para el intercambio de información sobre enfermedades transmisibles. Estos dictámenes se publican en el sitio web del SEPD y su aplicación es objeto de seguimiento sistemático.

La **aplicación del Reglamento sobre protección de datos** por parte de las instituciones y organismos se controla sistemáticamente mediante una evaluación periódica de los indicadores de rendimiento, que se aplica a todas las instituciones y organismos de la UE. En el marco del ejercicio de control general iniciado en la primavera de 2009, el SEPD siguió supervisando la aplicación de las normas y principios de protección de datos en las instituciones y organismos participantes. El próximo ejercicio de control general (primavera de 2011) comenzará en los primeros meses de 2011. En este apartado también se realizaron controles específicos en los que el SEPD, en el ejercicio de sus funciones de control, investigó el nivel de cumplimiento de determinadas instituciones u organismos. Algunos de ellos se llevaron a cabo mediante el intercambio de correspondencia, y otros a través de visitas a los organismos correspondientes. En 2010 el SEPD realizó dos inspecciones de esta índole. También llevó a cabo una inspección sobre el terreno en el Centro Común de Investigación de Ispra, para verificar su nivel de conformidad en algunos aspectos concretos.

En 2010, el SEPD recibió 94 **reclamaciones,** de las que 25 fueron admitidas a trámite**.** Muchas de las no admitidas estaban relacionadas con problemas a escala nacional que no eran competencia del SEPD. La mayor parte de las reclamaciones admitidas se referían a supuestas infracciones en materia de acceso, rectificación, recogida excesiva y eliminación de datos. En once casos, el SEPD concluyó que se habían infringido las normas de protección de datos.

El SEPD continuó prestando **asesoramiento sobre las medidas administrativas** previstas por las instituciones y organismos de la UE en materia de tratamiento de datos personales. Se abordaron diversas cuestiones, como las transferencias de datos internacionales, el acceso a la identidad del informante, el uso interno de los correos electrónicos y la vigilancia electrónica.

El SEPD publicó asimismo **directrices** sobre investigaciones administrativas, procedimientos disciplinarios y videovigilancia.

En diciembre de 2010, el SEPD publicó un documento de orientación titulado «Control y garantía del cumplimiento del Reglamento (CE) nº 45/2001». En él se establece el marco de actuación del SEPD en materia de supervisión, medición y garantía del cumplimiento de las normas de protección de datos por parte de la administración de la UE, se describen las características de las diversas **facultades de aplicación** conferidas al SEPD y se definen las causas y circunstancias que pueden dar lugar a la adopción de medidas formales.

Consulta

En 2010 la Comisión hizo importantes avances en la creación de un nuevo **marco jurídico para la protección de datos en Europa.** Se concluyó la consulta pública iniciada en 2009, complementándola con una serie de consultas específicas a varias partes interesadas relevantes. En noviembre de 2010, la Comisión publicó su Comunicación relativa a un enfoque global de la protección de los datos

personales en la Unión Europea, en la que se identifican las principales prioridades y objetivos para la revisión de las normas actualmente vigentes.

El SEPD dedicó una atención particular a este proceso de revisión a lo largo de 2010, transmitiendo sus mensajes por diversas vías. En particular, organizó una conferencia de prensa sobre el tema inmediatamente después de la publicación de la Comunicación, al objeto de expresar públicamente su punto de vista sobre el nuevo marco jurídico. En ese acto, insistió en la importancia de la revisión realizada, que considera sumamente oportuna, y comentó los aspectos más destacados del nuevo marco.

El SEPD siguió aplicando su **política de consulta** de carácter general y superó su propio registro emitiendo 19 dictámenes sobre actos legislativos relativos a diversos temas. Esta política prevé además un enfoque anticipativo, que implica la elaboración de un inventario periódico de las propuestas legislativas sometidas a consulta y la disponibilidad del SEPD para elaborar observaciones informales en las fases preparatorias de las mismas. La mayoría de los dictámenes del SEPD fueron objeto de seguimiento posterior en conversaciones con el Parlamento y el Consejo.

En 2010, el SEPD siguió de cerca diversas iniciativas relacionadas directamente con la aplicación del **Programa de Estocolmo**. Entre otros asuntos, el SEPD abordó los problemas críticos en materia de protección de datos surgidos en el marco de la Estrategia de Seguridad Interior de la UE, la gestión de la información, la política antiterrorista europea y los Reglamentos de Frontex y de Eurodac. En general, las actividades relacionadas con el Programa de Estocolmo ocuparon un lugar destacado en su agenda, y se prevé que lo seguirán ocupando durante los próximos años.

También la **interrelación entre la intimidad y los cambios tecnológicos** ha sido objeto de importantes intervenciones por parte del SEPD. En mayo de 2010, la Comisión publicó una Comunicación relativa a una Agenda digital para Europa, con el objetivo de definir las prioridades de la UE en el mundo de Internet y de las tecnologías digitales. En marzo de 2010, el SEPD emitió un dictamen sobre el «Fortalecimiento de la confianza en la sociedad de la información mediante el fomento de la protección de los datos y la intimidad», como contribución a la Agenda digital de la UE. También ha intervenido, en diversas formas, en iniciativas relacionadas con Internet y con la neutralidad de la Red, la revisión de la Directiva de conservación de datos, la Directiva sobre residuos electrónicos, el Reglamento de la ENISA y la justicia electrónica.

El SEPD fue consultado también acerca de varias iniciativas en el ámbito de la **cooperación internacional en materia de seguridad y orden público,** como el acuerdo entre la UE y Estados Unidos sobre la protección de datos y el intercambio de información financiera dentro del Programa de Seguimiento de la Financiación del Terrorismo (TFTP II). Intervino igualmente con relación al Acuerdo Comercial de Lucha contra la Falsificación (ACTA) y los acuerdos sobre utilización de datos del registro de nombres de los pasajeros (PNR).

Por último, el SEPD intervino en otras áreas, como las relativas a la fiscalidad y las aduanas (incluyendo la cooperación administrativa en estas materias), los intercambios masivos de datos en el contexto del Sistema de Información del Mercado Interior, el uso de escáneres de seguridad en los aeropuertos, y diversos asuntos judiciales referidos a la relación entre el acceso del público a los datos y la protección de éstos.

Cooperación

El foro principal de cooperación entre las autoridades de protección de datos en Europa es el **Grupo de trabajo del artículo 29.** El SEPD participa en las actividades del mismo, que desempeña un papel importante para la aplicación uniforme de la Directiva de protección de datos.

El SEPD y el Grupo de trabajo del artículo 29 colaboraron de manera eficaz en una serie de temas, en particular referidos a la aplicación de la Directiva de protección de datos y a la interpretación de algunas de sus principales disposiciones. El SEPD prestó también una contribución activa en otros ámbitos, por ejemplo a través de sus dictámenes sobre los conceptos de «responsable» y de «encargado» del tratamiento de datos, sobre el principio de asunción de responsabilidades y sobre la legislación aplicable.

El SEPD participó asimismo en las reuniones y actividades del Grupo de trabajo sobre policía y justicia**,** un grupo consultivo dedicado a las cuestiones del antiguo tercer pilar.

Una de las tareas de cooperación más importantes del SEPD es la relativa al sistema **Eurodac,** en el que las funciones de supervisión se comparten con las autoridades nacionales de protección de datos.

Algunas cifras clave del SEPD en 2010

➔ **Adoptó 55 dictámenes de control previo** en relación con los datos de salud, la evaluación del personal, la contratación de personal, la gestión del tiempo de trabajo, las investigaciones de seguridad, el registro telefónico y las herramientas relacionadas con el rendimiento.

➔ **Acusó recibo de 94 reclamaciones, 25 de ellas admitidas a trámite.** La mayoría se referían a supuestas infracciones de la confidencialidad, exceso de celo en la recogida de datos o utilización ilegal de los mismos por parte del funcionario responsable del tratamiento.

- **Resolvió 10 asuntos** en los que el SEPD no vio indicio de infracción de la normativa sobre protección de datos.
- **Declaró once casos de incumplimiento** de esa normativa.

➔ **Acusó recibo de 35 consultas sobre medidas administrativas.** Asesoró en un amplio abanico de cuestiones jurídicas relacionados con el tratamiento de los datos personales por parte de las instituciones y organismos de la UE.

➔ **Practicó una inspección sobre el terreno.**

➔ **Publicó dos orientaciones,** sobre las investigaciones y los procedimientos disciplinarios administrativos, y sobre la videovigilancia.

➔ **Emitió 19 dictámenes legislativos** sobre diversas iniciativas en el ámbito de la libertad, seguridad y justicia, los cambios tecnológicos, la cooperación internacional y las transferencias de datos, la fiscalidad y las aduanas.

➔ **Emitió siete comentarios formales,** entre otros temas, sobre la revisión del Reglamento de Frontex, la Internet abierta y la neutralidad de la Red, el Sistema de Información del Mercado Interior, los escáneres de seguridad y los acuerdos internacionales sobre intercambio de datos.

➔ **Organizó tres reuniones del Grupo de coordinación de la supervisión de Eurodac,** a raíz de las cuales se ha puesto en marcha una nueva inspección coordinada, así como los trabajos preparatorios para una auditoría de seguridad completa.

➔ **Contrató a doce nuevos funcionarios.**

El Grupo de Coordinación de la Supervisión de Eurodac, compuesto por las autoridades nacionales de protección de datos y el SEPD, celebró tres reuniones en Bruselas en los meses de marzo, octubre y diciembre de 2010, e inició los trabajos preparatorios para la auditoría de seguridad completa que deberán llevar a cabo las autoridades de protección de datos, tanto a nivel nacional como de la UE. A finales de 2010 se puso en marcha una nueva inspección coordinada, cuyos resultados se darán a conocer en 2011.

Por cuanto se refiere a la supervisión del **Sistema de Información Aduanera (SIA)**, el SEPD convocó en 2010 dos reuniones del Grupo de Coordinación de la Supervisión del SIA, que congregaron a los representantes de las autoridades nacionales de protección de datos, de la Autoridad Común de Control Aduanero y de la Secretaría de Protección de Datos. En su reunión de diciembre, el Grupo aprobó el reglamento interno por el que se regirán sus actividades futuras, y debatió las posibles medidas que se deberían adoptar en el período 2011-2012 para lograr una supervisión integral de la protección de los datos en dicho sistema.

El SEPD continuó colaborando estrechamente con las autoridades competentes al objeto de crear mecanismos de **supervisión conjunta de los sistemas informáticos a gran escala existentes en la UE.**

Se siguió prestando una gran atención a la cooperación en **otros foros internacionales,** en especial a las conferencias europeas e internacionales que los Comisarios de protección de los datos e intimidad celebraron, respectivamente, en Praga y Jerusalén.

En colaboración con la Universidad Europea de Florencia, el SEPD organizó igualmente un seminario

sobre **«Protección de datos en las organizaciones internacionales»,** en el que se abordaron los diversos retos que deben afrontar las organizaciones de esta índole con el fin de alcanzar un nivel adecuado de protección de datos, en contextos frecuentemente difíciles y sin disponer de unos fundamentos jurídicos claros.

1.3. Resultados alcanzados en 2010

Se cumplieron, en todo o en parte, la mayor parte de los objetivos principales establecidos en 2009 y que se indican a continuación.

- **Respaldo a la red de responsables de la protección de datos (RPD)**

El SEPD siguió ofreciendo su firme respaldo a los responsables de la protección de datos (RPD), propiciando el intercambio de conocimientos y de buenas prácticas entre ellos. En el marco de su red, los RPD han elaborado un documento sobre «Normas profesionales para los responsables de la protección de datos de las instituciones y organismos comunitarios sujetos a las disposiciones del Reglamento (CE) nº 45/2001», finalizado en octubre de 2010. El SEPD remitió un escrito a todos los directivos de las instituciones y agencias avalando esas normas y subrayando el importante papel desempeñado por los RPD para lograr la conformidad con las directrices sobre protección de datos definidas en el Reglamento.

- **Función de control previo**

El SEPD está a punto de finalizar el control previo de las operaciones de tratamiento realizadas en ese momento por la mayor parte de las instituciones y organismos de antigua creación, y ha insistido especialmente en el seguimiento de sus recomendaciones. Durante el año 2010 se concluyó el análisis de 137 casos. Se prestó una atención especial al control previo de las operaciones de tratamiento comunes a las agencias, y a la resolución de estos casos a través de consultas mutuas.

- **Directrices horizontales**

Para contribuir al cumplimiento por parte de las autoridades y organismos comunitarios y mejorar de los procedimientos de control previo, el SEPD ha publicado directrices relativas a las investigaciones administrativas, a los procedimientos disciplinarios y a la videovigilancia.

- **Política de inspección**

Durante 2010, el SEPD continuó el seguimiento de las inspecciones anteriores. Por otro lado, realizó una inspección del Centro Común de Investigación de la Comisión Europea (JRC), en Ispra. En diciembre de 2010 publicó una amplia directriz general sobre el control del cumplimiento y la aplicación de las normas de protección de datos en las instituciones y organismos.

- **Alcance de la consulta**

El SEPD superó su propio récord y emitió 19 dictámenes y 7 series de observaciones formales sobre propuestas de nueva legislación, basándose siempre en un análisis sistemático de los temas y prioridades pertinentes, y adoptando medidas para su adecuado seguimiento. Todos los dictámenes y observaciones, así como el inventario, se encuentran disponibles en el sitio web. Se prestó una atención especial al plan de acción para la aplicación del Programa de Estocolmo.

- **Revisión del marco jurídico**

El SEPD siguió impulsando, en diferentes ocasiones y con ayuda de distintas herramientas, una ambiciosa estrategia dirigida al desarrollo de un marco jurídico moderno e integral para la protección de los datos que abarque todos los ámbitos de la política de la UE, garantice una protección eficaz en la práctica y sea capaz de proporcionar seguridad jurídica durante largos años. Las opiniones del SEPD se plasmaron asimismo en un dictamen emitido en enero de 2011.

- **Agenda digital**

El SEPD centró su actividad consultiva en los principales desafíos con que se enfrenta la protección eficaz de los datos personales. Para abordarlos es preciso conjugar un equilibrio adecuado entre la necesidad de seguridad y la protección de los datos, los cambios tecnológicos y los efectos de los flujos de datos a escala mundial. La Agenda digital de la Comisión Europea fue objeto de una atención particular en el dictamen emitido en marzo de 2010, en el que se desarrolla más ampliamente el concepto de «privacidad por diseño».

- **Actividades informativas**

El SEPD siguió trabajando en la mejora de la calidad y eficacia de las actividades de información y las herramientas de comunicación. Una novedad

importante en este aspecto fue la incorporación del alemán como tercera lengua, además del inglés y francés, en las relaciones con la prensa y otras actividades de comunicación.

- **Organización interna**

Se reorganizó la Secretaría del SEPD con objeto de definir mejor las responsabilidades y lograr un desempeño más eficaz y eficiente de las distintas funciones y tareas. En la nueva estructura organizativa, el Director se responsabiliza de la aplicación de las políticas y de la coordinación horizontal de las actividades realizadas en cinco sectores. Puede consultarse en el sitio web el nuevo organigrama.

- **Gestión de recursos**

A lo largo de 2010 se produjo un incremento importante (en una tercera parte) del personal al servicio del SEPD. Fue necesario, por tanto, paralelamente a la reorganización interna, intensificar los esfuerzos en los ámbitos de la planificación, de los procedimientos internos y de la ejecución presupuestaria. Se dedicó una atención especial a las nuevas necesidades de espacio de oficina y al desarrollo de un sistema de gestión de expedientes.

2 SUPERVISIÓN Y APLICACIÓN

2.1. Introducción

La tarea del SEPD, en su calidad de supervisor independiente, consiste en supervisar el tratamiento de los datos personales llevado a cabo por las instituciones y organismos comunitarios (a excepción del Tribunal de Justicia cuando actúa en el ejercicio de sus funciones jurisdiccionales). El Reglamento (CE) n° 45/2001 (en lo sucesivo, «el Reglamento») describe y concede una serie de derechos y facultades que facultan al SEPD para cumplir ese cometido.

El Tratado de Lisboa supone un giro en el marco jurídico regulador de la protección de datos en la administración europea, al introducir el artículo 16 del TFUE en sustitución del artículo 286 del Tratado CE. La abolición de la estructura de pilares ha dado lugar a que las funciones de supervisión del SEPD abarquen ahora, en principio, todas las instituciones y organismos de la UE, incluso en los ámbitos no incluidos en lo que solía llamarse «Derecho comunitario»([5]), salvo que otros instrumentos legislativos de la UE dispongan específicamente lo contrario. Las implicaciones concretas de estos cambios para las actividades de supervisión del SEPD están siendo analizadas aún y podrían requerir nuevas aclaraciones.

([5]) Véase el artículo 3, apartado 1, del Reglamento (CE) nº 45/2001, cuya relevancia es ahora menor que antes del 1 de diciembre de 2009.

Durante 2010, el control previo de las operaciones de tratamiento siguió siendo un aspecto importante de la supervisión (véase la sección 2.3), habiéndose dedicado una atención especial al seguimiento de las recomendaciones recogidas en los dictámenes. El SEPD desarrolló además otras modalidades de supervisión, como la tramitación de las reclamaciones, la realización de inspecciones, el asesoramiento sobre medidas administrativas y la redacción de proyectos de directrices temáticas. La supervisión de Eurodac es una actividad específica del SEPD que requiere una estrecha colaboración con las autoridades nacionales de protección de datos (véase la sección 4.2).

El SEPD aprobó unas directrices en materia de cumplimiento y aplicación en las que se señala un cambio de rumbo en la aplicación del Reglamento.

2.2. Responsables de la protección de datos

Una característica importante dentro del panorama de protección de datos en las instituciones de la Unión Europea es la obligación de nombrar a un responsable de la protección de datos (RPD) (artículo 24, apartado 1, del Reglamento). Algunas instituciones se han dotado asimismo de un RPD auxiliar o adjunto. Además, la Comisión ha designado un RPD para la Oficina Europea de Lucha contra el Fraude (OLAF, una Dirección General de la Comisión). Otras instituciones han nombrado también coordinadores de la protección de datos encargados de armonizar todos los aspectos de esta materia en una dirección o unidad determinada.

En 2010 fueron designados dos nuevos RPD en nuevas agencias o empresas comunes, lo que eleva el número total de los mismos a 47.

Desde hace varios años, los RPD se reúnen a intervalos regulares para intercambiar experiencias y abordar cuestiones horizontales. La colaboración en el marco de esta red informal se ha revelado muy productiva y siguió siéndolo a lo largo de 2010.

Se creó un «cuarteto de RPD», integrado por los cuatro responsables de la protección de datos del Parlamento Europeo, el Consejo de la Unión Europea, la Comisión Europea y el Centro de Traducción de los Órganos de la Unión Europea, con el objetivo de coordinar la red de RPD. El SEPD colaboró estrechamente con este cuarteto.

El SEPD asistió a las reuniones del RPD celebradas en marzo de 2010 en la sede del Banco Central Europeo en Luxemburgo, y en octubre de 2010 en la Agencia Europea de Medicamentos de Londres, donde tuvo ocasión de poner a los RPD al corriente de las actividades de SEPD, ofrecer una visión general de los últimos hechos relacionados con la protección de datos en la UE y comentar los temas de interés común.

Más específicamente, el SEPD aprovechó esos foros para explicar y comentar los procedimientos correspondientes a los controles previos, informar sobre los progresos realizados en las notificaciones de los controles previos, poner al día a los RPD sobre los intercambios de ideas en los comités interinstitucionales, describir la nueva estructura del SEPD y presentar las directrices temáticas elaboradas. También informó a los RPD sobre las políticas adoptadas en materia de cumplimiento y aplicación. Por otro lado, los citados foros permitieron compartir iniciativas en torno al Día europeo de la protección de datos, que se conmemora el 28 de enero.

En el marco de su red, los RPD han elaborado un documento sobre «Normas profesionales para los responsables de la protección de datos de las instituciones y organismos comunitarios sujetos a las disposiciones del Reglamento (CE) nº 45/2001», que fue aprobado en la reunión de la red celebrada el 14 de octubre de 2010. El SEPD remitió un escrito a todos los directivos de las instituciones y agencias avalando estas normas y subrayando el importante papel desempeñado por los RPD para lograr el cumplimiento de las reglas sobre protección de datos definidas en el Reglamento. El SEPD tiene la intención de utilizar este documento, cuando sea procedente, como base de partida para el desempeño de su función supervisora en relación con las instituciones y organismos.

Responsables de la protección de datos durante su reunión en Bruselas (marzo de 2010).

2.3. Controles previos

2.3.1. Base jurídica

El artículo 27, apartado 1, del Reglamento (CE) nº 45/2001 establece que todos los tratamientos que puedan suponer riesgos específicos para los derechos y libertades de los interesados en razón de su naturaleza, alcance u objetivos estarán sujetos a control previo por parte del SEPD.

En el artículo 27, apartado 2, del Reglamento se enumeran una serie de operaciones de tratamiento que pueden entrañar dichos riesgos. Siguieron aplicándose en la interpretación de esta disposición los criterios desarrollados en años anteriores([6]), tanto para decidir si una notificación de un RPD debía someterse a control previo como para asesorar en una consulta sobre la necesidad de control previo (véase también la sección 2.3.4).

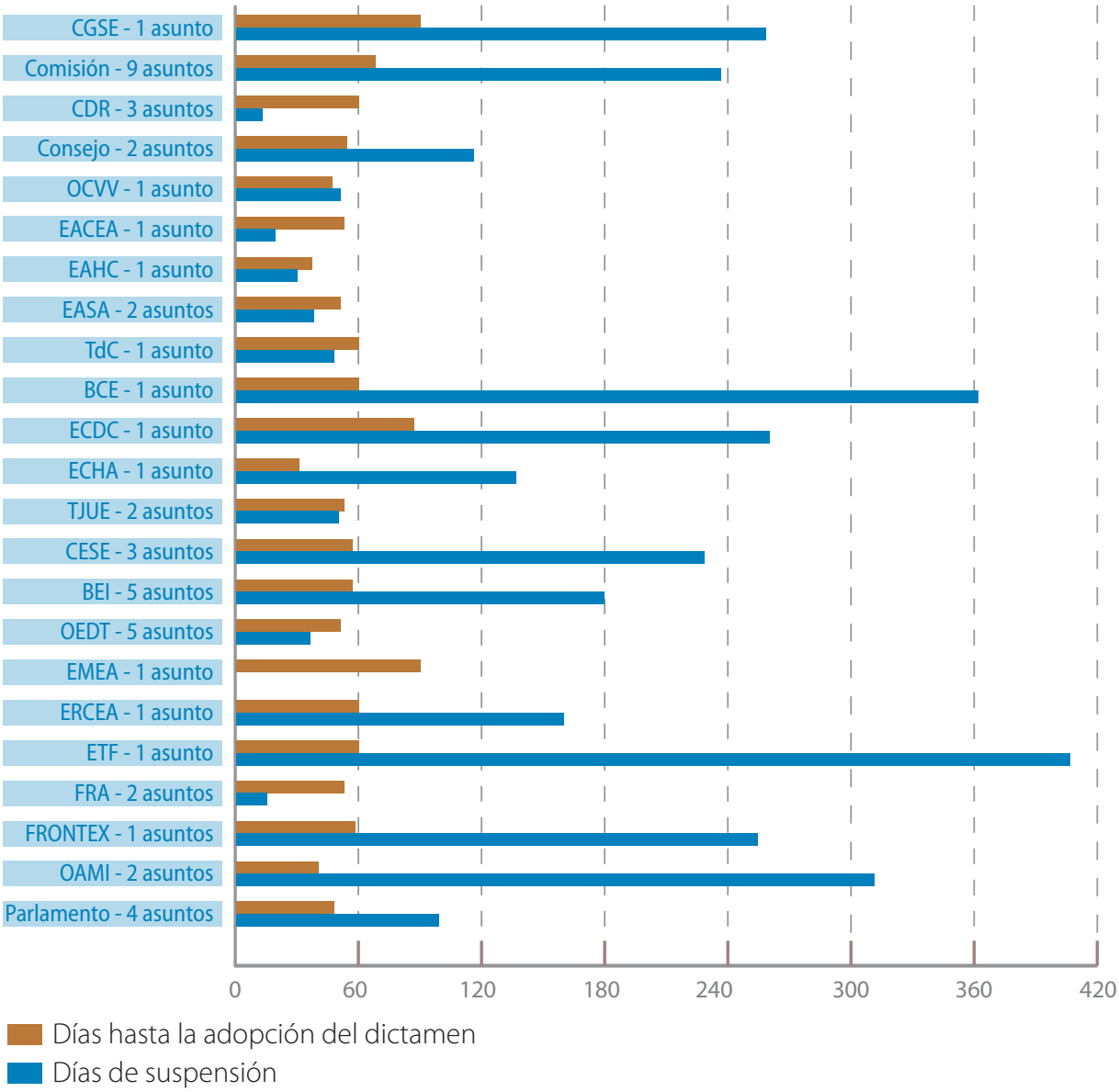
2.3.2. Procedimiento

Notificación

El SEPD debe efectuar controles previos siempre que recibe una notificación del RPD. En caso de que el RPD dude sobre si una operación de tratamiento determinada ha de someterse o no a control previo, puede consultarlo al SEPD (véase la sección 2.3.4).

([6]) Véase el Informe anual 2005, sección 2.3.1.

Plazos promedio por institución/agencia



Los controles previos afectan no sólo a las operaciones que aún no se hayan iniciado, sino también a las que se iniciaron con anterioridad al 17 de enero de 2004 (fecha del nombramiento del SEPD y el SEPD adjunto) o a la fecha de entrada en vigor del Reglamento (controles previos *ex post*). En dichas situaciones, el control a tenor del artículo 27 no puede ser «previo» en el sentido estricto de la palabra, sino que debe efectuarse *ex post*.

Plazo, suspensión y prórroga

El SEPD debe emitir su dictamen en un plazo de dos meses a partir de la recepción de la notificación([7]). En caso de que el SEPD solicite información complementaria, por lo general se deja en suspenso el plazo de dos meses hasta que la reciba. Esta suspensión se extiende durante el tiempo que se conceda al RPD de la institución u organismo para que formule sus observaciones y aporte más información, si procede, para completar el borrador de dictamen definitivo. En los casos complejos, el SEPD puede prorrogar el plazo inicial en otros dos meses. Si transcurrido el plazo de dos meses y las eventuales prórrogas no se ha emitido dictamen, se entenderá que éste es favorable. Hasta ahora no se ha producido nunca un dictamen tácito de este tipo.

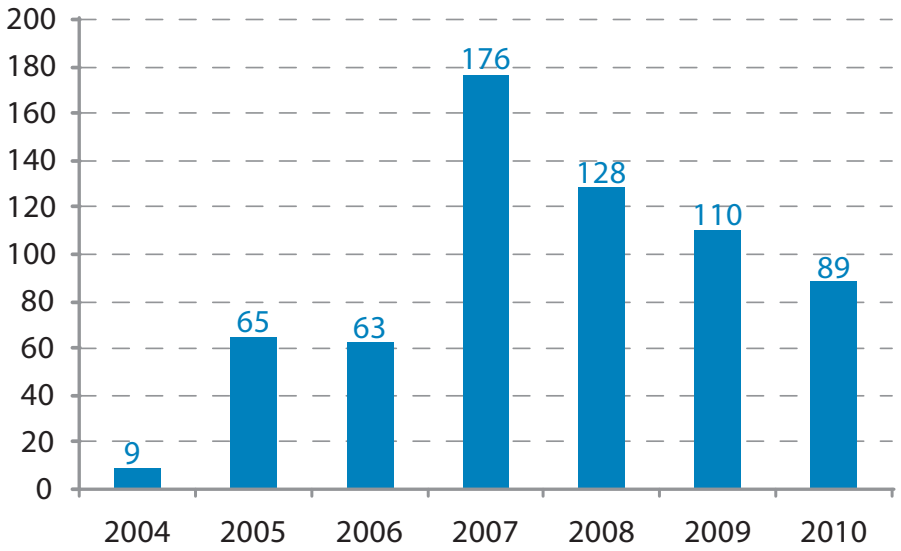
([7]) En los asuntos *ex-post* recibidos antes del 1 de septiembre de 2010 no se ha tenido en cuenta el mes de agosto, ni para las instituciones y organismos ni para el SEPD

Registro

En 2010, el SEPD recibió 89 notificaciones de control previo. Esta cifra supone una ligera disminución respecto a la de 2009, ya que el SEPD está recuperando el retraso acumulado en relación con los controles previos *ex post*.

El artículo 27, apartado 5, del Reglamento dispone que el SEPD llevará un registro de todos los tratamientos que se le hayan notificado sujetos a control previo. Este registro deberá contener la información indicada en el artículo 25 y estará abierto a consulta pública. Por motivos de transparencia, el registro público recogerá toda la información (con excepción de las medidas de seguridad, que no se mencionan) y podrá consultarse en el sitio web del SEPD.

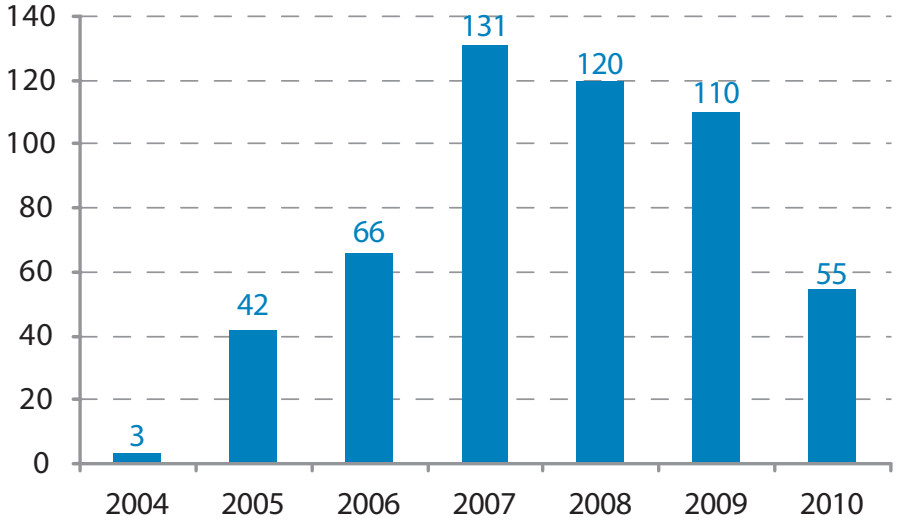
Notificaciones al SEPD



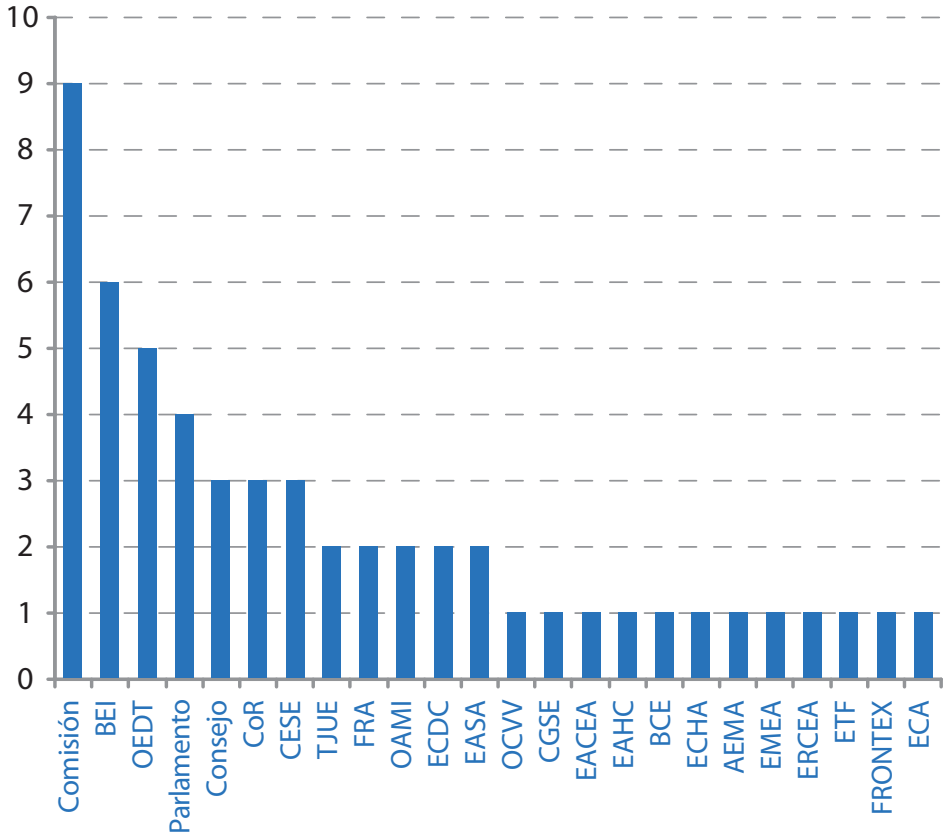
Dictámenes

La posición definitiva del SEPD se refleja en un dictamen dirigido al responsable de la operación de tratamiento y al RPD de la institución u organismo (artículo 27, apartado 4). En 2010, el SEPD emitió **55 dictámenes de control previo** (véase el gráfico anterior «Dictámenes de control previo del SEPD, por año», y **ocho dictámenes sobre operaciones no sujetas a control previo** (véase la sección 2.3.5). Aunque estas cifras representan una disminución frente a las de años anteriores, vale la pena señalar que, siguiendo la pauta iniciada con las directrices sobre videovigilancia y contratación del personal, el SEPD recurrió en un número importante de asuntos a la modalidad de dictamen conjunto, lo que permitió examinar las cuestiones de un modo más eficiente.

Dictámenes de control previo del SEPD, por año



Dictámenes de control previo del SEPD en 2010, por instituciones



Una **proporción sustancial de estos dictámenes** corresponden a operaciones de tratamiento realizadas por las **instituciones más relevantes**, entre ellos nueve de control previo (más tres de operaciones no sujetas a control previo) relativas a la Comisión Europea, cuatro al Parlamento Europeo y tres al Consejo (véase el gráfico «Dictámenes de control previo del SEPD en 2010, por instituciones»). También las agencias siguieron notificando sus actividades básicas y procedimientos administrativos normalizados con arreglo a los procedimientos aplicables establecidos por el SEPD (véase la sección 2.3.2).

Los dictámenes contienen una descripción del procedimiento, una exposición sumaria de los hechos y un análisis jurídico en el que se examina si la operación de tratamiento cumple las disposiciones pertinentes del Reglamento. En caso necesario, se formulan recomendaciones dirigidas al responsable del tratamiento con el fin de cumplir lo dispuesto en el Reglamento. Por lo general, las conclusiones del SEPD señalan que la operación de tratamiento no parece infringir ninguna de las disposiciones del Reglamento, pero siempre que se tengan en cuenta las recomendaciones formuladas.

Una vez que el SEPD ha emitido su dictamen, éste se hace público. Todos los dictámenes pueden consultarse en el sitio web del SEPD, junto con una exposición sumaria del asunto.

Un manual de consulta garantiza que todo el equipo trabaje partiendo de unos principios comunes, y que los dictámenes del SEPD se redacten tras un completo análisis de toda la información pertinente. El manual incluye modelos de dictámenes basados en la experiencia práctica acumulada y se actualiza de forma permanente. Se usa un sistema de flujo de trabajo para garantizar que se aplican todas las recomendaciones de cada asunto concreto y, si procede, que se cumplen todas las decisiones de aplicación (véase la sección 2.3.6).

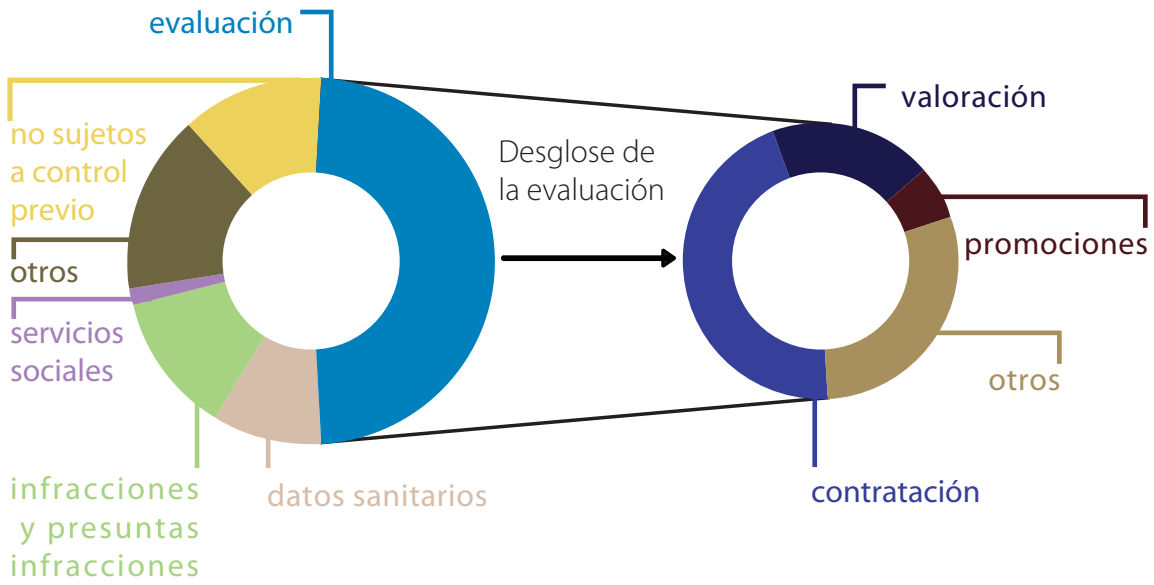
Procedimiento para los controles previos *ex post* en las agencias

En octubre de 2008, el SEPD puso en práctica un nuevo procedimiento para los controles previos *ex post* en las agencias de la UE. Dado que, en numerosas ocasiones, estos procedimientos normalizados coinciden con los de la mayoría de las agencias de la UE y se basan en decisiones de la Comisión, lo que se pretende es reagrupar las notificaciones que se refieren a temas similares y elaborar, o bien un dictamen común (para varias agencias), o bien un «minicontrol previo», en el que abordan únicamente las especificidades de una determinada agencia. Para ayudar a las agencias a cumplimentar sus notificaciones, el SEPD presenta un resumen de los puntos y las conclusiones principales de cada uno de los temas tratados en los dictámenes de control previo en forma de directrices temáticas (véase más adelante la sección 2.7, «Directrices temáticas»).

El primero de los temas así analizados fue la **contratación de personal,** la cual fue objeto de un dictamen horizontal en mayo de 2009 en el que se trataron las notificaciones recibidas de doce agencias. Un segundo conjunto de directrices sobre el **tratamiento de los datos de salud** se remitió a las agencias a finales de septiembre de 2009. En el momento de redactar el presente informe, el SEPD ha enviado su proyecto de dictamen horizontal a las 19 agencias implicadas, con el fin de recibir los comentarios correspondientes, y confía en publicarlo a principios de 2011. En abril de 2010, el SEPD publicó las directrices relativas al tratamiento de datos personales en las **investigaciones administrativas y procedimientos disciplinarios** realizadas por las instituciones y organismos comunitarios. El SEPD sigue recibiendo notificaciones de las agencias sobre este tema y tiene la intención de adoptar un dictamen conjunto en los seis primeros meses de 2011.

2.3.3. Principales temas de los controles previos

Dictámenes de 2010 por categorías



2.3.3.1. Sistema de Alerta Precoz y Respuesta – Comisión Europea

El Sistema de Alerta Precoz y Respuesta (EWRS) es una herramienta de comunicación utilizada por la Comisión, el Centro Europeo para la Prevención y el Control de las Enfermedades (ECDC) y los Estados miembros de la UE para intercambiar información sobre la prevención de enfermedades transmisibles (como tuberculosis, sarampión, síndrome respiratorio agudo grave, H1N1 y otras) con la finalidad de facilitar las actuaciones transfronterizas. Uno de los elementos del EWRS es el **«seguimiento de los contactos»**, procedimiento que permite identificar y localizar a quienes han podido estar en contacto con una persona infectada. Solo después de localizados estos contactos será posible diagnosticarlos y tratarlos adecuadamente. El seguimiento de los contactos favorece asimismo los intereses generales de la salud pública al reducir o impedir la propagación ulterior de la enfermedad.

En el correspondiente dictamen (asunto 2009-0137), el SEPD destacó la necesidad de **definir claramente las funciones, tareas y responsabilidades** de las partes implicadas en la aplicación y utilización del sistema y, en particular, las funciones de la Comisión y del ECDC. Es preciso designar inequívocamente a los responsables y los encargados y las funciones que desempeñan realmente, así como el estatuto jurídico de las organizaciones afectadas.

Deben especificarse claramente las responsabilidades de las partes y la forma en que los titulares de los datos pueden ejercer sus derechos. A corto plazo, se recomendó que el EWRS adoptase un **conjunto de directrices para la protección de datos.** También se invitó a la Comisión a efectuar una **revisión del marco jurídico** para establecer un fundamento jurídico más firme y una asignación de responsabilidades más clara.

Por otro lado, el SEPD hizo hincapié en la necesidad de aplicar el principio de **«privacidad integrada en el diseño»** y de incluir la protección de datos en la formación impartida a los usuarios. Debe existir un mecanismo claro para que los titulares de los datos puedan ejercer su **derecho de acceso**. Y por último, para garantizar la coherencia y transparencia, el operador del sistema EWRS debe ofrecer en su sitio web **información completa y de fácil**

El sistema EWRS es una herramienta de comunicación para el intercambio de información sobre enfermedades transmisibles.

comprensión a los intere-sados. Todo ello podría complementarse con avisos proporcionados por los puntos de contacto de los Estados miembros, con arreglo a la legislación nacional en materia de protección de datos.

2.3.3.2. Sistema Europeo de Vigilancia (TESSy) – Centro Europeo para la Prevención y el Control de las Enfermedades

El 3 de septiembre de 2010, el SEPD emitió un dictamen de control previo (asunto 2009-0474) sobre los aspectos del TESSy relacionados con la protección de datos. TESSy es una herramienta de comunicación del Centro Europeo para la Prevención y el Control de las Enfermedades, diseñada para garantizar un intercambio rápido y eficaz de los datos de vigilancia epidemiológica entre los Estados miembros de la UE.

El dictamen aclara que los **datos estadísticos** deben seguir siendo considerados «datos personales», estando por tanto sometidos a las disposiciones del Reglamento, siempre que permitan identificar a las personas aunque sea de forma indirecta. El hecho de haber aplicado determinadas «técnicas de anonimización» no implica necesariamente que los datos deban considerarse anónimos en el sentido del considerando 8 del Reglamento y no deban ser tratados en adelante como «datos personales».

El SEPD reiteró muchas de las recomendaciones formuladas en su dictamen sobre el EWRS (véase la sección anterior), añadiendo que sería preciso adoptar cuando antes una política específica para garantizar la seguridad del sistema TESSy.

2.3.3.3. Régimen Común del Seguro de Enfermedad

El Comité del Régimen Común del Seguro de Enfermedad (JSIMC) es responsable del funcionamiento de este sistema. El JSIMC está formado por representantes designados por los comités de personal de las instituciones y por representantes de las administraciones. Se ocupa de las modificaciones de la normativa y de las reclamaciones de los afiliados, publicando dictámenes, recomendaciones y propuestas relativas a las actividades del Régimen.

El SEPD se reunió con el JSIMC en noviembre de 2008 con el fin de comentar los temas de protección de datos en relación con los registros

gestionados por el JSIMC. Dado que las reclamaciones de los afiliados suelen incluir datos confidenciales, se decidió que el Comité enviaría una notificación al SEPD.

Dicha notificación dio lugar a un dictamen (asunto 2009-0070) emitido el 18 de enero de 2010, en el que las recomendaciones del SEPD se centraban especialmente en la **transmisión de datos personales** al JSIMC, en el **plazo máximo de conservación** en CIRCA (una aplicación basada en la web para los grupos de trabajo que utilizan datos compartidos) y en la adopción de una **política de seguridad apropiada** en el plazo de seis meses desde la publicación del dictamen.

2.3.3.4. Inspecciones de seguridad – Comisión Europea (DG Centro Común de Investigación de Ispra)

El 6 de septiembre de 2010 (asunto 2009-0682), el SEPD emitió un dictamen de control previo sobre las inspecciones de seguridad realizadas en el Centro Común de Investigación de Ispra, dependiente de la Comisión Europea. Durante esas inspecciones se examinaron las operaciones de tratamiento, con vistas a mantener y mejorar las normas de seguridad aplicables.

El SEPD reconoció que la «*Procedura in caso d'infortunio*» se refería al tratamiento de datos de salud con vistas a prevenir y minimizar las consecuencias de incidentes de seguridad de este tipo en el centro de Ispra.

El SEPD publicó recomendaciones dirigidas a **garantizar el respeto del principio de «limitación de la finalidad» en las transferencias de datos,** así como la **conformidad con los principios de calidad** aplicables al almacenamiento y tratamiento posterior de los datos personales en este contexto. También se recomendó efectuar la oportuna revisión de la actual declaración de intimidad.

2.3.3.5. Cuestionario BELBIN de autopercepción – Escuela Europa de Administración

La finalidad de este tratamiento de datos consiste en proporcionar a los participantes en los cursos de formación de la Escuela Europea de Administración (EAS) los resultados de una prueba sobre su función preferida dentro de un equipo. Los datos no se utilizan para realizar evaluación alguna sobre la persona en cuestión. En su dictamen de 15 de marzo de 2010 (asunto 2009-0377), el SEPD se centró en dos aspectos:

- **la relación entre la autoridad responsable, los encargados del tratamiento y el subcontratista:** aunque la EAS no tiene acceso a los datos tratados por el contratista, éste último ha de actuar con arreglo a las instrucciones impartidas por la EAS. Por consiguiente, el SEPD consideró que la EAS era la responsable de los datos de esta operación de tratamiento, ya que es la que determina los objetivos y los medios (el uso de la herramienta basada en la web). Los tres contratistas a cargo de los cursos de formación y el subcontratista responsable de la herramienta basada en la web se consideran encargados del tratamiento de datos personales que actúan por cuenta de la EAS. El subcontratista no está autorizado a realizar ninguna otra operación de tratamiento ulterior que vaya más allá de lo establecido por la EAS y especificado en el contrato suscrito entre el subcontratista y el contratista, con arreglo a lo estipulado en el contrato principal de la EAS con el contratista.

- **el carácter anónimo de los datos**: el informe entregado a los participantes no puede considerarse «anónimo» por que el subcontratista está en condiciones de relacionar las respuestas con los titulares de los datos, ya que los participantes suelen utilizar una dirección de correo electrónico que contiene su nombre y apellido.

El SEPD formuló recomendaciones sobre ambos aspectos, indicando en particular que el contrato entre el contratista y el subcontratista debe incluir las cláusulas correspondientes a los temas de obligado cumplimiento, especialmente la **confidencialidad y seguridad en el tratamiento**.

2.3.3.6. Vigilancia electrónica – Tribunal de Cuentas

El **Tribunal de Cuentas (TdC)** ha preparado un procedimiento de **acceso a los discos duros y correos electrónicos privados** con el fin de solucionas diversas situaciones (por ejemplo, la de las personas fallecidas, o que han abandonado la institución, o que se encuentran ausentes) en las que la información obtenida por esta vía es necesaria para el funcionamiento de la institución. El procedimiento propuesto requiere que la persona que solicita la información cumplimente un formulario normalizado. La solicitud debe incluir una descripción detallada del motivo o motivos que justifican el acceso, el nombre o nombres de los ficheros o cuentas de correo electrónico y/o la información buscada. Dicho formulario debe enviarse al responsable de la seguridad de la información y, en ausencia de este, al responsable de la seguridad física.

El Tribunal de Cuentas desarrolló un sistema para acceder a los discos duros y sistemas de correo electrónico privados.

Anteriormente, la solicitud se enviaba al SEPD a efectos de consulta, dado que este procedimiento **implica potencialmente el acceso a datos confidenciales** y el SEPD consideraba que la operación de tratamiento presentaba riesgos específicos que requerían una notificación de control previo.

En su dictamen de 10 de enero de 2010 (asunto 2009-0620), el SEPD recomendó al TdC que adoptase un **fundamento jurídico específico** para el uso y almacenamiento de los correos electrónicos de carácter privado, y que definiese **directrices claras para el usuario** de los recursos de la red y el correo electrónico.

2.3.3.7. Deducciones salariales en caso de huelga – Banco Central Europeo

De acuerdo con el artículo 1.4 del Reglamento de personal del Banco Central Europeo (BCE), a los miembros del personal les asiste el derecho de huelga. El artículo 1.4.5 establece que «salvo que el Comité Ejecutivo decida lo contrario, se deducirá el período total de duración de la huelga de las retribuciones salariales de los miembros del personal que participen en la misma». Por otro lado, «no se adoptarán medidas disciplinarias contra ningún miembro del personal que participe en una huelga, excepto en el caso de aquellos que, habiendo sido designados para prestar los servicios mínimos anteriormente indicados, se nieguen a prestarlos para adherirse a la huelga» (artículo 1.4.7).

En la medida en que la participación en una huelga trae consigo automáticamente una deducción del salario y otras percepciones, el tratamiento de los datos personales relacionados con esta deducción está sujeto a control previo del SEPD, ya que dicho tratamiento excluye a determinadas personas de un derecho, beneficio o contrato.

El 28 de septiembre de 2010, el SEPD emitió un dictamen de control previo (asunto 2009-0514) relativo a esta operación de tratamiento, formulando recomendaciones sobre los **plazos de conservación** de la documentación almacenada en el sistema de gestión de documentos y registros electrónicos del BCE y sobre la **información** que es preciso facilitar a los titulares de los datos.

2.3.3.8. Investigación de fraudes – Banco Europeo de Inversiones

La División de Investigación de Fraudes (IG/IN) del Banco Europeo de Inversiones (BEI) investiga las denuncias de prácticas prohibidas con arreglo a los procedimientos antifraude del BEI. Con el fin de poder llevar a cabo estas investigaciones, la IG/IN tiene pleno acceso a toda la información, documentos y datos relativos al personal, incluyendo los datos electrónicos en poder del BEI, aunque no se permite interceptar las comunicaciones o conversaciones. El Director de la IG/IN debe decidir si una reclamación o denuncia ha quedado demostrada, dando en tal caso traslado del expediente a las autoridades competentes, dentro y/o fuera del BEI, para que adopten las medidas apropiadas. Si, después de realizar las indagaciones

La División de Investigación de Fraudes del BEI investiga las denuncias sobre prácticas prohibidas.

consideradas razonables, la IG/IN determina que la reclamación o denuncia no ha sido corroborada, debe documentar sus conclusiones en una nota y proceder al archivo del caso.

El SEPD emitió un dictamen de control previo (asunto 2009-0459) acerca de las operaciones de tratamiento relacionadas con estas investigaciones de fraudes, recomendando que el BEI revise el **fundamento jurídico** de las mismas, apruebe un **protocolo oficial para los análisis informáticos de tipo forense,** armonice los plazos de conservación de los datos y facilite información a sus titulares.

2.3.3.9. Análisis empírico de las correlaciones entre las variables del sistema de trabajo y el proceso de toma de decisiones – Oficina de Armonización del Mercado Interior

Este control previo (asunto 2010-0468) se refería a los aspectos de protección de datos de un estudio llevado a cabo por la Oficina de Armonización del Mercado Interior (OAMI) bajo el título «Análisis empírico de las correlaciones entre las variables del sistema de trabajo y el proceso de toma de decisiones». El estudio debía contribuir a definir los perfiles de puestos de trabajo con características comparables y a elaborar buenas prácticas en la gestión de los recursos humanos aplicables a dichos perfiles. Además de las ventajas de tipo práctico en beneficio de la OAMI, el proyecto perseguía también objetivos científicos, ya que el analista que llevó a cabo la investigación tenía previsto publicar las conclusiones en una tesis de doctorado (después de someterlas a un cuidadoso trabajo de edición para proteger la intimidad de los participantes en el estudio). El SEPD planteó una serie de recomendaciones, especialmente en relación con la conservación de los datos, su transferencia a terceros y la información a sus titulares.

El SEPD recomendó que todos los datos personales almacenados en los servidores de la OAMI fuesen eliminados una vez transcurrido el plazo de conservación (2011). Advirtió asimismo al analista de que debía tener en cuenta la legislación nacional aplicable en relación con los microdatos conservados para posibles investigaciones futuras o comunicados a terceros, al objeto de garantizar el cumplimiento de las obligaciones relativas a la necesidad, finalidad y confidencialidad.

2.3.3.10. Base de datos central de exclusión – Comisión Europea

Con objeto de proteger los intereses económicos de las instituciones y sobre la base del Reglamento Financiero, la Comisión Europea realiza el tratamiento de los datos contenidos en una base de datos central de exclusión. Estos datos solamente se pueden utilizar para excluir a las entidades que representan una amenaza para los intereses económicos europeos de todas las contrataciones y subvenciones financiados con fondos de la UE o a través del Fondo Europeo de Desarrollo.

El SEPD llevó a cabo el correspondiente análisis (asunto 2009-0681**)** contando desde el primer momento con la plena colaboración de la institución afectada.

El SEPD concluyó que no había motivos para creer que se hubiera infringido ninguna de las disposiciones del Reglamento sobre protección de datos. No obstante, formuló algunas recomendaciones relativas a la información que debían recibir previamente los candidatos, licitantes y solicitantes de subvenciones en las convocatorias de propuestas y en las licitaciones.

2.3.3.11. Operaciones de retorno conjuntas – FRONTEX

El 26 de abril de 2010, el SEPD adoptó un dictamen (asunto 2009-0281) sobre el tratamiento de datos personales por parte de FRONTEX en relación con la «recogida de nombres y otros datos relevantes de las personas repatriadas en las operaciones de retorno conjuntas (ORC)». Este tratamiento debía servir para preparar y llevar a cabo las ORC organizadas por FRONTEX, a fin de poder facilitar a las compañías aéreas una lista de pasajeros y conocer, entre otros datos, el nombre y características de los repatriados, los riesgos que pudieran representar para la seguridad de la ORC y su estado de salud, con vistas a prestarles la asistencia médica necesaria durante la operación.

FRONTEX informó al SEPD de que hasta el momento no se habían tratado datos personales, pero que en un futuro próximo sería necesario hacerlo para: 1) cumplir mejor y seguir desarrollando las tareas de la Agencia en el contexto de las ORC; 2) prestar ayuda al Estado miembro o país asociado a Schengen que organiza la operación para elaborar y actualizar las listas de pasajeros; 3) mantener en todo momento una visión global de los Estados miembros o países asociados a Schengen participantes que habían facilitado (o no) los datos solicitados al Estado organizador de la operación, y 4) aumentar la eficacia y eficiencia de la ayuda prestada por FRONTEX para la organización de las ORC.

El SEPD dedicó una atención particular al fundamento jurídico del tratamiento, admitiendo que la Agencia, para la correcta ejecución de sus tareas en el contexto de las ORC, necesita realizar determinadas operaciones de tratamiento de datos personales, actuando como responsable de las mismas. Sin embargo, debido a la sensibilidad de los datos y actividades que afectan a un grupo de población vulnerable, el SEPD consideró que el artículo 9 del Reglamento de FRONTEX (Cooperación en materia de retorno) y el artículo 5, letra a), del Reglamento sobre protección de datos solamente pueden servir como fundamentos jurídicos provisionales de la actividad de tratamiento, que debería ser objeto de una cuidadosa revisión dirigida a definir un fundamento jurídico más específico.

El SEPD solicitó también a FRONTEX que ponga en práctica los pertinentes **procedimientos para garantizar los derechos de los titulares de los datos,** y para cumplir con la **obligación de informar** antes de realizar el tratamiento.

2.3.4. Consultas sobre la necesidad de control previo

La mera posibilidad de la presencia de datos sensibles no conlleva automáticamente un control previo. No obstante, el tratamiento de datos sensibles relacionados, por ejemplo, con la salud o con infracciones de tipo civil o penal, implica la necesidad de prestar una atención particular a la adopción de medidas de seguridad, tal como dispone el artículo 22 del Reglamento.

En caso de duda, las instituciones y organismos de la UE pueden consultar al SEPD sobre la necesidad de control previo. Durante 2010, el SEPD recibió de los RPD seis consultas de este tipo.

Entre los temas analizados por el SEPD cabe citar los procedimientos de selección para puestos directivos, las listas de asistentes y miembros de asociaciones que participan en los actos organizados por una institución, las actividades de tratamiento de un comité de personal y la política de formación de personal.

2.3.5. Notificaciones no sometidas a control previo o retiradas

Tras un analisis detallado, en ocho de los asuntos que fueron objeto de examen en 2010 se decidió que no debían ser sometidos a control previo, aunque ello no implica que en tales situaciones (denominadas también «no sujetas a control previo») el SEPD no pueda formular sus recomendaciones. Por otro lado, tres notificaciones fueron retiradas y otro sustituida.

En un caso relativo a la formación (asunto 2010-0638), la información complementaria recibida de la Autoridad Europea de Seguridad Alimentaria (EFSA) en el contexto de la notificación permitió aclarar que los datos recogidos eran primordialmente de tipo estadístico y se destinaban exclusivamente a garantizar la calidad de la política de formación de la EFSA. Aunque pueden incluir datos sobre la valoración de los formadores, los informes elaborados no tenían como objetivo evaluar a los formadores de manera individual. Basándose en esta información, el SEPD concluyó que esta notificación no estaba sujeta a control previo.

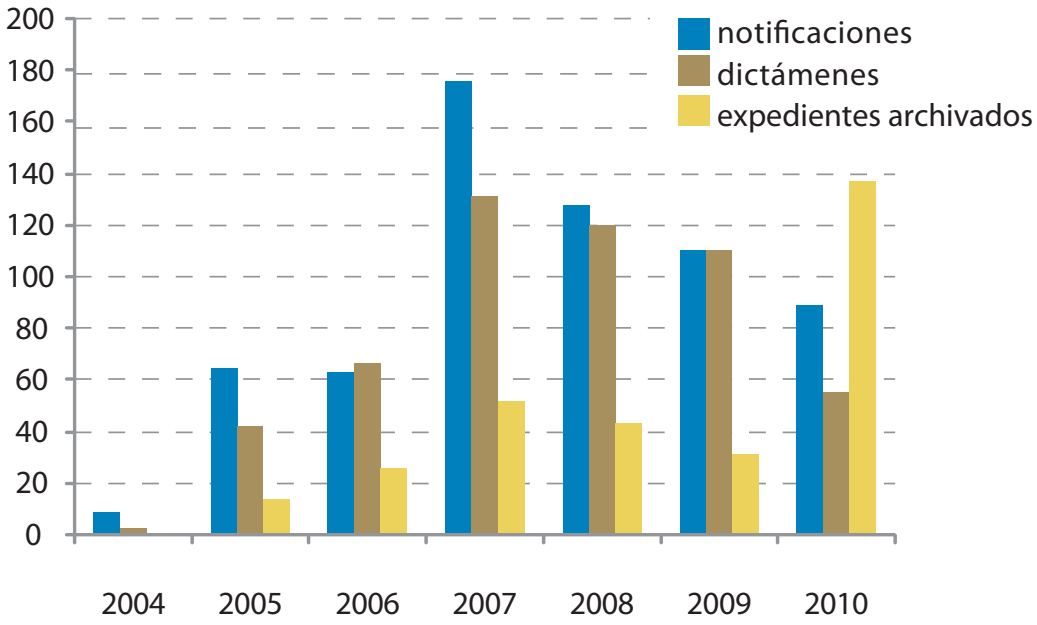
2.3.6. Seguimiento de los dictámenes de control previo anteriores

Por regla general, los dictámenes de control previo del SEPD concluyen declarando que la operación de tratamiento no infringe el Reglamento, siempre que se sigan determinadas ***recomendaciones.*** *También se formulan recomendaciones cuando, al analizar un caso para decidir si requiere control previo, se ponen de manifiesto ciertos aspectos críticos que parecen requerir medidas correctoras. Si el responsable del tratamiento desatiende estas recomendaciones, el SEPD podrá ejercer las atribuciones que le otorga el artículo 47 del Reglamento (CE) nº 45/2001.*

Las instituciones y organismos han mostrado buena disposición para seguir las recomendaciones del SEPD, por lo que hasta la fecha no ha sido necesario adoptar decisiones ejecutivas. El SEPD pide, en la carta oficial que adjunta a su dictamen, que la institución u organismo de que se trate le informe en un plazo de tres meses de las medidas adoptadas para dar cumplimiento a sus recomendaciones.

El SEPD considera que este seguimiento representa un **elemento clave para lograr la plena conformidad** con el Reglamento. De acuerdo con las indicaciones de su documento de orientación «Control y garantía del cumplimiento del Reglamento (CE) nº 45/2001», de reciente publicación, el SEPD espera

Comparación



que las instituciones y organismos **asuman responsabilidades** en relación con las recomendaciones formuladas. Dicho de otro modo, son responsables de su aplicación y deben ser capaces de demostrarlo ante el SEPD. Por consiguiente, cualquier institución u organismo que omita poner en práctica las recomendaciones se expone a la adopción de medidas de aplicación formales.

2.3.7. Conclusiones

Los 55 dictámenes emitidos por el SEPD le han permitido adquirir valiosos conocimientos sobre las operaciones de tratamiento, creando las condiciones precisas para aplicar estas experiencias y ofrecer directrices genéricas en determinadas áreas, como por ejemplo los procedimientos administrativos comunes. Así se advierte claramente en el tratamiento relacionado con las investigaciones administrativas y los procedimientos disciplinarios (véase la sección 2.7. «Directrices temáticas»). El SEPD seguirá transmitiendo esas directrices a las instituciones y organismos y facilitando el proceso de notificación de las mismas.

Dado que la mayor parte de las instituciones han finalizado el proceso de notificación de sus actuales operaciones de tratamiento relacionadas con los procedimientos administrativos normalizados, durante 2010 el SEPD recibió muchas notificaciones que se referían a procesos básicos específicos de determinadas instituciones o agencias.

El SEPD alcanzó en 2010 un hito importante en el seguimiento de sus dictámenes de control previo, ya que se cerraron 137 expedientes en el año, aunque continuará insistiendo en esta labor de vigilancia para garantizar que las instituciones y agencias adoptan las recomendaciones formuladas por él de forma rápida y satisfactoria.

2.4. Reclamaciones

2.4.1. Mandato del SEPD

En virtud de lo establecido en el artículo 46 del Reglamento (CE) nº 45/2001, una de las principales funciones del SEPD consiste en «conocer e investigar las reclamaciones» y «efectuar investigaciones por iniciativa propia o en respuesta a reclamaciones».

En principio, una persona solo puede presentar reclamaciones relativas a supuestas vulneraciones de su derecho da la protección de sus datos

Cualquier persona puede presentar una reclamación al SEPD relativa al tratamiento de sus datos personales por parte de la administración de la UE.

personales. Únicamente los miembros del personal de la UE pueden presentar reclamaciones por supuestas infracciones de las normas de protección de datos, estén o no afectados directamente por el tratamiento. El Estatuto de los funcionarios de la Unión Europea autoriza también a presentar reclamaciones al SEPD (artículo 90, letra b).

De conformidad con el Reglamento, el SEPD solo puede investigar reclamaciones presentadas por **personas físicas**. Las presentadas por empresas u otras personas jurídicas no son admisibles.

Además, los reclamantes deben identificarse, por lo que las peticiones anónimas no se consideran «reclamaciones». Sin embargo, se podrá tener en cuenta la información anónima en el marco de otros procedimientos (como una investigación por iniciativa propia, una petición de notificación de una operación de tratamiento de datos, etc.).

Las reclamaciones presentadas al SEPD solo pueden referirse al tratamiento de datos personales. *El SEPD no es competente para ocuparse de asuntos de mala administración de carácter general, para modificar el contenido de documentos que el reclamante cuestione o para conceder indemnizaciones financieras en concepto de daños.*

El tratamiento de datos personales objeto de una reclamación ha de ser una actividad llevada a cabo por ***una institución u organismo de la UE****. Por otra parte, el SEPD no es una instancia de recurso para las resoluciones de las autoridades nacionales de protección de datos.*

Un miembro del personal de la Comisión Europea reclamó contra el contenido de su informe de evaluación, elaborado por sus superiores. Solicitó del SEPD que ordenase a la Comisión modificar el informe debido a que incluía sus datos personales. El SEPD no aceptó los argumentos del reclamante. En efecto, si bien los datos de la evaluación tienen carácter personal, son por definición valoraciones subjetivas, que no pueden ser objeto de una rectificación automática basada en las normas de protección de datos. Para impedir la inclusión de los datos habría que introducir un procedimiento específico de impugnación de las conclusiones de los informes de evaluación.

2.4.2. Procedimiento de tramitación de las reclamaciones

El SEPD tramita las reclamaciones ajustándose al marco jurídico vigente, a los principios generales del Derecho comunitario y a las buenas prácticas administrativas comunes a las instituciones y organismos de la UE. En diciembre de 2009 el SEPD adoptó un **manual interno** para orientar al personal sobe esa tramitación. También puso a punto una **herramienta estadística** que permite llevar un control de las actividades relacionadas con reclamaciones y, en particular, controlar la evolución de determinados expedientes.

En todas las fases de la tramitación de una reclamación, el SEPD observa los principios de proporcionalidad y racionalidad. Guiado también por los principios de transparencia y no discriminación, emprende las acciones apropiadas teniendo en cuenta:

- la naturaleza y la gravedad de la supuesta infracción de las normas de protección de datos;
- la importancia del perjuicio que uno o más titulares de datos hayan o puedan haber sufrido a resultas de la infracción;
- la importancia global potencial del caso, también en relación con el resto de los intereses públicos o privados implicados;
- la probabilidad de que se llegue a determinar que la infracción se ha cometido realmente;
- la fecha exacta en que sucedieron los hechos, si las operaciones cuestionadas han dejado de generar los efectos impugnados, si tales efectos han sido eliminados o si existen garantías adecuadas de que se vayan a eliminar.

Toda reclamación recibida por el SEPD se somete a un atento examen. Este examen preliminar está diseñado específicamente para verificar si la reclamación cumple las condiciones para ser admitida a trámite, incluida la condición de que existan motivos suficientes para una investigación.

Las reclamaciones para las que el SEPD **carezca de competencia jurídica** se declararán no admisibles a trámite, hecho del cual se informará debidamente a los reclamantes. En estos casos, si procede, el SEPD podrá indicar a los reclamantes que se dirijan a otra autoridad competente (por ejemplo, el Tribunal de Justicia, el Defensor del Pueblo Europeo, las autoridades nacionales de protección de datos, etc.).

Las reclamaciones sobre hechos **manifiestamente insignificantes,** o cuya investigación requeriría esfuerzos desproporcionados, no se siguen investigando. El SEPD solo puede investigar reclamaciones relativas a **infracciones reales o potenciales**, y no puramente hipotéticas, de las normas pertinentes relativas al tratamiento de datos personales. Se requiere, pues, un análisis de las restantes opciones disponibles para solventar el problema, ya sea por parte del reclamante o del SEPD. Por ejemplo, el SEPD puede abrir una investigación por iniciativa propia sobre un problema general, en lugar de investigar un asunto que concierna de forma individual a un reclamante. En estos casos se informa al reclamante sobre estas modalidades de actuación alternativas.

Una candidata en un proceso de selección preguntó al SEPD si podría acceder a los datos personales de los restantes candidatos o si se le denegaría dicho acceso por motivos de protección de datos. El SEPD no adoptó una posición sobre el tema, porque la pregunta tenía carácter hipotético, ya que el organismo comunitario implicado todavía no había denegado el acceso a la información deseada, y por consiguiente no había invocado aún la protección de datos como motivo para la denegación.

En principio, si el reclamante no **se ha puesto previamente en contacto con la institución** de que se trate para corregir la situación, **la reclamación es inadmisible**. Si no se ha puesto previamente en contacto con la institución, ha de presentar al SEPD razones suficientes para no hacerlo.

Si la cuestión ya está siendo examinada por los organismos administrativos (es decir, si la institución ya está llevando a cabo una investigación interna), en principio la reclamación se podrá admitir a trámite. Sin embargo, el SEPD puede decidir, sobre la base de los hechos particulares del asunto, esperar el resultado de estos procedimientos administrativos antes de empezar a investigar. En cambio, si la misma cuestión (los mismos supuestos de hecho) ya está siendo examinada por un tribunal, la reclamación se declara inadmisible.

A fin de garantizar el tratamiento coherente de las reclamaciones sobre protección de datos y evitar repeticiones innecesarias, en noviembre de 2006 el **Defensor del Pueblo Europeo** y el SEPD firmaron un memorándum de acuerdo. Entre otras cosas, este documento establece que una reclamación presentada previamente no deberá ser reabierta por la otra institución, salvo que se aporten nuevas pruebas significativas.

En cuanto a los **plazos máximos para reclamar**, si el asunto planteado ante el SEPD se refiere a hechos ocurridos hace más de dos años, en principio la reclamación es inadmisible. Este plazo de dos años empieza a contar desde la fecha en que el reclamante haya tenido conocimiento de los hechos.

Si se considera admisible la reclamación, normalmente el SEPD pondrá en marcha **una investigación.** Esta investigación puede incluir una petición de información a la institución afectada, un análisis de los documentos pertinentes, una reunión con el responsable del tratamiento, una inspección sobre el terreno, etc. El SEPD está facultado para obtener de la institución u organismo de que se trate acceso a todos los datos personales y a toda la información necesaria para la investigación. También puede obtener acceso a cualquier local en que un responsable del tratamiento o institución u organismo lleve a cabo sus actividades.

Al término de la investigación, se envía una **decisión** al reclamante, así como al responsable del tratamiento de los datos. En su decisión, el SEPD manifiesta su posición acerca de cualquier infracción de las normas de protección de datos por la institución de que se trate. Las amplias **facultades del SEPD** van desde el simple asesoramiento a los titulares de los datos hasta la imposición de una prohibición de tratamiento o la remisión del asunto al Tribunal de Justicia, pasando por la formulación de advertencias o amonestaciones dirigidas al responsable del tratamiento.

Cualquier persona interesada puede solicitar al SEPD que realice una **revisión** de esa decisión en el plazo de un mes desde la fecha de la misma, y también es posible recurrir directamente al Tribunal de Justicia.

En 2009, dos reclamantes recurrieron las decisiones del SEPD ante el Tribunal de Primera Instancia (asuntos T-164/09 y T-193/09). En el primer asunto, el Tribunal falló que no había necesidad de pronunciarse sobre la actuación del SEPD por falta de objeto de litigio. En el segundo asunto, el Tribunal rechazó la solicitud de asistencia jurídica planteada por el demandante, sin entrar en el fondo de la demanda.

2.4.3. Garantía de confidencialidad para los reclamantes

*El SEPD reconoce que algunos reclamantes ponen su carrera profesional en peligro al denunciar infracciones de las normas de protección de datos y que, por consiguiente, se debe garantizar la **confidencialidad** a los reclamantes e informantes que la soliciten. Por otra parte, el SEPD se ha comprometido a trabajar de **forma transparente** y a publicar al menos lo esencial de sus decisiones. Sus procedimientos internos reflejan este difícil equilibrio.*

La práctica habitual es dar a las reclamaciones un **tratamiento confidencial**. Ello implica la no revelación de información personal a personas externas al SEPD. Sin embargo, para la adecuada realización de la investigación puede ser necesario informar a los servicios pertinentes de la institución afectada y a los terceros implicados acerca del contenido de la reclamación y de la identidad del reclamante. Además, el SEPD remite al responsable de la protección de datos (RPD) de la institución de que se trate copia de toda la correspondencia intercambiada con esta institución.

Si el reclamante solicita mantener el **anonimato** frente a la institución, al RPD o a los terceros implicados, se le invita a explicar las razones de tal solicitud. A continuación, el SEPD analiza los argumentos del reclamante y examina sus consecuencias para la viabilidad de la investigación posterior. Si el SEPD decide no conceder el anonimato al reclamante, le explica su valoración del caso y le pregunta si desea que examine la reclamación sin garantizarle el anonimato o si prefiere retirarla. Si el reclamante decide retirar la reclamación, la institución de que se trate no será informada de la existencia de ésta. En tal caso, el SEPD podría emprender otras acciones en relación con la cuestión sin revelar a la institución afectada la existencia de la reclamación, es decir, podría realizar una investigación por iniciativa propia o solicitar una notificación de operación de tratamiento de datos.

Una vez terminada una investigación, en principio todos los **documentos relacionados con la reclamación**, incluida la decisión final, siguen siendo confidenciales. No se publican íntegramente ni se transfieren a terceros. No obstante, el SEPD podrá publicar en su sitio web y en su Informe anual un resumen anónimo de la reclamación, de forma que el reclamante y las terceras partes no puedan ser identificados. El SEPD podrá también decidir publicar la decisión final *in extenso*, cuando se trate de asuntos importantes. Ello se deberá hacer teniendo en cuenta cualquier petición de confidencialidad del reclamante y, por lo tanto, de forma que no sea posible identificar al reclamante ni a otras personas afectadas.

2.4.4. Reclamaciones tramitadas en 2010

2.4.4.1. Número de reclamaciones

Durante 2010 aumentó el nivel de complejidad de las reclamaciones recibidas, aunque se redujo su número. ***En 2010, el SEPD recibió 94 reclamaciones*** *(un 15 % menos que en 2009). De éstas,* ***69 no fueron admitidas a trámite****, la mayoría de ellas por estar relacionadas con un tratamiento a nivel nacional, y no de ninguna institución u organismo de la UE.*

Las 25 reclamaciones restantes requirieron investigaciones de mayor calado (lo que supone una disminución del 41 % respecto a 2009). Además, 18 reclamaciones presentadas en años anteriores y admitidas a trámite (16 de 2009 y dos de 2008) seguían en fase de investigación o de revisión en 2010.

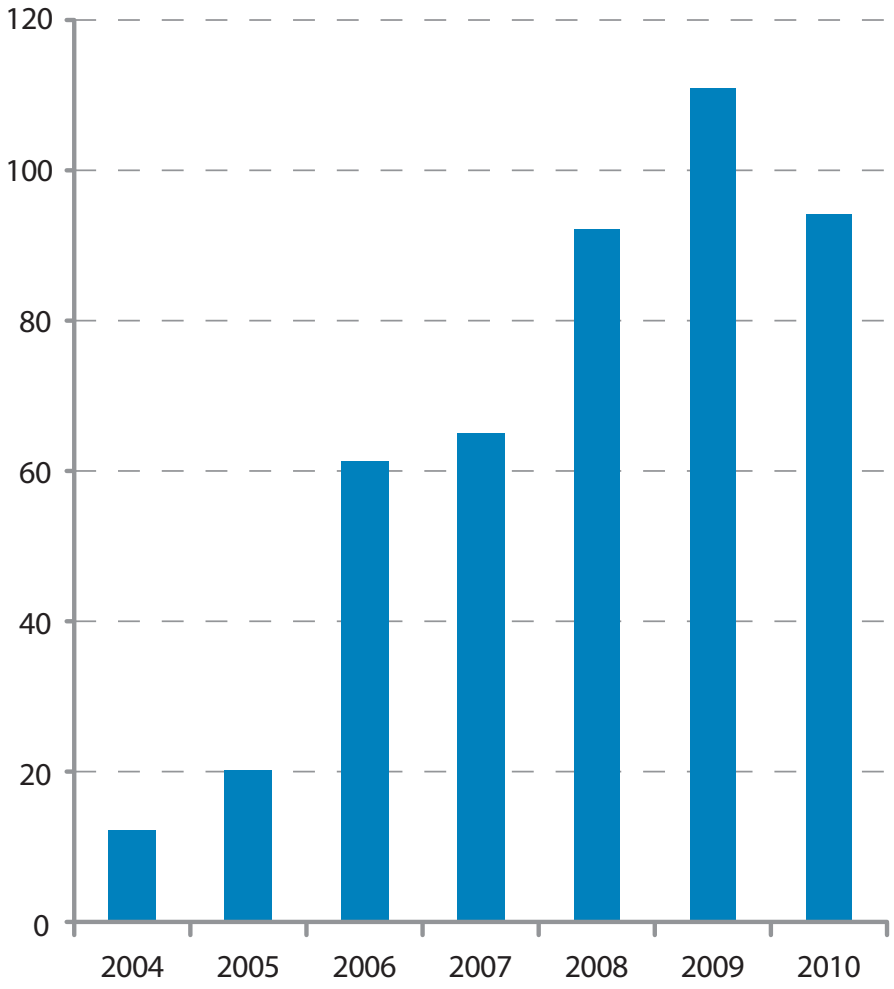
2.4.4.2. Tipos de reclamantes

De las 94 reclamaciones recibidas, 17 (el 18 %) fueron presentadas por miembros del personal de las instituciones u organismos de la UE, incluidos antiguos miembros del personal y candidatos a un puesto. En los 77 casos restantes, el reclamante no parecía mantener una relación laboral con la administración de la UE.

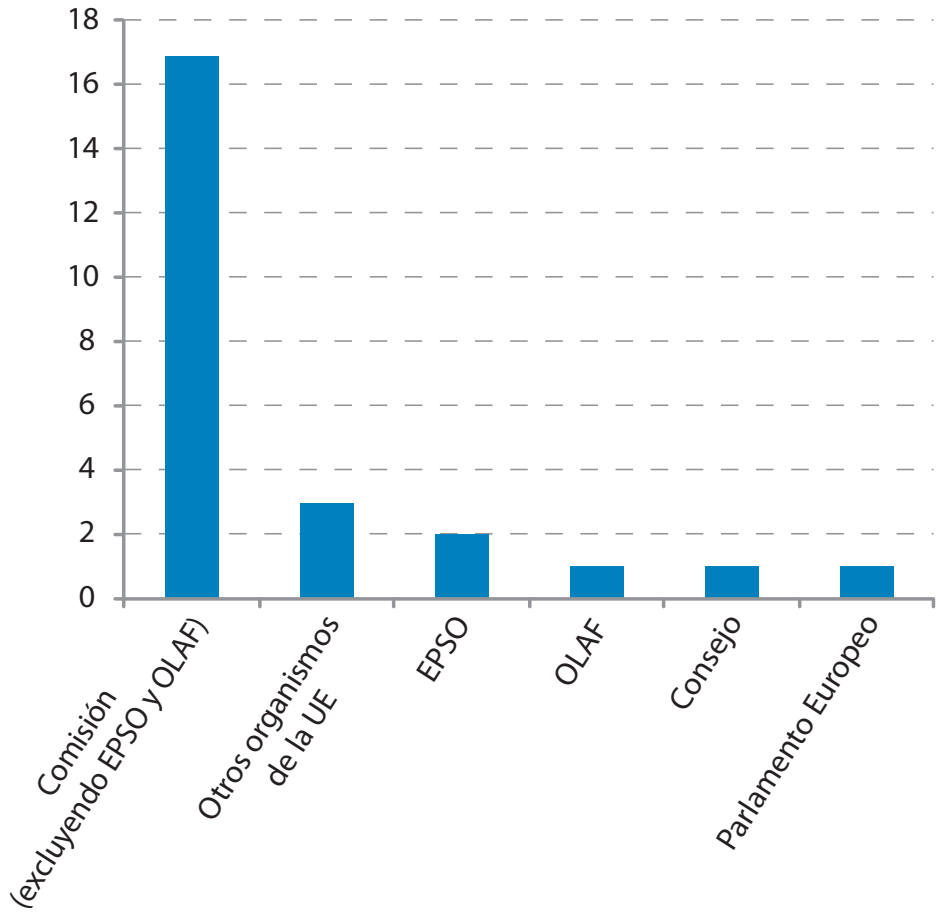
2.4.4.3. Instituciones objeto de reclamación

De las reclamaciones admitidas a trámite en 2010, la mayoría (80 %) iban dirigidas contra la **Comisión Europea, la OLAF y la EPSO**. Este dato responde a una situación previsible en el caso de la Comisión, desde el momento en que trata más datos personales que las demás instituciones y organismos de la UE. En cuando al elevado número de reclamaciones relacionadas con la OLAF y la EPSO, puede explicarse por la naturaleza de las actividades de estos organismos.

Número de reclamaciones recibidas (evolución 2004-2010)



Instituciones y organismos de la UE afectados



2.4.4.4. Lengua de las reclamaciones

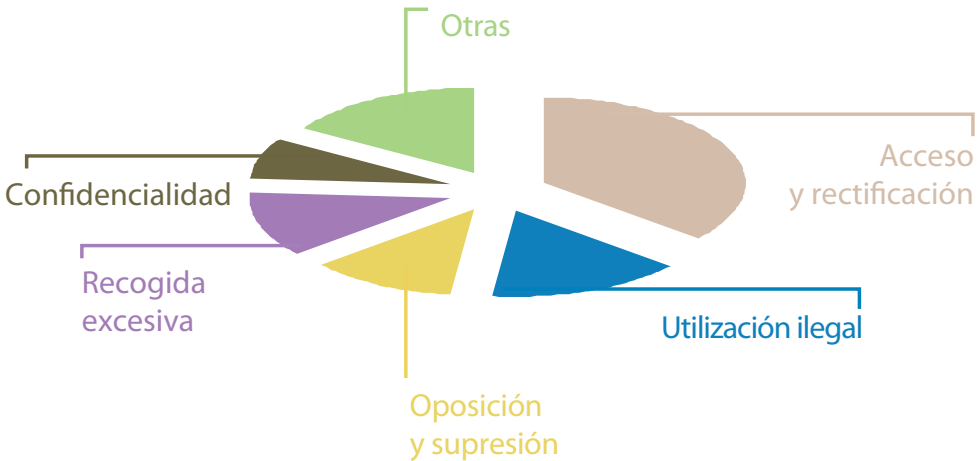
La mayor parte de las reclamaciones se presentaron en inglés (44 %) o alemán (33 %), y en menor medida en francés (15 %). Las reclamaciones en otras lenguas fueron relativamente escasas (8 %).

2.4.4.5. Tipos de infracciones denunciadas

Los principales tipos de infracción de las normas de protección de datos denunciadas por los reclamantes en 2010 se referían a:

- violaciones de los derechos de los interesados, como el acceso y la rectificación (36 %), o bien la oposición y supresión (12 %);

Tipos de violaciones denunciadas

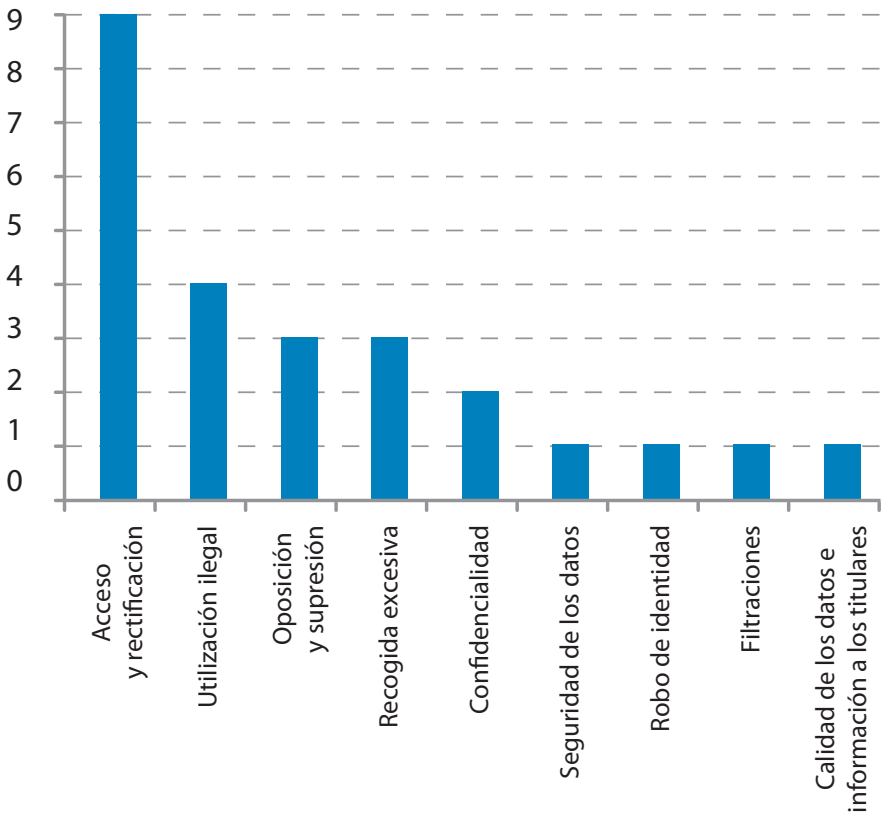


- utilización ilegal (16 %), recogida excesiva de datos personales (12 %), violación de la confidencialidad (8 %).

Otras infracciones denunciadas con menor frecuencia fueron las relacionadas con la seguridad de los datos (4 %), los robos de identidad (4 %), las filtraciones (4 %), la calidad de los datos y la información a los titulares (4 %).

2.4.4.6. Resultados de las investigaciones del SEPD

Resultados de las investigaciones del SEPD



En 11 de los asuntos resueltos durante 2010, el SEPD no detectó infracción de las normas de protección de datos.

Por el contrario, en diez de los casos se halló que no se habían respetado las normas de protección de datos, por lo que se formularon recomendaciones dirigidas al responsable del tratamiento.

El SEPD recibió una reclamación relativa al acceso del interesado a su expediente médico personal conservado en los servicios médicos de una institución. El SEPD confirmó que, de acuerdo con las normas de protección de datos, el acceso a los datos personales no significa que el responsable del tratamiento esté obligado a entregar el fichero original conteniendo los datos de salud, sino que debe tener la posibilidad práctica de examinarlo (personalmente o en algunos casos a través de un médico) y/o de realizar copias del mismo. Respecto al derecho de rectificación de los datos inexactos o incompletos, el SEPD hizo hincapié en que la obligación de rectificar los datos de salud se refiere únicamente a su contenido factual y no a las valoraciones relacionadas con la salud. Por consiguiente, el responsable del tratamiento no está obligado, en virtud de las normas de protección de datos, a modificar las conclusiones de un informe médico específico. En este contexto, el derecho a la rectificación de los datos podría conllevar la posibilidad de incluir otro informe de un médico distinto con una valoración diferente. En consecuencia, el SEPD concluyó que en este asunto no se habían incumplido las normas de protección de datos.

Se recibió una reclamación relacionada con la publicación de datos personales altamente sensibles en el Diario Oficial de la Unión Europea y en las actas de una sesión del Parlamento Europeo. Después de investigar el asunto, el SEPD concluyó que tanto la opinión del diputado al Parlamento como el mensaje político de la declaración escrita se hubieran podido expresar y transmitir eficazmente sin necesidad de revelar la identidad de las personas en cuestión. El SEPD solicitó la supresión de los nombres de las personas mencionadas por el diputado en su declaración escrita y en cualquier otro medio. Solicitó igualmente que se estableciera un procedimiento formal y efectivo para garantizar que las versiones definitivas de los documentos publicados en el sitio Internet del Parlamento tengan en cuenta las modificaciones introducidas por los servicios encargados de la elaboración de los mismos.

Se recibió una reclamación relativa a la comunicación de los números de empleados de los miembros del personal de una agencia a todos los usuarios, a través de las direcciones internas de correo electrónico. La finalidad de este tratamiento específico consistía en invitar a todos los miembros del personal a fijar una cita con el departamento de seguridad de la agencia para ser fotografiados. El SEPD consideró que para lograr estos fines hubiera bastado con que la lista enviada incluyese el nombre y apellidos de las personas afectadas. La inclusión en dicha lista de los números de empleados no era pertinente y resultaba excesiva con relación a los fines perseguidos, lo que constituía una infracción del artículo 4 del Reglamento. El SEPD invitó a la agencia a impartir instrucciones oficiales al personal que maneja los datos personales para que trabaje de forma selectiva y ponga un cuidado especial en los envíos masivos de mensajes de correo, internos o externos, que contengan datos personales, de forma que se garantice la inclusión únicamente de los datos pertinentes para los fines del mensaje.

Un miembro del personal presentó una reclamación contra la videovigilancia realizada ocultamente en su institución. En particular, cuestionó la legalidad de la utilización de una videocámara que le grababa, sin su conocimiento, siempre que entraba en el despacho de su jefe en ausencia de este último. El SEPD concluyó que la institución no había demostrado que existiesen fundamentos jurídicos que contemplasen explícitamente la realización de estas operaciones altamente intrusivas y definiesen las condiciones y garantías oportunas. A falta de un fundamento jurídico transparente y de un procedimiento estructurado, existían dudas acerca de la proporcionalidad de dicha videovigilancia oculta. Por consiguiente, el SEPD invitó a la institución a reconsiderar si convenía seguir recurriendo a la vigilancia oculta en el futuro y, en caso afirmativo, a presentar sus planes al SEPD para su control previo.

2.4.5. Actuaciones posteriores relativas a las reclamaciones

El SEPD ha tratado de facilitar el proceso de presentación de reclamaciones y de acelerar su tramitación mediante un **formulario de reclamación en línea** disponible en su sitio web (véase la sección 5.6.1). Desde primeros de 2010 se encuentra disponible en ese sitio una versión provisional del formulario, aunque la versión definitiva será más interactiva. El SEPD confía en que el uso generalizado de esta aplicación ayudará a los reclamantes a comprobar si su reclamación reúne las condiciones para ser admitida a trámite, sometiendo de este modo al SEPD únicamente los asuntos procedentes. Por otro lado, se espera obtener así una información más completa y relevante que permita tramitar las reclamaciones con mayor eficacia, reduciendo el número de las que son claramente inadmisibles.

Está previsto igualmente revisar el manual de procedimientos internos para la tramitación de reclamaciones, adoptado en 2009. Los procedimientos modificados incluirán la nueva estructura organizativa del SEPD y clarificarán el flujo de trabajo interno de las reclamaciones.

2.5. Control del cumplimiento

*El SEPD tiene atribuida la función de supervisar y **garantizar la aplicación del Reglamento (CE) nº 45/2001**. La supervisión se ha efectuado principalmente mediante un **ejercicio de notificación** denominado «Primavera de 2009». Además de este ejercicio de control general, se realizaron controles específicos en los casos en que el SEPD, en el desempeño de sus funciones de supervisión, consideró que existían motivos de preocupación acerca del grado de cumplimiento por parte de determinadas instituciones u organismos. Algunos de estos controles se efectuaron por correspondencia, mientras que otros revistieron la forma de **visitas** de un día de duración al organismo correspondiente, al objeto de analizar los posibles incumplimientos. Por último, se llevaron a cabo **inspecciones** en determinadas instituciones y organismos para verificar el cumplimiento en determinadas aspectos.*

2.5.1. Acciones específicas de control y notificación

El SEPD puso en marcha intervenciones de control específicas por correspondencia en los casos en que existían motivos de preocupación acerca del cumplimiento del Reglamento por parte de una institución o agencia. Así sucedió, por ejemplo, con las investigaciones administrativas internas del BCE o con las operaciones de tratamiento de la DG RELEX.

Investigaciones administrativas internas – Banco Central Europeo

En enero de 2010, el SEPD abrió un expediente sobre la protección de datos personales en la tramitación de las investigaciones administrativas internas del Banco Central Europeo (BCE). Se adoptó esta decisión en virtud del artículo 46, letra b), del Reglamento, y como consecuencia del dictamen de 22 de diciembre sobre tales investigaciones del BCE. Las investigaciones se centraron en el posible acceso a los ficheros electrónicos y a la interceptación de las conversaciones telefónicas. Se remitieron al BCE diversas preguntas relacionadas con la aplicación de la circular administrativa nº 01/2006 sobre las investigaciones administrativas internas y sus principios. Algunas de estas preguntas se referían a la forma de documentar el procedimiento, a la presencia o ausencia de un protocolo informático forense y a las estadísticas anuales de interceptación de las conversaciones telefónicas y de acceso a los ficheros electrónicos y a los datos de tráfico. Este expediente sigue aún abierto.

Inventario de la DG RELEX

A raíz de diversas reclamaciones, el SEPD se preocupó por la posibilidad de que el inventario de operaciones de tratamiento bajo la responsabilidad de la DG RELEX no reflejase exactamente el alcance de dichas operaciones en relación con los datos personales en las delegaciones europeas. Por otra parte, el SEPD deseaba comprobar si la DG RELEX había notificado todas las operaciones de tratamiento de las delegaciones al RPD de la Comisión en cumplimiento del artículo 25. Como consecuencia de esta actuación, la DG RELEX aportó datos y garantías adicionales, por lo que se archivó el expediente.

Visita a la Agencia Europea de Seguridad de las Redes y de la Información

El 17 de septiembre de 2010, el SEPD inspeccionó la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) para comprobar y discutir el nivel de conformidad con el Reglamento (CE) nº 45/2001. La inspección se llevó a cabo a raíz de los diversos indicios recogidos por el SEPD en su labor de supervisión, es decir, una reclamación, una consulta y la falta de seguimiento del anterior dictamen de control previo.

La inspección sirvió asimismo para que el RPD informase al SEPD acerca de los progresos realizados por la ENISA en esta materia, entre ellos un registro electrónico, un mecanismo de seguimiento y un nuevo inventario de operaciones. El RPD destacó el problema de la falta de independencia en el ejercicio de las responsabilidades de su cargo, y el Supervisor adjunto hizo referencia al documento sobre los estándares profesionales (adoptado poco después, en octubre de 2010) que debería permitir al RPD fortalecer y clarificar sus cometidos dentro de la institución.

Durante la reunión de clausura, ambas partes acordaron una hoja de ruta de supervisión basada en los requisitos planteados por el SEPD, en la que se destacaba la importancia de los tres principales mecanismos para el cumplimiento del Reglamento: el inventario, el registro y las notificaciones al SEPD

mencionadas en el artículo 27. El SEPD vigilará estrechamente los progresos realizados por la ENISA en la aplicación de la hoja de ruta, a fin de garantizar el cumplimiento del Reglamento.

Visita a la Agencia Europea de Medio Ambiente

El 10 de diciembre de 2010, el SEPD realizó una visita la Agencia Europea de Medio Ambiente (AEMA) con el fin de comprobar y comentar el nivel de cumplimiento del Reglamento por parte de la misma.

La visita adoptó la forma de una reunión del SEPD con el Director de la AEMA, seguida de otras reuniones con el RPD y con los encargados de las operaciones de tratamiento. En estas reuniones, el SEPD tuvo la oportunidad de manifestar sus preocupaciones sobre los niveles de cumplimiento de la AEMA, y ésta, a su vez, le puso al corriente de sus progresos hacia la plena conformidad. En este contexto, el SEPD constató con satisfacción los importantes esfuerzos realizados por la Agencia, así como el empeño puesto para solucionar las deficiencias.

Ambas partes convinieron una hoja de ruta para el cumplimiento (con plazos específicos), que será objeto de una atenta vigilancia por parte del SEPD.

2.5.2. Vigilancia y elaboración de informes de carácter general: ejercicio «Primavera de 2009»

En el marco del ejercicio de control general iniciado en la primavera de 2009, el SEPD siguió supervisando la aplicación de las normas y principios de protección de datos en las instituciones y organismos participantes.

Las **instituciones de la UE** siguieron manifestando **buenos progresos** en el cumplimiento de las obligaciones de protección de datos que les incumben, mientras que en **las agencias** se constató, por lo general, **un nivel de cumplimiento inferior**, aun cuando algunas también consiguieron mejoras.

En los casos en que el SEPD consideró que los progresos en la vía del cumplimiento eran insuficientes, se establecieron los objetivos apropiados. Es de lamentar que algunas de las organizaciones inspeccionadas no alcanzaran dichos objetivos, por cuyo motivo el SEPD solicitó nuevos informes de actualización. En los casos en que no se recibieron estos informes o en los que se consideró que los progresos eran demasiado lentos, el SEPD procedió a realizar acciones de control más específicas (véase anteriormente).

Resultados actualizados del ejercicio «Primavera de 2009»

- **Notificación al RPD de las operaciones de tratamiento por parte de los responsables de los datos:** por regla general, el número de notificaciones ha aumentado, y el SEPD, al tiempo que sigue tratando de averiguar los avances realizados, investigará a las instituciones y organismos que no alcancen el nivel de cumplimiento requerido, de acuerdo con su documento de orientación, recientemente publicado, sobre el control y la garantía del cumplimiento.
- **Notificación al SEPD de las operaciones de tratamiento para su control previo:** la mayoría de las instituciones han realizado avances significativos en este aspecto, aunque, una vez más, el nivel de cumplimiento por parte de las agencias sigue siendo inferior, por lo que el SEPD tratará de abordar este problema a lo largo del presente año.

2.5.3. Próximos pasos

El SEPD fomentará y supervisará atentamente los avances ulteriores, especialmente en las instituciones y agencias en las que sea preciso mejorar el cumplimiento en lo relativo al control previo por parte del SEPD y a las notificaciones al RPD. Seguirá insistiendo igualmente en la conveniencia de elaborar un **inventario de operaciones** y un plan de **seguimiento interno de sus recomendaciones** dirigidas a garantizar el cumplimiento del Reglamento.

El próximo ejercicio de control general (**Primavera de 2011**) comenzará en los primeros meses de 2011, aunque como resultado de los elementos de prueba recogidos en los ejercicios anteriores es probable que deban realizarse nuevas actuaciones específicas en el ámbito del cumplimiento.

2.5.4. Inspecciones

Las inspecciones son una herramienta fundamental que permite al SEPD supervisar y garantizar la aplicación del Reglamento, estando basadas en su artículo 41, apartado 2, artículo 46, letra c), y artículo 47, apartado 2.

Las amplias facultades de acceso a toda la información y datos personales necesarios para sus investigaciones y a cualquier local donde el responsable del tratamiento o las institución u organismo de la UE lleven a cabo su actividad permiten garantizar que el SEPD dispone de las herramientas precisas para desempeñar su función. El SEPD puede iniciar las inspecciones a raíz de una reclamación, o bien por iniciativa propia.

El artículo 30 del Reglamento insta a las instituciones y organismos de la UE a cooperar con el SEPD en el cumplimiento de sus obligaciones y a facilitarle la información y el acceso que solicite.

Durante las inspecciones, el SEPD **procede a comprobar los hechos sobre el terreno** con el objetivo adicional de garantizar el cumplimiento. Las inspecciones van seguidas de la correspondiente comunicación de las conclusiones a la institución u organismo inspeccionado.

Durante 2010 el SEPD continuó con el seguimiento de las inspecciones anteriores. Por otro lado, en diciembre de 2010 realizó una inspección en el Centro Común de Investigación de la Comisión Europea (JRC), situado en Ispra.

Las inspecciones son una herramienta fundamental para supervisar y garantizar la aplicación del Reglamento sobre protección de datos.

Seguimiento de la inspección de la Oficina Europea de Selección de Personal

En marzo de 2009, el SEPD llevó a cabo una inspección en la Oficina Europea de Selección de Personal (EPSO). Tenía como objetivo investigar las operaciones de tratamiento de datos personales que ya habían sido objeto de controles previos y que estaban relacionadas con la selección de funcionarios, agentes temporales y contractuales, así como cualquier otra operación de tratamiento de datos personales asociada. El SEPD formuló una serie de observaciones, en particular sobre la transparencia de los procedimientos y la conservación de los datos, que posteriormente fueron tenidas en cuenta por la EPSO.

Otro objetivo de la inspección era verificar el cumplimiento de la legislación en el caso de **determinadas bases de datos y herramientas informáticas de la EPSO** utilizadas para los procedimientos de selección. El SEPD sigue a la espera de ulteriores precisiones sobre los progresos realizados en la aplicación de sus recomendaciones, motivo por el cual se reserva la formulación de las conclusiones definitivas de esta inspección hasta que reciba la información pendiente.

Seguimiento de la inspección del Tribunal de Cuentas Europeo

A raíz de la inspección del Tribunal de Cuentas Europeo (TdC) realizada por el SEPD en marzo de 2009 en relación con la aplicación de **control del personal** (herramienta de Internet para el control y las auditorías), la cooperación establecida con el Tribunal ha dado sus frutos, y el SEPD ha podido constatar los avances realizados en el cumplimiento de los asuntos revisados.

Por cuanto se refiere al **asunto relativo al control de Internet** (asunto 2008-0284), el SEPD planteó recomendaciones específicas en su informe de seguimiento del dictamen emitido. Continúan las conversaciones encaminadas a lograr la plena conformidad, dentro del marco general del examen de esta cuestión en el ámbito institucional.

Respecto a la consulta acerca de un procedimiento para acceder a los dispositivos de almacenamiento y/o a los correos electrónicos privados del personal, el SEPD concluyó que era necesario presentar una notificación formal de control previo relativa a esta operación de tratamiento, ya que podía suponer un riesgo específico a la luz de lo dispuesto en el artículo 27, apartado 1, del Reglamento. En enero de 2010, el SEPD emitió un dictamen (asunto 2009-0620) autorizando estas operaciones de tratamiento con sujeción a algunas recomendaciones específicas, que posteriormente fueron aplicadas por el TdC. En consecuencia, el SEPD procedió a archivar el asunto.

Seguimiento de la inspección de la red s-TESTA

La red s-TESTA (Servicios Transeuropeos Seguros de Telemática entre Administraciones) ofrece una infraestructura general que atiende a las necesidades de gestión y de intercambio de información entre las administraciones nacionales y europeas.

En la actualidad, más de 30 aplicaciones se basan en esta red segura que facilita la Comisión Europea.

En enero de 2010, el SEPD emitió un dictamen con 22 recomendaciones referidas a la inspección realizada previamente en el Centro Operativo y de Servicios (SOC) de s-TESTA. En diciembre de 2010, la Comisión envió al SEPD un informe de ejecución relativo a estas recomendaciones, indicando que ya se habían aplicado doce de ellas. Las diez restantes, que requerían una inversión más importante, se habían incluido en el plan de mejora continua del sistema para ser completadas en 2011. El SEPD verificará estos aspectos pendientes durante una acción de seguimiento programada para mediados de 2011.

Inspección del Centro Común de Investigación

En diciembre de 2010, el SEPD llevó a cabo una inspección sobre el terreno en el Centro Común de Investigación (JRC) de Ispra. La decisión de realizar esta inspección obedeció a una ausencia general de colaboración por parte del JRC, unida a la necesidad de comprobar la realidad de los hechos y de verificar *in situ* el cumplimiento de sus recomendaciones.

Se inspeccionaron principalmente dos áreas: la selección y contratación del personal de JRC y los procedimientos aplicados por el servicio de seguridad (control de seguridad de los antecedentes, investigaciones de seguridad, control de accesos y grabación de las llamadas de emergencia). Se disponía de información sobre todos estos aspectos, obtenida en los anteriores análisis de control previo.

Durante la inspección se estableció una colaboración productiva entre el SEPD y los departamentos relevantes del JRC, lo que permitió a los inspectores llegar, entre otras, a la conclusión de que la falta de colaboración anterior había obedecido sobre todo a problemas de comunicación. Basándose en estas conclusiones, el SEPD emitirá un informe de inspección con nuevas recomendaciones dirigidas a lograr un mejor cumplimiento del Reglamento.

2.6 Consultas sobre medidas administrativas

2.6.1. Consultas relativas al artículo 28, apartado 1, y al artículo 46, letra d)

*El Reglamento (CE) n° 45/2001 establece que se informará al SEPD cuando se elaboren medidas administrativas relacionadas con el tratamiento de datos personales (artículo 28, apartado 1). El SEPD puede emitir dictámenes, bien a **petición** de la institución u organismo, bien a **iniciativa propia**.*

Por «medida administrativa» debe entenderse toda decisión de aplicación general adoptada por la administración y relacionada con el tratamiento de datos personales por la institución u organismo en cuestión (por ejemplo, medidas de aplicación del Reglamento, o medidas y políticas internas de aplicación general adoptadas por la administración en relación con el tratamiento de datos personales).

Además, las funciones del SEPD en materia de asesoramiento tienen, según el artículo 46, letra d), del Reglamento, un ámbito de aplicación material muy amplio, ya que abarcan «todos los asuntos relacionados con el tratamiento de datos personales». Esta es la base de las actividades del SEPD en materia de asesoramiento a las instituciones y organismos sobre casos concretos de operaciones de tratamiento, o sobre cuestiones genéricas de interpretación del Reglamento.

En el marco de las consultas relativas a las medidas administrativas proyectadas por las instituciones u organismos comunitarios, se han planteado múltiples cuestiones, algunas de las cuales se describen a continuación.

2.6.2. Solicitud de acceso a la identidad de un informante – Defensor del Pueblo Europeo

El Defensor del Pueblo Europeo consultó al SEPD sobre un problema surgido en una denuncia presentada contra la OLAF. Dicha consulta incluía una serie de preguntas, como las siguientes:

- si la identidad de las personas que proporcionan información a la OLAF, como los informantes o denunciantes, puede ser revelada a terceros distintos de las autoridades judiciales;

- si es preciso garantizar la protección de los informantes y denunciantes una vez cerrada la investigación cuando no existe un seguimiento posterior y, en caso afirmativo, en qué forma y con qué alcance.

En los comentarios formulados por el SEPD se abordan las normas y políticas en su globalidad, no estando relacionados con la denuncia específica dirigida contra la OLAF. El SEPD adoptó la posición de que, con carácter general, no se debe revelar la identidad del denunciante o informante, salvo que ello infrinja las normas nacionales o procedimientos judiciales, y/o en los casos de falsedad en las declaraciones. En tales casos, los datos se pueden revelar exclusivamente a las autoridades judiciales.

En cuanto a la segunda pregunta, el SEPD concluyó que existían buenas razones para creer que la protección de los denunciantes e informantes debe continuar tras el cierre de una investigación, independientemente de que continúen o no las actuaciones. La situación de vulnerabilidad de los denunciantes e informantes, y por consiguiente los riesgos para su intimidad e integridad, no varían según que la investigación siga abierta o se haya cerrado sin actuaciones ulteriores.

En la práctica, es evidente que un planteamiento de este tipo no excluye las situaciones en que la protección de los denunciantes o informantes no debe prevalecer sobre las pretensiones legítimas de terceros. El tiempo transcurrido puede ser un factor relevante, pero es obvio que resulta difícil especular sobre este aspecto de manera abstracta.

2.6.3. Transferencias internacionales de datos personales – Agencia Europea de Seguridad Aérea

La Agencia Europea de Seguridad Aérea (EASA) lleva a cabo determinadas actividades (por ejemplo servicios en el ámbito de la certificación) que dan lugar al pago de tasas y otros cargos por parte de los solicitantes. Estas actividades de certificación pueden llevarse a cabo parcialmente fuera del territorio de los Estados miembros. En algunos casos, los solicitantes han pedido a la Agencia los nom-

bres y datos de viaje de los expertos, con el fin de proceder al pago de los importes facturados.

El RPD de la EASA solicitó el asesoramiento del SEPD sobre la aplicabilidad del artículo 9 del Reglamento al caso sometido a consideración.

En virtud del artículo 9, apartado 1, los datos personales solo se podrán transmitir a destinatarios distintos de las instituciones y organismos comunitarios y no sujetos al Derecho nacional adoptado en aplicación de la Directiva 95/46/EC, **cuando se garantice un nivel de protección suficiente** en el país del destinatario.

El SEPD hizo hincapié en que, si el tercer país en cuestión, no perteneciente al EEE, no garantiza un nivel de protección suficiente, será preciso tomar en consideración las restantes condiciones indicadas en el artículo 9. El artículo 9, apartado 6, estipula que «no obstante lo dispuesto en los apartados 1 y 2, la institución o el organismo comunitario podrán efectuar una transmisión de datos personales si: (...) d) la transmisión es necesaria o requerida legalmente por razones importantes de interés público (...)».

Dado que, en el presente caso, la realización de dichos servicios es una de las actividades básicas de la EASA, las transmisiones de datos efectuadas para facilitar el pago de tales servicios debe considerarse, en principio, **necesarias para el funcionamiento de este organismo,** por lo que se justifica la excepción prevista en el artículo 9, apartado 6, letra d).

El SEPD señaló igualmente que, en el presente caso, aparentemente las transmisiones de datos no tenían carácter «repetido, masivo o estructural», sino que se efectuaban «de una en una» a distintos destinatarios de diferentes países. En lo tocante a los riesgos para los titulares de los datos, no se mencionó riesgo específico alguno. Los tipos de datos transmitidos (el nombre y la fecha de viaje de los expertos en cuestión) no parecían suscitar tampoco problemas particulares.

El SEPD señaló, sin embargo, que no se habían establecido garantías para los casos en que se aplicaba alguna excepción. Por este motivo, recomendó incluir una cláusula especificando que el destinatario estaba autorizado legalmente para recabar estos datos y que el uso de los mismos quedada limitado exclusivamente a los motivos por los que se realizaba dicha transmisión.

2.6.4. Política sobre el uso interno del correo electrónico – Comisión Europea

La Comisión Europea elevó una consulta al SEPD en relación con la política aplicada sobre el uso interno del correo electrónico. El SEPD analizó los aspectos de esta política referidos específicamente a la protección de los datos personales y a los principios en materia de intimidad, así como las medidas de seguridad.

En este contexto, la Comisión informó al SEPD que no realiza controles masivos a nivel individual. En un escrito enviado al SEPD, afirmó que «*la única modalidad de control ordinario que se aplica al servicio de correo electrónico de la Comisión (DG DIGIT) tiene lugar a nivel de DG o de servicio. y no a nivel de los buzones de correo electrónico o de tráfico de datos individuales. La DG DIGIT vigila el uso con el fin de reducir los riesgos operativos, pero no se elaboran informes rutinarios relativos a la actividad de correo individual ni se suministran datos individuales de tráfico que pudieran servir para detectar abusos a nivel individual*».

Lo anterior implica que el control de los buzones individuales de correo **únicamente** se podrá realizar si **forma parte de una investigación en marcha**. El SEPD acogió con satisfacción este planteamiento, por considerar que se ajusta a las buenas prácticas.

2.6.5. Privilegios de acceso del administrador de las TI – Banco Europeo de Inversiones

El 26 de marzo de 2010, el SEPD respondió a una consulta del Banco Europeo de Inversiones (BEI) formulando algunas recomendaciones relativas al acceso de los administradores de las TI a los datos personales almacenados en los sistemas y programas informáticos. El SEPD insistió en la necesidad de aplicar el **principio de segregación de funciones.** El alcance de esta segregación deberá definirse a la luz del nivel de riesgo identificado para el proceso en cuestión.

Los derechos de acceso del administrador de las TI deberían aplicarse a través de una combinación equilibrada de medidas organizativas y técnicas. El SEPD recomendó igualmente que tales medidas se documenten adecuadamente en una política de seguridad detallada definida por la institución.

2.6.6. Vigilancia de las conversaciones telefónicas

Se consultó al SEPD en relación con un proyecto que incluía la vigilancia de las comunicaciones telefónicas cuya duración excediese de un límite predefinido.

El sistema proyectado se basaba en asignar al personal un determinado límite máximo (número de horas o coste de las comunicaciones telefónicas autorizados). Al término de cada mes, los directivos recibirían una lista de los empleados de su departamento cuyo uso del teléfono durante el mes para llamadas (tanto particulares como profesionales) al extranjero o a móviles hubiera superado el límite establecido.

El SEPD reconoció que la legalidad del tratamiento de tales datos está amparada por el ejercicio legítimo del poder público conferido a la institución u organismo a efectos de comprobar el uso autorizado del sistema de telecomunicaciones (artículo 5, letra a), del Reglamento, complementado con los dispuesto en el artículo 37, apartado 2, del mismo). Sin embargo, el SEPD consideró igualmente que no siempre es necesario recurrir a una vigilancia de tipo global, en lugar de efectuar un control más selectivo.

Aunque el SEPD aceptó que la gestión presupuestaria era un objetivo legítimo, estimó que la vigilancia del uso del teléfono para conversaciones particulares, incluso sin obtener información sobre los detalles de las llamadas realizadas, podría ser considerada una violación del derecho a la intimidad de los miembros del personal.

A este respecto, el SEPD solicitó que la institución u organismo se cerciore de que el límite establecido que genera el envío de una lista a los directivos sea lo suficientemente elevado para evitar la vigilancia injustificada, y que la identificación de las personas se lleve a cabo exclusivamente en los casos en que se produzcan abusos evidentes o repetidos del sistema. Se invitó también a la institución u organismo a examinar la posibilidad de utilizar otros indicadores para detectar los posibles abusos.

En consecuencia, el SEPD pidió a la institución que volviese a evaluar el sistema propuesto y que comprobase la posibilidad de utilizar otros métodos menos intrusivos.

2.6.7. Tratamiento posterior de los datos transmitidos a AMEX – Agencia Europea de Seguridad Alimentaria

La Agencia Europea de Seguridad Alimentaria (EFSA) realiza el tratamiento de las declaraciones de intereses (DoI) anuales de determinadas personas que intervienen en sus actividades, al objeto de

La vigilancia del uso del teléfono para fines privados debe considerarse, en principio, una vulneración del derecho a la intimidad de los miembros del personal.

verificar si hay conflictos de intereses que pudieran interferir con tales actividades.

Con ocasión del control previo de estas operaciones de tratamiento de datos (asunto 2008-0737), el RPD de la EFSA solicitó el asesoramiento del SEPD sobre el tratamiento posterior de la base de datos de DoI con el fin que su agencia de viajes AMEX pudiera conocer los datos de los expertos externos.

El RPD de la EFSA preguntó al SEPD si el tratamiento posterior de los datos incluidos en la base de datos de DoI para permitir a la agencia de viajes identificar a los expertos externos sería conforme con el artículo 4, apartado 1, letra b), del Reglamento.

Según esta disposición, los datos personales deben recogerse con fines determinados, explícitos y legítimos, y no ser tratados posteriormente de manera incompatible con dichos fines.

En su dictamen, el SEPD concluyó que todo tratamiento posterior por parte de la EFSA de los datos incluidos en su base de datos de DoI con el fin de transmitir los datos identificativos de las personas que pudieran utilizar los servicios de AMEX se destinaría a una **finalidad completamente distinta**, no siendo compatible con el objetivo original de la recogida y tratamiento de los datos. Por lo tanto, dicho tratamiento posterior por parte de la EFSA no sería conforme con el artículo, 4, apartado 1, letra b), del Reglamento.

Por otra parte, el SEPD señaló que la función y las responsabilidades de AMEX respecto a los datos no se habían aclarado suficientemente en el acuerdo sobre protección de datos suscrito por las partes, no quedando claro, en particular, los motivos por los que AMEX actuaba como encargado y/o responsable del tratamiento, ni las circunstancias en que podía ejercer tales funciones. Se deben establecer las salvaguardias adecuadas para proteger los derechos de los titulares de los datos y para evitar ulteriores transmisiones de AMEX a otros destinatarios, de conformidad con la legislación vigente sobre protección de datos.

2.6.8. Plazos de conservación de los documentos de carácter médico – Colegio de Jefes de Administración

En noviembre de 2006, el Presidente del Colegio de Jefes de Administración (el Colegio) solicitó la opinión del SEPD sobre una nota elaborada por la Comisión relativa a los plazos de conservación de terminados documentos de tipo médico. El SEPD emitió un dictamen el 26 de febrero de 2007 aclarando que el período de 30 años indicado en la nota no debe tomarse como el plazo *mínimo* de conservación para los documentos relacionados

El plazo de conservación de 30 años para los documentos médicos debe considerarse como el máximo admisible.

con la salud. Por el contrario, con pocas excepciones, se ha de considerar como el plazo *máximo* durante el cual deberán conservarse dichos datos. Por otro lado, el SEPD sostuvo que la aplicación de las disposiciones del artículo 4 del Reglamento implica la necesidad de analizar la naturaleza de los documentos médicos con el fin de determinar los plazos de conservación más convenientes para cada tipo de documento.

El problema de la conservación de los documentos médicos surgió de nuevo en septiembre de 2010, cuando el *Comité de Préparation pour les Affaires Sociales* (el CPAS), subcomité del Colegio responsable de estos temas, elaboró un informe sobe una serie de casos con plazos específicos para la conservación de los documentos de tipo médico. En octubre de 2010, el Colegio consultó al SEPD en relación con este informe. El SEPD está examinando actualmente el asunto y emitirá su dictamen sobre la consulta teniendo en cuenta su dictamen anterior de febrero de 2007 y su posición en los dictámenes de control adoptados previamente.

2.6.9. Normas de desarrollo relativas al Responsable de la Protección de Datos

El Reglamento sobre protección de datos requiere que cada institución u organismo de la UE adopte ulteriores ***normas de desarrollo relativas a las tareas, obligaciones y facultades de los RPD.*** *En julio de 2010, el SEPD publicó* ***directrices*** *dirigidas a facilitar la elaboración de normas de desarrollo en los casos en que aún no se hubieran adoptado, o cuando fuera preciso revisarlas.*

En mayo de 2010, la Agencia Ejecutiva del Consejo Europeo de Investigación (ERCEA) sometió a consulta del SEPD sus normas de desarrollo sobre la función del RPD. Estas normas abarcaban también las funciones de los responsables del tratamiento y las reglas para el ejercicio de sus derechos por parte de los titulares de los datos. El SEPD acogió con satisfacción este planteamiento integral, sobre todo teniendo en cuenta que la ERCEA había adoptado las buenas prácticas que el SEPD había estado sugiriendo a lo largo del tiempo, entre ellas las siguientes:

- mantener un inventario anónimo de las solicitudes por escrito de cada interesado relativas al ejercicio de alguno de sus derechos (acceso, rectificación, bloqueo, etc.);
- colaborar con los servicios de TI y de seguridad informática de la Agencia para complementar las fuentes de información a disposición del RPD.

También la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) y el Tribunal de Cuentas sometieron sus normas de desarrollo a la consulta del SEPD, de conformidad con las directrices publicadas por este.

2.7. Directrices temáticas

La experiencia reunida en la aplicación del Reglamento sobre protección de datos ha permitido al personal del SEPD traducir sus conocimientos en directrices genéricas para las instituciones y organismos en los ámbitos de la contratación de personal, los datos de salud, las investigaciones administrativas, los procedimientos disciplinarios y la videovigilancia. El SEPD está elaborando actualmente las directrices para la evaluación del personal y el tratamiento de los datos personales en el marco de la lucha contra el acoso en el trabajo.

2.7.1. Directrices relativas a las investigaciones administrativas y procedimientos disciplinarios

En abril de 2010, el SEPD publicó directrices relativas al tratamiento de datos personales en las investigaciones administrativas y procedimientos disciplinarios realizados por las instituciones y organismos comunitarios.

El objetivo de estas directrices consistía en armonizar las buenas prácticas en este ámbito y facilitar el cumplimiento de las disposiciones del Reglamento. Las directrices presentan, de forma clara y concisa, las conclusiones de las posiciones adoptadas por el SEPD en sus anteriores dictámenes de control previo. Incluyen asimismo una serie de recomendaciones relativas a cada uno de los principios básicos del Reglamento.

Una recomendación importante es la relativa al **derecho de acceso y rectificación** del titular de los datos. Aunque tales derechos pueden ser restringidos ocasionalmente, el responsable de los datos deberá garantizar que dichas restricciones sean necesarias y se impongan en cada caso de manera individual. Por otra parte, el responsable

de los datos debe garantizar que tanto el derecho de acceso y rectificación como el de información sigan garantizándose por otros medios.

El SEPD señaló igualmente que la falta de una estrategia armonizada en cuanto al **plazo de conservación de los datos de tipo disciplinario** daba lugar a conflictos con los principios de protección de datos y otros derechos fundamentales del titular de los datos. Esto se debía a una serie de lagunas importantes en el Anexo IX del Estatuto de los funcionarios y a la ausencia de una política común sobre la conservación de este tipo de datos por parte de las instituciones y organismos de la UE.

Por último, el SEPD hizo hincapié en la necesidad de seguir estudiando el problema específico de la **interceptación de las comunicaciones,** insistiendo especialmente en el fundamento jurídico para el registro de las comunicaciones de voz y la posibilidad de hacerlo sin un orden o autorización judicial.

Aunque las agencias deberán aplicar estas directrices en sus notificaciones al SEPD sobre los procedimientos en esta materia sujetos a control previo, también deben utilizarse como guía de utilidad práctica para todas las instituciones y organismos. El próximo paso consistirá en que el SEPD emitirá un dictamen conjunto sobre las notificaciones de control previo presentadas por las agencias a la luz de estas directrices.

2.7.2. Directrices sobre videovigilancia

En marzo de 2010, el SEPD publicó un conjunto de directrices prácticas dirigidas a las instituciones y organismos de la UE sobre el uso responsable de videovigilancia y el establecimiento de unas garantías eficaces. En estas directrices se definían los principios aplicables a la evaluación de la necesidad de recurrir a la videovigilancia, y se ofrecían orientaciones sobre la forma de aplicarla para que la intimidad y otros derechos fundamentales se vieran mínimamente afectados.

En julio de 2009 se publicó un borrador de texto para consulta, como se indicaba en el Informe anual del SEPD correspondiente a 2009. El proceso de consulta produjo respuestas enfocadas a la mejora de las directrices propuestas y a una mayor cooperación con las partes interesadas.

Las decisiones sobre si se pueden instalar o no videocámaras y sobre el modo de utilizarlas no deben basarse únicamente en consideraciones de seguridad, sino que es preciso **hallar un equilibrio entre los requisitos de la seguridad y los derechos fundamentales de las personas.** Sin embargo, los derechos fundamentales y la seguridad no tienen por qué ser mutuamente excluyentes. Aplicando un enfoque pragmático basado en los principios de selectividad y proporcionalidad, los sistemas de videovigilancia pueden satisfacer las necesidades de seguridad sin dejar de respetar la intimidad.

Dentro de los límites establecidos por las normas sobre protección de datos, cada institución y organismo dispone de un margen discrecional al diseñar su propio sistema. Las directrices tratan de ayudar a llevar a cabo esta personalización. Dicha flexibilidad debe excluir una interpretación rígida o burocrática de los principios de la protección de datos que impida atender los requisitos de seguridad justificados y perseguir otros objetivos legítimos.

Al mismo tiempo, las instituciones deberán poder **demostrar que han establecido procedimientos para garantizar el cumplimiento** de los requisitos de la protección de datos. Entre las medidas organizativas recomendadas se incluye la adopción de un conjunto de garantías de protección de datos que deberán definirse en la política sobre videovigilancia de la institución, realizando periódicamente auditorías dirigidas a verificar su cumplimiento. Se insta a las instituciones a realizar evaluaciones de impacto, teniendo en cuenta que sigue siendo necesario el control previo del SEPD para la videovigilancia que implique niveles de riesgo elevados (como la vigilancia encubierta, o los sistemas de vigilancia de tipo dinámico-preventivo).

Las instituciones de la UE tienen de plazo hasta el 1 de enero del 2011 para demostrar que cumplen las directrices del SEPD.

Período transitorio

Las directrices se aplicaban tanto a los sistemas actuales como a los futuros, y las instituciones disponían de plazo hasta el 1 de enero de 2011 para ajustar sus prácticas con el fin de alcanzar la plena conformidad. El SEPD continuó ofreciendo asesoramiento en los casos en que se necesitaban recomendaciones adicionales sobre cuestiones específicas.

También prestó ayuda a las instituciones que ya habían enviado sus notificaciones de control previo antes de la publicación de las directrices, lo que sucedió en nueve casos. En julio de 2010, el SEPD publicó sus recomendaciones preliminares relativas a dichos casos, si bien su adopción no podía considerarse un sustitutivo del análisis interno detallado realizado por la propia institución acerca de las directrices, las prácticas empleadas y el nivel de cumplimiento. Los comentarios del SEPD debían servir de ayuda a las instituciones afectadas para centrar su atención en los temas claves que requerían una solución. Entre estos se encontraban la vigilancia encubierta y los plazos de conservación.

De forma similar, el SEPD emitió también un directriz preliminar dirigida a la OLAF, cuyo sistema de videovigilancia era el único controlado previamente por él antes de la publicación de las directrices (debido a que se trataba de una auténtica notificación de control previo relacionada con un nuevo sistema, debiendo recibir como tal un tratamiento prioritario).

El SEPD siguió facilitando orientación a otras instituciones en relación con la interpretación y aplicación de las directrices, y continuó tramitando las reclamaciones y consultas, entre ellas una relativa a las prácticas de vigilancia encubierta en una institución y otra relativa al uso de grabaciones de videovigilancia como elemento de prueba en una investigación administrativa, cuando tales grabaciones habían sido obtenidas infringiendo las normas sobre protección de datos.

2.8. Política del SEPD en materia de cumplimiento y aplicación

En diciembre de 2010, el SEPD publicó un documento de orientación titulado «Control y garantía del cumplimiento del Reglamento (CE) nº 45/2001».

En él se anuncia un cambio de rumbo radical en lo relativo a la aplicación de las disposiciones del Reglamento. Hasta la fecha, el SEPD ha preferido formular recomendaciones e invitar a cumplirlas, en lugar de dirigir advertencias o amonestaciones a los responsables del tratamiento, o de emitir órdenes de obligado cumplimiento. Después de cinco años de actuaciones de esta clase, el SEPD cree llegado el momento de adoptar una **estrategia de mayor severidad en materia de aplicación,** especialmente en los casos de incumplimiento grave, deliberado y repetido de los principios de la protección de

datos. Por consiguiente, con la nueva política se introduce una serie de criterios para garantizar una aplicación anticipativa, así como coherente y transparente, de sus facultades al respecto.

El documento define el marco de actuación en el que el SEPD controla, mide y garantiza el cumplimiento de las normas de protección de datos dentro de la administración de la UE. En el mismo se describen las características de las diversas facultades de aplicación conferidas al SEPD y se describen las causas y circunstancias que pueden dar lugar a la adopción de medidas formales.

La política aplicada trata de estimular el **cumplimiento voluntario y las buenas prácticas,** creando incentivos para ello a través de:

- la insistencia en señalar a los responsables del cumplimiento:
- la explicación de la forma en que el SEPD apoya dicho cumplimiento, y
- la información sobre las medidas que en SEPD adoptará en caso de incumplimiento.

También se hace un gran hincapié en el **principio de «asunción de responsabilidades»**, con objeto de estimular al cumplimiento y a la adopción de las buenas prácticas dentro de la administración comunitaria. La asunción de responsabilidades requiere que las instituciones y organismos de la UE, así como los responsables del tratamiento que actúan en su nombre, apliquen medidas apropiadas y eficaces para garantizar el cumplimiento de las obligaciones en la esfera de la protección de datos, y justifiquen que lo han hecho ante el SEPD.

Finalmente, el documento describe la estrategia del SEPD en relación con la **transparencia y la publicidad** en el contexto de las medidas de aplicación, destacando la importancia de estos instrumentos tanto para las propias partes interesadas como para la mejora de la gobernanza. Por lo tanto, en el futuro el SEPD publicará con carácter general la información relativa a todos los asuntos remitidos oficialmente al Parlamento, al Consejo, a la Comisión o al Tribunal de Justicia. Por otro lado, analizará en cada caso concreto la conveniencia de publicar cualquier de sus restantes medidas de aplicación.

El SEPD confía en que, al permitirle desempeñar mejor sus responsabilidades en materia de control y garantía del cumplimiento en virtud de un enfoque de la aplicación selectivo, focalizado y basado en los riesgos, este documento de orientación contribuirá a un uso más eficaz y eficiente de los recursos.

El SEPD considera que ha llegado el momento de aplicar una estrategia de mayor severidad en materia de aplicación.

3 CONSULTA

3.1. Introducción: visión general y principales tendencias durante el año

En 2010 la Comisión llevó a cabo avances importantes en la creación de un nuevo **marco jurídico para la protección de datos en Europa.** Se concluyó la consulta pública iniciada en 2009, complementándola con una serie de consultas específicas a varias partes interesadas importantes.

En noviembre de 2010, la Comisión publicó su Comunicación relativa a un enfoque global de la protección de los datos personales en la Unión Europea, en la que se identifican las principales prioridades y objetivos para la revisión de las normas actualmente en vigor.

Este proyecto ocupó un lugar destacado en la agenda del SEPD durante 2010 y será una de sus principales prioridades para los próximos años.

Por otra parte, la Comisión Europea dedicó también esfuerzos considerables en 2010 a la **aplicación del Programa de Estocolmo, -** una Europa abierta y segura que sirva y proteja al ciudadano - adoptado por el Consejo de la UE en diciembre de 2009. El Programa define las orientaciones estratégicas para la planificación de carácter legislativo y operativo en el espacio de libertad, seguridad y justicia, dedicando una atención especial a los intereses y necesidades de los ciudadanos.

*El Programa de Estocolmo puso el acento en que las **medidas de seguridad y de orden público deben ir de la mano del respeto de los derechos fundamentales, entre ellos el de protección de datos**. También insistió en la necesidad de proteger los datos personales en una sociedad global caracterizada por los rápidos cambios tecnológicos y por el intercambio de información sin fronteras.*

El SEPD siguió de cerca las diversas iniciativas relacionadas directamente con la aplicación del Programa de Estocolmo. Entre otros asuntos, abordó los problemas relativos a la protección de datos sensibles, surgidos en el marco de la estrategia de seguridad interior de la UE, la gestión de la información, la política antiterrorista europea y los reglamentos de Frontex y de Eurodac. En general, las actividades relacionadas con el Programa de Estocolmo ocuparon un lugar destacado entre las prioridades del SEPD, y se prevé que lo seguirán ocupando durante los próximos años.

También la **interfaz entre la intimidad y los cambios tecnológicos** ha sido objeto de importantes intervenciones por parte del SEPD. En mayo de 2010, la Comisión publicó una Comunicación relativa a una Agenda digital para Europa, con el objetivo de definir las prioridades de la UE en el mundo de Internet y de las tecnologías digitales. Algunas de estas iniciativas revisten una gran relevancia desde la perspectiva de la protección de datos y son objeto de estrecha vigilancia por parte del SEPD. El SEPD tiene el convencimiento de que las nuevas tecnologías no solo plantean nuevos desafíos en relación con

la intimidad y la protección de datos, sino que ofrecen al mismo tiempo nuevas oportunidades para la protección de los mismos.

Por consiguiente, resulta esencial integrar los requisitos de la intimidad desde el primer momento en las fases de diseño, funcionamiento y administración de los sistemas TIC y a lo largo de todo el ciclo de vida de la información. Por este motivo, el SEPD aboga firmemente por la inclusión del principio de «privacidad por diseño» en el nuevo marco jurídico.

El SEPD fue consultado también acerca de varias iniciativas en el ámbito de la **cooperación internacional en materia de seguridad y de orden público** como el acuerdo entre la UE y Estados Unidos sobre la protección de datos, y el intercambio de información financiera dentro del Programa de Seguimiento de la Financiación del Terrorismo (TFTP II). Ha participado igualmente en el Acuerdo Comercial de Lucha contra la Falsificación (ACTA) y en los acuerdos sobre utilización de datos del registro de nombres de los pasajeros (PNR).

El SEPD intervino igualmente en otras áreas, como los intercambios masivos de datos realizados en el contexto del Sistema de Información del Mercado Interior, el uso de escáneres de seguridad en los aeropuertos y la cooperación en el terreno de la fiscalidad.

La amplia diversidad de ámbitos de la política sobre los que se formularon consultas al SEPD demuestra que el tratamiento de datos se ha convertido en un aspecto esencial de un número creciente de iniciativas legislativas que a menudo plantean problemas graves en materia de protección de datos y que, por ende, justifican la labor continuada del SEPD como órgano asesor de las instituciones europeas.

3.2. Marco normativo y prioridades

3.2.1. Aplicación de las directrices del SEPD en materia de consulta

Aunque los métodos de trabajo del SEPD en el ámbito de la consulta han ido evolucionando con el tiempo, el enfoque básico de las intervenciones no ha cambiado. El documento de orientación «El Supervisor Europeo de Protección de Datos como asesor de las instituciones comunitarias para las propuestas legislativas y documentos conexos»[8] sigue vigente, si bien debe ser leído a la luz del Tratado de Lisboa.

Los dictámenes formales del SEPD, basados en el artículo 28, apartado 2, o en el artículo 41 del Reglamento (CE) nº 45/2001, constituyen sus principales instrumentos, y representan un análisis exhaustivo de todos los elementos relacionados con la protección de datos contenidos en una propuesta de norma comunitaria u otros instrumentos pertinentes.

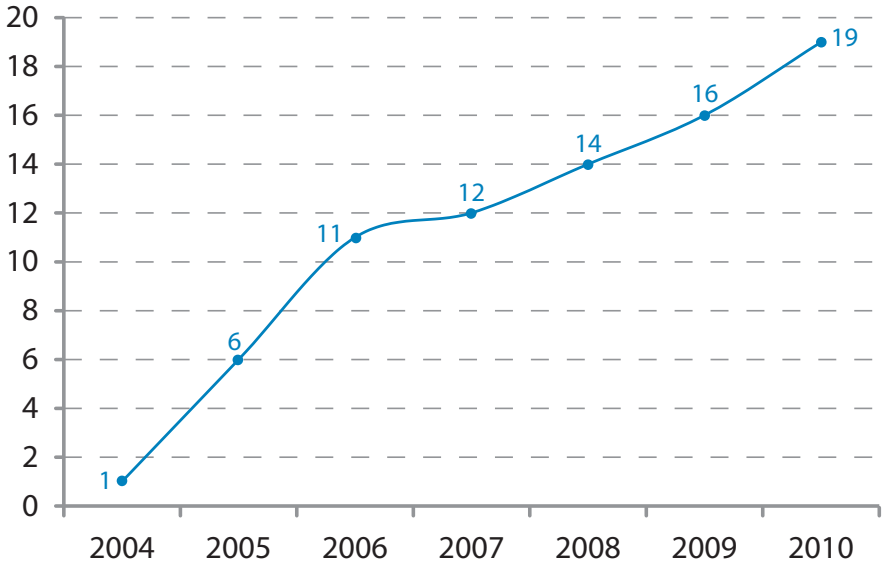
Por regla general, el SEPD emite dictámenes sobre textos que no tienen carácter legislativo (como son los documentos de trabajo, comunicaciones o recomendaciones de la Comisión), cuando la protección de datos constituye un elemento esencial de los mismos. Ocasionalmente, el SEPD formula por escrito observaciones de alcance más limitado, con el fin de comunicar un mensaje político rápido y referido a los aspectos esenciales, o de sintetizar o reiterar observaciones realizadas con anterioridad.

También puede servirse de otros medios, como las presentaciones orales, las cartas aclaratorias, las conferencias y los comunicados de prensa. Por ejemplo, en 2010 convocó una conferencia de prensa sobre el «futuro del marco jurídico de la UE para la protección de datos», con motivo de la presentación del Informe anual 2009.

El SEPD está presente en todas las fases del proceso de definición de políticas y de desarrollo legislativo, y en su capacidad asesora utiliza un amplio abanico de instrumentos. Aunque para ello se requiere un estrecho contacto con las instituciones de la UE, la

[8] En dos de estos casos (la revisión del Reglamento (CE) nº 831/2002 relativo al acceso con fines científicos a datos confidenciales, y la Decisión marco del Consejo sobre los ataques contra los sistemas de información), no se consideró necesario formular un dictamen en esta fase.

Evolución de los dictámenes legislativos 2004-2010



salvaguardia de su independencia es en todo momento la preocupación fundamental.

Los contactos con la Comisión tienen lugar en las diferentes fases de la preparación de las propuestas, variando su intensidad en función del tema y también del enfoque adoptado por los servicios de la Comisión. Esto se aplica especialmente a los proyecto a largo plazo, como son los relativos a la iniciativa sobre justicia electrónica o la revisión del marco jurídico para la protección de datos, a la que el SEPD ha contribuido en sus distintas etapas.

También se mantuvieron contactos regulares con los servicios de las instituciones implicadas en la fase de seguimiento. En algunos casos, el SEPD y sus agentes participaron intensamente en los debates y negociaciones desarrollados en el Parlamento y en el Consejo. En otros, la Comisión desempeñó en papel de interlocutor principal en la fase de seguimiento. El proceso legislativo relacionado con la legislación sobre Frontex, el seguimiento de la Agenda digital (por ejemplo en el tema de la neutralidad de la red) y el Sistema de Información del Mercado Interior son ejemplos de esta implicación que dio lugar a la emisión de observaciones complementarias por parte del SEPD durante el año 2010.

3.2.2. Resultados de 2010

En 2010 se mantuvo el incremento continuo en el número de dictámenes. El SEPD emitió 16 dictámenes sobre un amplio abanico de temas.

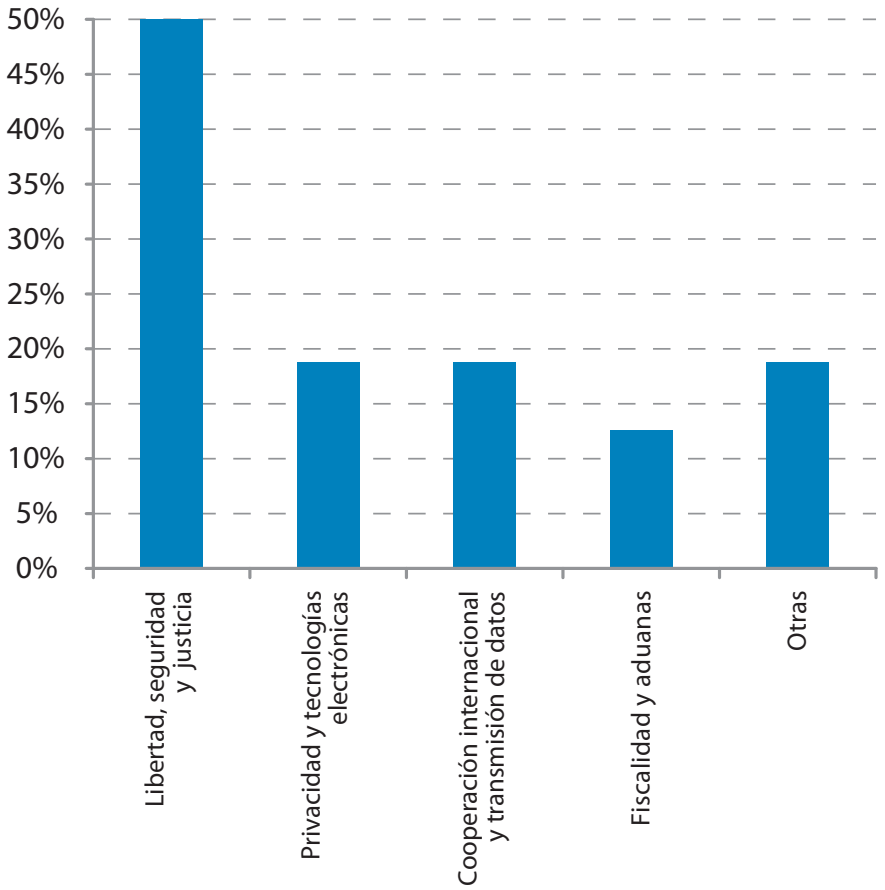
En estos dictámenes y en las restantes iniciativas de intervención, el SEPD aplicó las prioridades establecidas para 2010, tal como se reflejan en su inventario. Los 19 dictámenes se referían a distintas áreas de la política.

El inventario de 2010 definió cuatro ámbitos de atención principales:

- el nuevo marco jurídico para la protección de datos;
- el espacio de libertad, seguridad y justicia;
- la cooperación internacional y la transferencia de datos, y
- los avances tecnológicos.

El SEPD dedicó una gran atención a estos aspectos durante 2010. De acuerdo con el programa de actividades para 2010, se concentró sobre todo en las iniciativas a las que se había asignado una alta prioridad (es decir, las marcadas en rojo): el SEPD emitió un dictamen o se manifestó de algún otro modo en

Principales áreas de la política de los dictámenes legislativos de 2010



trece de los quince proyectos de alta prioridad desarrollados a lo largo de 2010.(9)

A continuación se describe con mayor detalle el contenido de los dictámenes del SEPD y de sus restantes contribuciones relacionadas con las consultas.

3.3. Revisión del marco jurídico de la UE para la protección de datos

La revisión del marco jurídico de la UE en materia de protección de datos era ya una de las principales prioridades del SEPD en 2009, año en que dio comienzo el debate oficial sobre la reforma. En 2010, el interés por la reforma aumentó de forma importante con la publicación, en noviembre de este año, de la Comunicación de la Comisión relativa a un enfoque global de la protección de los datos personales en la UE. El SEPD dedicó una atención particular a esta cuestión a lo largo de 2010, formulando sus opiniones a través de diversas vías.

El nuevo marco para la protección de datos debe ser ambicioso y contribuir realmente a la eficacia de los instrumentos de protección de datos en una sociedad globalizada y gobernada por la tecnología.

(9) En dos de estos casos (la revisión del Reglamento (CE) nº 831/2002 relativo al acceso con fines científicos a datos confidenciales, y la Decisión marco del Consejo sobre los ataques contra los sistemas de información), no se consideró necesario formular un dictamen en esta fase.

En particular, organizó una **conferencia de prensa** sobre este tema inmediatamente después de publicada la Comunicación, al objeto de expresar públicamente su punto de vista sobre el nuevo marco jurídico. En dicho acto, el SEPD hizo hincapié en la importancia de la revisión realizada, que consideraba sumamente oportuna, y comentó los aspectos más destacados del nuevo marco.

*El SEPD insistió en la necesidad de una **protección de datos sólida y eficaz**, en una sociedad que hace uso de la información en cantidades incalculables, y muchas veces sin el conocimiento de los interesados. El SEPD acogió con satisfacción la Comunicación de la Comisión, pero señalando que **no había margen para el error**, porque los desafíos son enormes y las soluciones propuestas tienen que ser, por un lado, **ambiciosas**, y por otro capaces de mejorar la eficacia de los mecanismos de protección de datos.*

El SEPD expresó igualmente su opinión sobre los puntos más destacados del nuevo marco, en particular:

- su respaldo al objetivo de la ulterior **armonización** de la legislación nacional sobre protección de datos;
- la necesidad de un planteamiento **tecnológicamente neutral**;
- la inclusión de los principios de **privacidad por diseño y asunción de responsabilidades**;
- la introducción de una **notificación obligatoria de las violaciones de la seguridad** para todos los sectores afectados, y
- la **inclusión de las áreas de policía y justicia** en el marco general.

El SEPD siguió desarrollando estos temas en un extenso dictamen que emitió en enero de 2011.

Se prevé que la Comisión elaborará una propuesta legislativa de gran alcance durante 2011, por lo que el SEPD seguirá observando de cerca el proceso legislativo y hará las nuevas aportaciones que considere apropiadas.

3.4. El espacio de libertad, seguridad y justicia

A lo largo de 2010, el SEPD dedicó una especial atención a todas las novedades surgidas en la aplicación del **Programa de Estocolmo,** y formuló recomendaciones sobre una serie de iniciativas, tanto legislativas como de otro tipo, relacionadas directa o indirectamente con el espacio de libertad, seguridad y justicia.

3.4.1. Estrategia de Seguridad Interior

La Estrategia de Seguridad Interior (ESI) de la UE define el modelo de seguridad europeo que integran las actividades en materia de cooperación policial y judicial, gestión de las fronteras y protección civil. La ESI, aprobada por el Consejo en febrero de 2010 y ratificada por el Consejo Europeo un mes más tarde, fue seguida en noviembre de 2010 de una Comunicación de la Comisión en la que se abordaban las amenazas más urgentes para la seguridad europea, como la delincuencia organizada, el terrorismo, la ciberdelincuencia, la gestión de las fronteras exteriores de la UE y las catástrofes humanitarias.

Debido al carácter **potencialmente intrusivo** de las medidas que es preciso adoptar en el marco de la EIS, el SEPD siguió de cerca el debate sobre este tema y las acciones previstas para su implantación. En su dictamen de diciembre de 2010, el SEPD destacó la necesidad de garantizar un **equilibrio**

El SEPD reclamó una Estrategia de Seguridad Interior eficiente, apoyada por un sólido plan de protección de datos que la complemente.

adecuado entre la seguridad de los ciudadanos y la protección eficaz de su intimidad y datos personales. El SEPD hizo también una llamada de atención sobre el hecho de que la EIS presenta evidentes **nexos de carácter político con otras estrategias** que se están desarrollando actualmente en el ámbito de la UE, como la Estrategia de Gestión de la Información y la revisión del marco jurídico para la protección de datos.

El SEPD abogó por un **planteamiento más amplio e integrado de la EIS,** en el que contemplen los vínculos e interacciones entre las distintas iniciativas. Adoptó la posición de que no sería posible instaurar una EIS eficiente sin contar con el apoyo de un sólido plan de protección de datos que la complemente.

3.4.2. Gestión de la información

El Programa de Estocolmo instaba a la Comisión a sopesar la necesidad de desarrollar un Modelo Europeo de Intercambio de Información, basándose en la evaluación de los actuales instrumentos en este terreno. El Programa mencionaba también que un **régimen de protección de datos de mayor solidez** era un requisito previo para la Estrategia de Gestión de la Información de la UE. En julio de 2010, la Comisión publicó una **Comunicación sobre el panorama general de la gestión de la información** en el espacio de libertad, seguridad y justicia, sobre la cual el SEPD emitió un dictamen en septiembre de ese mismo año.

El SEPD respaldó plenamente los trabajos en curso para la evaluación de todos los mecanismos relacionados con la gestión de la información en el espacio de libertad, seguridad y justicia. Puso de relieve que esta iniciativa representaba un **primer paso en el proceso de evaluación,** instando a llevar a cabo un **examen objetivo, completo y detallado** de todos los instrumentos utilizados actualmente en el marco de la Estrategia de Gestión de la Información, antes de proponer otros nuevos.

El SEPD sugirió asimismo que en los futuros trabajos sobre gestión de la información se analizasen teniendo en cuenta las deficiencias y puntos débiles que presentan los sistemas actuales.

3.4.3. FRONTEX

En febrero de 2010, la Comisión presentó una **propuesta de revisión del marco jurídico que regula el FRONTEX,** al objeto de reforzar las capacidades operativas de la Agencia. En el dictamen emitido en mayo de 2010, el SEPD analizó las nuevas funciones de la Agencia y sus consecuencias para la protección de datos.

El SEPD se mostró especialmente crítico con el hecho de que la propuesta no especificase si se permitiría al FRONTEX tratar datos personales y en qué medida. El SEPD invitó al legislador a definir unas normas precisas sobre protección de datos, y a clarificar las condiciones y circunstancias en que FRONTEX podría realizar dicho tratamiento de datos.

También siguió atentamente el debate sobre este proyecto en el seno del Parlamento Europeo. En un escrito dirigido al ponente del Parlamento, formuló sugerencias concretas con el fin de introducir en la propuesta un **fundamento jurídico específico** que resuelva este problema, con **sólidas garantías respecto a la protección de los datos** y respetando los principios de proporcionalidad y necesidad.

Los datos personales relacionados con sospechas no confirmadas de actividades terroristas no deben conservarse por tiempo indefinido.

3.4.4. Política antiterrorista

La lucha contra el terrorismo es un área en la que los datos personales acostumbran a tratarse de forma masiva y preventiva.

En su dictamen sobre la política antiterrorista de la UE, el SEPD reclamó **iniciativas concretas** de apoyo a los derechos fundamentales en este ámbito, y en particular el derecho a la protección de los datos personales. Subrayó la necesidad de garantizar la **coherencia** y la claridad de las relaciones entre todas las políticas e iniciativas en materia policial y de seguridad interior. Recomendó asimismo que el legislador europeo **potenciase el papel de la protección de datos en esta área.** En particular, todas las propuestas deben tener en cuenta de manera explícita el **principio de necesidad.** De este modo se evitaría la aparición de posibles duplicidades con los instrumentos existentes y la recogida e intercambio de datos personales se limitaría a lo realmente necesario para la finalidad perseguida.

Además, sería necesario proponer una estrategia completa y global en el terreno de las **medidas de bloqueo de activos** dirigidas a países específicos y a sospechosos de terrorismo, con vistas a garantizar tanto la eficacia de las acciones policiales como el respeto de los derechos fundamentales. En relación con la cooperación internacional, el SEPD recuerda la necesidad de asegurar que se establezcan salvaguardias apropiadas cuando se intercambien datos personales con terceros países y organismos internacionales, con el fin de garantizar que los derechos de los ciudadanos a la protección de los datos se respeten de manera adecuada en este contexto.

3.4.5. Comercialización y utilización de precursores de explosivos

Desde el punto de vista de la protección de datos, la recopilación de informaciones sobre transacciones sospechosas de determinados productos químicos constituye el aspecto más delicado de la propuesta de la Comisión relativa a la comercialización y a la utilización de precursores de explosivos. El principal objetivo de las medidas propuestas consiste en reducir el riesgo de que los terroristas u otros delincuentes perpetren atentados utilizando artefactos explosivos de fabricación artesanal. El SEPD solicitó aclaraciones sobre las disposiciones pertinentes, con el fin de garantizar que el **tratamiento de los datos siga siendo proporcionado y se eviten los abusos.**

Garantizar un nivel elevado de protección de los datos contribuye asimismo a la lucha contra el racismo, la xenofobia y la discriminación, lo que, a su vez, puede contribuir a prevenir la radicalización y la captación para fines terroristas.

Las principales recomendaciones del SEPD fueron las siguientes:

- **Los datos no deben utilizarse para un propósito distinto** de la lucha contra el terrorismo (u otros delitos que entrañen el uso indebido de productos químicos para la fabricación de artefactos explosivos artesanales).

- **Los datos no deben conservarse durante largos períodos,** especialmente si el número de destinatarios de los datos, potenciales o reales, es importante y si estos últimos van a utilizarse para la extracción automatizada de datos (*data mining*). Ello es aún más importante en los casos en los que se pueda demostrar que la sospecha inicial fue infundada. El SEPD solicitó que el Reglamento estableciese un plazo máximo de conservación (que en principio no debería exceder de los dos años) para todos los datos personales relativos a las transacciones calificadas como sospechosas.

- **Debe prohibirse expresamente el tratamiento de categorías especiales de datos,** a fin de evitar prácticas discriminatorias, como la elaboración de perfiles basados en la raza o religión.

3.4.6. Reglamento Eurodac

En su dictamen publicado en diciembre de 2010, el SEPD se centró en el problema del «**fallo en el registro**» (que en este contexto concreto significa la imposibilidad de obtener huellas digitales legibles de un solicitante de asilo). El SEPD insistió en el principio de que el fallo en el registro no debería suponer por sí solo la denegación de los derechos de los solicitantes de asilo. En particular, rechazó enérgicamente la presunción de que la persona cuyas huellas dactilares no puedan leerse haya tratado *ipso facto* de frustrar el procedimiento de identificación, por ejemplo mediante la automutilación.

El dictamen constató con satisfacción que **en el proyecto actual se había eliminado la posibilidad de permitir a los organismos policiales el acceso a EURODAC.**

El SEPD formuló recomendaciones relacionadas con la información sobre el titular de los datos, desde el momento que la precaria situación de los solicitantes de asilo o inmigrantes ilegales constituía un motivo añadido para facilitarles información clara y práctica sobre sus derechos. El dictamen abordó asimismo la utilización de las mejores técnicas disponibles como método para implementar la «privacidad por diseño», así como las consecuencias derivadas de la subcontratación (parcial) a un tercero del desarrollo o gestión del sistema.

Son ya varios los dictámenes del SEPD que han abordado este tema. Las recomendaciones formuladas en este dictamen se refieren a nuevos acontecimientos o recomendaciones anteriores que todavía no han sido plenamente aplicadas.

3.4.7. Abusos sexuales a menores y pornografía infantil

En mayo de 2010, el SEPD emitió un dictamen acerca de una propuesta de Directiva de la Comisión relativa a la lucha contra los abusos y la explotación sexual de menores y la pornografía infantil.

En la misma insistió en la necesidad de garantizar la **seguridad jurídica** de todas las partes implicadas, incluidos los proveedores de servicios de Internet (ISP), las víctimas y los usuarios de la Red.

Aunque la propuesta mencionaba la necesidad de tener en cuenta los derechos fundamentales de los usuarios finales, el SEPD consideraba que se debería incluir en la misma la obligación de los Estados miembros de garantizar unos **procedimientos armonizados, claros y detallados,** sometidos al **control de organismos públicos independientes,** en la lucha contra los contenidos ilegales.

El SEPD no cuestiona la necesidad de adoptar un marco mejorado con medidas apropiadas para proteger a los niños contra el abuso. Sin embargo, llama la atención sobre los **efectos** de algunas de las medidas, como el bloqueo de los sitios web y la creación de teléfonos de emergencia, y sobre los **derechos fundamentales a la protección de la intimidad y de los datos** de las personas afectadas. El problema planteado no se refería específicamente a la lucha contra el abuso de menores, sino a cualquier iniciativa relacionada con la colaboración del sector privado para fines policiales.

3.4.8. La Orden Europea de Protección y la Orden Europea de Investigación

Las iniciativas de algunos Estados miembros relacionadas con una Directiva sobre la Orden Europea de Protección (EPO) y la Orden Europea de Investigación (EIO) se basan en el Programa de Estocolmo y contemplan el intercambio de datos personales entre los Estados miembros implicados. Mientras que la EPO pretende mejorar la protección de las víctimas de actos delictivos (en particular de las mujeres), con la EIO se trata de crear un instrumento unificado, eficiente y flexible para obtener los elementos de prueba que se encuentran en otro Estado miembro de la UE.

En su dictamen, el SEPD hizo hincapié en que el tratamiento de datos personales, especialmente en el ámbito sensible de la libertad, seguridad y justicia, debe realizarse de conformidad con las normas de la UE sobre protección de datos.

La protección eficaz de los datos personales no sólo es importante para los interesados, sino que contribuye igualmente al éxito de la propia cooperación judicial, fortaleciéndola mediante el reconocimiento mutuo y la mejor calidad de los datos intercambiados.

Entre las diversas recomendaciones, el SEPD defendió la adopción de las salvaguardias adecuadas para garantizar la protección de las personas en

relación con el tratamiento de datos personales, la imparcialidad en los procedimientos y el debido respeto de los principios de confidencialidad y secreto profesional. En particular, el SEPD insistió en la necesidad de garantizar que: 1) los sistemas de autenticación solamente permitan que accedan a los datos las personas autorizadas; 2) se efectúe un seguimiento de los accesos y de las operaciones, y 3) se apliquen controles de auditoría.

Este dictamen representó asimismo una oportunidad importante para que el SEPD pudiese destacar la necesidad de establecer **procedimientos específicos** en orden a garantizar que se eleva también la correspondiente **consulta al SEPD** cuando los Estados miembros introduzcan iniciativas relacionadas con el tratamiento de datos personales.

3.5. La protección de la intimidad en las comunicaciones y tecnologías electrónicas

3.5.1. Fortalecimiento de la confianza en la sociedad de la información

En mayo de 2010, la Comisión Europea aprobó la Agenda digital, una estrategia compuesta por un conjunto de políticas y acciones destinadas a fomentar la economía digital en el horizonte de 2020. Como contribución a esta estrategia, el SEPD publicó en marzo de 2010 su dictamen acerca de la «Promoción de la confianza en la sociedad de la información mediante el impulso de la protección de datos y la intimidad».

En el mismo se recalcaba que la confianza del consumidor constituye un elemento esencial para que surjan y se desarrollen las tecnologías de la información y la comunicación (TIC), de las que la identificación por radiofrecuencia (RFID), las redes sociales y los sistemas de salud y de transporte electrónico son tan solo algunos ejemplos.

Esta confianza solo podrá generarse si las TIC son fiables y seguras, si están sometidas al control de los usuarios y si se garantiza la protección de los datos personales y la intimidad de estos.

La UE posee un sólido marco regulador en materia de protección de datos que, en principio, debe garantizar que los datos de los ciudadanos se encuentran debidamente protegidos. Sin embargo, en muchos casos las TIC plantean nuevos problemas que no están contemplados en el marco jurídico vigente. En el dictamen se analizan las medidas que la UE podría aplicar o promover para reforzar dicho marco. En particular, el SEPD instó a la Comisión Europea a emprender las acciones siguientes:

- Incluir el principio de «**privacidad por diseño**» como **norma de obligado cumplimiento** en el actual marco jurídico en materia de protección de datos. La privacidad por diseño debería contar con el pleno respaldo de la Agenda digital europea y constituir un elemento obligatorio de las políticas de la UE en el futuro, como por ejemplo el transporte electrónico, la administración electrónica, etc.

- Aplicar el principio de privacidad por diseño, de acuerdo con una estrategia definida específicamente, en las tres **áreas de las TIC que presentan riesgos específicos** para la protección de la intimidad y de los datos: a) **RFID**: proponer medidas legislativas para regular las principales cuestiones que plantea el uso de la RFID, en caso de que la autorregulación no logre los resultados esperados (por ejemplo, permitiendo la elección en el punto de venta); b) **Redes sociales**: contemplar la obligatoriedad de la «intimidad por defecto» en su configuración; c) **Publicidad personalizada**: incluir en los buscadores la configuración de intimidad por defecto, de modo que a los usuarios les resulte más fácil dar su consentimiento para recibir publicidad.

3.5.2. Internet y la neutralidad de la Red

En junio de 2010, la DG INFSO inició una consulta pública sobre la Internet abierta y la neutralidad de la Red en Europa. En dicha consulta se plantearon diversas cuestiones relacionadas con las políticas de gestión del tráfico utilizadas por los operadores de redes y por los ISP para gestionar el tráfico de datos de un modo determinado.

En sus comentarios de respuesta a la consulta de la DG INFSO, el SEPD destacó los problemas relacionados con la protección de los datos y la intimidad que pueden surgir a raíz de las actividades de gestión de tráfico por parte de los ISP y operadores de redes.

Puso de relieve dos aspectos relacionados con la implantación de los mecanismos de gestión del tráfico: en primer lugar, permite a los proveedores de servicios examinar el contenido de los mensajes o transmisiones y, en segundo lugar, les da la posibilidad de relacionar esta información con un usuario concreto. El SEPD subrayó la necesidad de tener debidamente en cuenta el marco regulador europeo para la protección de datos, antes de embarcarse en estas actividades. Recordó, en particular, que dicho marco regulador exige el **consentimiento libre e informado** de los usuarios, y facilitó directrices prácticas sobre los requisitos para obtener tal consentimiento.

3.5.3. Directiva sobre la conservación de datos

En ocasión de una conferencia organizada por la Comisión en diciembre de 2010, el SEPD pronunció una alocución en la que se refirió a la Directiva de conservación de datos como «el momento de la verdad», argumentando a favor de aprovechar la oportunidad para **demostrar claramente la necesidad y justificación** de la misma.

La Directiva sobre la conservación de los datos implica que las empresas de comunicaciones electrónicas (compañías de telefonía fija y móvil, proveedores de servicios de Internet) tienen la obligación de conservar los datos del tráfico, de la dirección y otros datos del abonado para fines de investigación, detección y procesamiento judicial.

El SEPD hizo hincapié en que esta invasión masiva de la intimidad requería de un sólida justificación. Por consiguiente, invitó a la Comisión Europea a aprovechar el proceso de consulta para **demostrar la necesidad** de la Directiva. Mediante hechos y cifras concretos debería ser posible determinar si los resultados planteados en la evaluación se hubieran podido obtener mediante otros métodos menos invasivos.

La creación o modificación de los instrumentos legislativos de la UE deberían definir sus objetivos con claridad, contribuyendo así a la seguridad jurídica de los ciudadanos. Esto significa que se deberían regular también las modalidades de acceso y uso posterior de los datos por parte de las autoridades policiales, sin dejar margen alguno a los Estados miembros para que puedan utilizarse para otros fines distintos.

Sentencia del Tribunal Constitucional de Alemania

El 2 de marzo de 2010, el Tribunal Constitucional de Alemania **falló en contra de la ley alemana con la que se aplicaba la Directiva sobre conservación de datos**. El Tribunal consideró que el uso de los datos almacenados debía estar sometido a unos requisitos más estrictos que los contemplados por el legislador alemán. En su sentencia, el Tribunal

El SEPD instó a la Comisión a demostrar la necesidad de conservar los datos de comunicaciones a tan gran escala.

formuló asimismo criterios para un acceso y uso más restringido de los datos. Tales criterios deben introducirse en la legislación nacional a fin de garantizar el cumplimiento de la obligación de conservar los datos sin que se vulneren los derechos fundamentales consagrados por la Constitución alemana.

En un comunicado de prensa, el SEPD manifestó que los restantes Estados miembros de la UE debían ver en la sentencia una fuente de inspiración de gran autoridad y una valiosa aportación para la valoración de la Directiva sobre protección de datos, especialmente a la luz del nuevo marco jurídico establecido en el Tratado de Lisboa.

3.5.4. Los residuos electrónicos

La protección de la intimidad y de los datos personales está íntimamente relacionada con las medidas de seguridad de los dispositivos capaces de almacenar datos personales en cantidades cada vez mayores. El SEPD insistió sobre este aspecto en su dictamen de abril de 2010 acerca de la propuesta de la Comisión sobre la versión refundida de la Directiva relativa a los residuos de aparatos eléctricos y electrónicos (también conocidos como *residuos electrónicos*).

Aunque apoya el objetivo de la propuesta de mejorar las políticas de respeto al medio ambiente en lo relativo a los residuos electrónicos, el SEPD señaló, sin embargo, que la iniciativa se centraba exclusivamente en los riesgos medioambientales relacionados con la eliminación de estos residuos, sin tener en cuenta los **riesgos para la protección de datos** que podrían derivarse de una **eliminación inadecuada, reutilización o reciclado** de los residuos de aparatos eléctricos y electrónicos.

Existe un riesgo cada vez mayor de pérdida y dispersión de los datos personales de los usuarios y/o de terceros que permanecen almacenados en los equipos informáticos y de telecomunicaciones (por ejemplo ordenadores personales, ordenadores portátiles y terminales de comunicaciones electrónicas) en el momento de la eliminación de los aparatos.

A la vista de tales riesgos, el SEPD remachó la importancia de adoptar las **medidas de seguridad** apropiadas en cada fase del tratamiento de datos personales, incluyendo la fase de eliminación de los dispositivos que contienen datos personales (de principio a fin).

Por otra parte, sería preciso tener debidamente en cuenta el principio de «**privacidad por diseño**» y, en este contexto, de «**seguridad integrada en el diseño**», al objeto de lograr que las garantías de intimidad y seguridad se integren por defecto en el diseño de los equipos eléctricos y electrónicos.

Los datos personales almacenados en los residuos electrónicos deben ser objeto de una protección adecuada.

3.5.5. Agencia Europea de Seguridad de las Redes y de la Información (ENISA)

En un dictamen publicado en diciembre de 2010, el SEPD manifestó su satisfacción por la ampliación del mandato de la ENISA y de sus funciones actuales, tal como figuraban en la propuesta correspondiente de la Comisión Europea, destacando que la **seguridad de los datos** es un **componente fundamental de la protección de los mismos**. A este respecto, dio su respaldo al objetivo de la propuesta de reforzar las competencias de la Agencia mediante la incorporación de las **autoridades de protección de datos** y los **organismos policiales** como **partes interesadas de pleno derecho**.

El SEPD recomendó una mayor precisión en relación con la ampliación de las tareas de la Agencia al objeto de eliminar cualquier inseguridad jurídica, señalando la necesidad de establecer unos canales de comunicación estables con las partes interesadas, al objeto de garantizar la coherencia y una estrecha cooperación.

Insistió igualmente en la necesidad de incorporar las **recomendaciones de seguridad y las buenas prácticas** en las operaciones internas de la Agencia, lo que permitirá a la ENISA ensayar y aplicar mejor estas medidas en otros organismos y agencias.

El nuevo Reglamento de la ENISA ampliará su mandato a cinco años y reforzará sus competencias.

3.5.6. La justicia electrónica

El SEPD colabora estrechamente con los equipos de expertos de la Comisión y del Consejo que trabajan en el diseño y ejecución del plan de acción para la justicia electrónica. Con esta iniciativa se trata de modernizar y simplificar la comunicación al público de la información de índole jurídica, para que puedan beneficiarse de una «ventanilla única y multilingüe en Internet para cualquier información relacionada con la justicia».

El sitio web fue inaugurado en julio de 2009 con funciones limitadas, estando previsto incorporar los nuevos servicios definidos en la ambiciosa hoja de ruta establecida por el Consejo, que contempla, entre otros, los servicios de información, los pagos por Internet, la orden de pago europea, las reclamaciones de menor cuantía, la búsqueda de profesionales y la recuperación de datos de los registros públicos interconectados.

Puesto que algunos de estos servicios conllevarán probablemente el tratamiento de volúmenes importantes de datos personales, el SEPD ha recomendado, desde el primer momento, la inclusión de las **salvaguardias adecuadas para la protección de los datos** en los instrumentos jurídicos que aporten el fundamento jurídico y en las infraestructura TIC que presta los servicios.

3.5.7. El Séptimo Programa Marco de IDT (investigación, desarrollo tecnológico y demostración) y el proyecto Turbine

En aplicación de las opciones de interacción mencionadas en su documento de orientación de abril de 2008 «El SEPD y la investigación y desarrollo tecnológico en la UE»([10]), el SEPD facilitó en 2010 los contactos y la cooperación entre las autoridades nacionales de protección de datos y los consorcios para proyectos de investigación.

El proyecto TURBINE([11])

En 2008, después de analizar los elementos del proyecto de la UE «*TrUsted Revocable Biometric IdeNtitiEs*» (Identidades biométricas revocables de confianza, Turbine), en el que se llevan a cabo investigaciones relacionadas con las **tecnologías biométricas revocables**, el SEPD decidió atender la solicitud de un consorcio para emitir un dictamen sobre este proyecto europeo([12]). El SEPD confirmó la gran relevancia del proyecto en el ámbito de la protección de datos y consideró que reflejaba las prioridades indicadas en su Informe anual.

Entre mayo y octubre de 2010, el consorcio facilitó al SEPD toda la documentación relativa a los aspectos de protección de datos de las investigaciones realizadas en el marco del proyecto Turbine. El SEPD mantuvo asimismo diversas conversaciones con los representantes del consorcio con el fin de obtener aclaraciones y, en su caso, documentos complementarios. Los modelos de demostración desarrollados por Turbine y puestos en marcha durante el verano de 2010 se consideraron un elemento importante del análisis. Los puntos principales del dictamen del SEPD se presentaron con oca-

([10]) Disponible en el sitio del SEPD en Internet, en Publicaciones > Documentos.

([11]) www.turbine-project.eu

([12]) Véase el Informe anual 2008, p. 70.

sión de la conferencia final sobre el proyecto, celebrada en Bruselas en enero de 2011.

Séptimo Programa Marco: punto de partida para la aplicación del principio de la privacidad por diseño.

3.6. La cooperación internacional y la transmisión de datos

3.6.1. Registros de nombres de pasajeros

Al igual que en años anteriores, en 2010 el tratamiento de los registros de nombres de los pasajeros (PNR) por las autoridades policiales dio lugar a problemas de protección de datos desde una perspectiva europea.

En relación con el **acuerdo PNR con Estados Unidos**, el SEPD reiteró algunas de sus preocupaciones ya manifestadas anteriormente en sus intervenciones ante el Tribunal de Justicia y en los dictámenes emitidos en el contexto del Grupo de trabajo del artículo 29, y que no había sido solucionados satisfactoriamente en la versión definitiva del acuerdo. En particular, insistió en que el acuerdo no está enfocado únicamente a las personas que suponen un riesgo, sino que contempla más bien la recogida masiva de datos personales y la aplicación de análisis de riesgo a todos los pasajeros. Por el contrario, el acuerdo PNR suscrito con Australia presentaba menos problemas relacionados con la intimidad.

El SEPD adoptó también una posición en relación con la propuesta de la Comisión dirigida a definir su **estrategia externa en materia de los PNR**. En esta propuesta se establecen los principios generales, incluida una serie de normas de protección de datos, que deberían incorporarse en todos los acuerdos PNR suscritos con terceros países. En su dictamen, el SEPD acogió con satisfacción el enfoque horizontal adoptado por la Comisión y respaldó firmemente el objetivo de lograr un nivel elevado y armonizado de protección de datos aplicable tanto a los programas PNR existentes como a los que se contemplen en el futuro.

Sin embargo, para que la propuesta resulte aceptable, han de **restringirse considerablemente** las condiciones aplicables a la recogida y tratamiento de los datos PNR. Al igual que ocurrió con el acuerdo PNR con Estados Unidos, el SEPD se mostró especialmente preocupado por el **uso de los programas PNR para los análisis de riesgo y la elaboración de perfiles**. Manifestó una serie de dudas importantes sobre la **necesidad y legitimidad** de algunos aspectos importantes de los regímenes propuestos. En su opinión, el uso anticipativa de los datos PNR de todos los pasajeros para fines de análisis de riesgo requiere una justificación y salvaguardias más explícitas.

En cuanto al contenido de las normas de protección de datos propuestas, el SEPD reclamó una **mayor precisión** en relación con las **garantías mínimas** aplicables a todos los acuerdos PNR. En particular, se deberían aplicar restricciones más severas al tratamiento de datos sensibles, a las condiciones para las transmisiones ulteriores y a la conservación de los datos. Insistió asimismo en la necesidad de que todos los acuerdos PNR contengan disposiciones específicas por las que se reconozcan a las personas, a título individual, **derechos directamente aplicables.**

Para el análisis de riesgos se utilizan datos personales de todos los pasajeros, lo que plantea serias dudas sobre su necesidad y proporcionalidad.

3.6.2. Programa de seguimiento de la financiación del terrorismo

El SEPD planteó importantes salvedades al proyecto de acuerdo con Estados Unidos elaborado por la Comisión Europea relativo al **Programa de seguimiento de la financiación del terrorismo (TFTP)**. Este acuerdo autoriza a las autoridades estadounidenses a acceder a los datos financieros europeos gestionados por la empresa belga **SWIFT** en el marco de las investigaciones destinadas a combatir el terrorismo. A raíz de la decisión del Parlamento Europeo de vetar el acuerdo provisional a mediados de febrero, el nuevo proyecto de acuerdo pretendía abordar las preocupaciones referentes a la intimidad y a la protección de datos.

*El SEPD consideró que no se habían aportado **pruebas suficientes de la necesidad y proporcionalidad de este tipo de acuerdo** intrusivo para la intimidad, que en muchos aspectos se solapaba con otros acuerdos europeos e internacionales ya existentes en este terreno.*

Insistió en que era preciso establecer inequívocamente la **necesidad** del acuerdo propuesto, dada la existencia de otros métodos menos intrusivos para la intimidad (como, por ejemplo, el acuerdo sobre asistencia jurídica mutua entre la UE y los Estados Unidos). Se manifestó especialmente preocupado sobre el plan para permitir la **transmisión de grandes volúmenes de datos bancarios** a las autoridades de Estados Unidos (transferencias masivas).

Además, el dictamen especificó los elementos clave que necesitaban mejoras desde el punto de vista de la protección de los datos, y que eran los siguientes:

- sustituir las **transferencias masivas** por otros mecanismos que permitan el filtrado de los datos financieros en la UE y vigilar para que únicamente se envíen a las autoridades de Estados Unidos los datos relevantes y necesarios;
- reducir considerablemente el **plazo de conservación** de los datos no extraídos y a los que la autoridades no hayan accedido en sus investigaciones relacionadas con el terrorismo;
- confiar la valoración de las solicitudes del Tesoro de Estados Unidos a una **autoridad judicial pública,** de acuerdo con el mandato para la negociación y el actual marco jurídico de la UE en materia de protección de datos;
- garantizar que los **derechos relativos a la protección de datos** de los interesados sean **efectivamente aplicables**, sobre todo en el territorio de Estados Unidos, y
- mejorar los **mecanismos de control** y **supervisión independientes.**

Algunos de estos puntos ya han sido abordados por la Comisión Europea, el Parlamento Europeo y el Consejo en el procedimiento final. El 1 de agosto de 2010 entró en vigor un acuerdo que incluía ligeras modificaciones.

El SEPD expresó su preocupación por el plan para permitir la transmisión de grandes volúmenes de datos bancarios a las autoridades de Estados Unidos.

3.6.3. Acuerdo entre la UE y Estados Unidos sobre el intercambio de información y la protección de los datos personales

El SEPD contribuyó al debate relativo a la redacción de un acuerdo internacional sobre protección de datos entre la UE y Estados Unidos. Este acuerdo debe prever **medidas de salvaguardia de alto nivel** aplicables al intercambio de datos personales en el ámbito de la **cooperación policial y judicial en asuntos penales.**

Desde 2007, el SEPD ha seguido de cerca los trabajos del Grupo de Contacto de Alto Nivel en el que participan representantes europeos y norteamericanos, habiendo contribuido activamente a las distintas fases de los trabajos preparatorios. Emitió un dictamen en noviembre de 2008 y ha intervenido en las reuniones y consultas públicas organizadas por la Comisión. Con respecto al mandato de negociación elaborado por la Comisión, el SEPD apoyó la

inclusión en el proyecto de acuerdo de requisitos esenciales de la protección de datos, como la clara exposición de su finalidad y de su ámbito de aplicación, el conocimiento de derechos aplicables a favor de los interesados y la supervisión independiente.

3.6.4. Acuerdo Comercial de Lucha contra la Falsificación

A lo largo de 2010, la Unión Europea participó en las negociaciones emprendidas con vista a la celebración de un Acuerdo Comercial de Lucha contra la Falsificación (ACTA). El acuerdo, que se adoptó en diciembre de 2010, pretende reforzar la aplicación de los derechos de propiedad intelectual, también en Internet.

Durante las negociaciones, ampliamente criticadas por su falta de transparencia, transcendió que algunas de las cláusulas del borrador de acuerdo podían suponer vulneraciones de los derechos individuales relacionados con la intimidad y la protección de datos.

Al SEPD, que no había sido consultado al respecto en ningún momento, manifestó su preocupación en especial por las presuntas disposiciones del ACTA en las que se legitimaba la ***vigilancia a gran escala de los usuarios de Internet*** *y por la obligación impuesta a los proveedores de servicios de Internet de adoptar «****políticas de desconexión a los tres avisos****»*([13]).

Para aclarar estas dudas, el SEPD emitió un dictamen en febrero de 2010 que incluía las siguientes recomendaciones:

- **investigar otros métodos menos intrusivos para combatir la piratería en Internet:** en opinión del SEPD, para lograr el objetivo de aplicar los derechos de propiedad intelectual no era imprescindible recurrir a las políticas basadas en los tres avisos, por lo que solicitó que se tuviesen en cuentas otras soluciones alternativas menos intrusivas o, al menos, que se redujese el alcance de la vigilancia proyectada, considerando la posibilidad de realizar controles *ad hoc***;**

([13]) Estos políticas implican normalmente la desconexión de Internet después de recibir tres avisos por compartir o descargar materiales protegidos por derechos de autor.

El SEPD manifestó sus dudas sobe las presuntas disposiciones del ACTA en las que se legitimaba la vigilancia a gran escala de los usuarios de Internet.

- **aplicar garantías adecuadas a todas las transmisiones de datos realizadas en el contexto del ACTA**: en la medida en que el ACTA conlleva intercambios internacionales de datos personales entre autoridades y/o organizaciones privadas situadas en los países signatarios, el SEPD instó a la UE a aplicar las garantías apropiadas en todas las transmisiones de datos realizadas en el contexto del ACTA. Dichas garantías deberían revestir la forma de pactos vinculantes entre los emisores de la UE y los destinatarios de terceros países.

3.7. Fiscalidad y aduanas

3.7.1. Cooperación en materia fiscal

El primer dictamen emitido por el SEPD en 2010 se refería a una propuesta de la Comisión para mejorar la cooperación administrativa entre los Estados miembros en materia fiscal. La propuesta versaba sobre los impuestos indirectos, excluidos el IVA y los impuestos especiales, contemplados en otros instrumentos jurídicos.

Uno de los principales objetivos de la propuesta consistía en mejorar el intercambio de información entre los Estados miembros. En la mayor parte de los casos se trata de información sobre personas físicas, por lo que son de aplicación las normas en materia de protección de datos.

En su dictamen, publicado en enero de 2010, el SEPD declaró que la propuesta de la Comisión era un claro ejemplo de **falta de sensibilidad sobre la protección de datos,** aspecto que había sido ignorado casi por completo. A consecuencia de ello, la propuesta contenía varios puntos que no eran conformes con los requisitos de la protección de datos. En el dictamen se resaltaban y analizaban estas deficiencias.

Además de formular otras observaciones, el SEPD invitaba al legislador a acotar con mayor claridad la responsabilidad de la Comisión en relación con el **mantenimiento y seguridad de la red** prevista para el intercambio de información. Le pedía asimismo que definiese mejor los tipos de información personal que se podían transmitir y los fines para los que se podían utilizar, y que valorase la necesidad de tales transmisiones, o como mínimo que garantizase el respeto del principio de necesidad.

3.7.2. Cooperación aduanera entre la UE y Japón

En febrero de 2010, la Comisión adoptó una propuesta relativa a una Decisión del Consejo sobre la posición que la Unión Europea debía adoptar en el seno del Comité Conjunto de Cooperación Aduanera UE-Japón acerca del reconocimiento mutuo de los programas de Operador Económico Autorizado en la Unión Europea y Japón([14]). El artículo IV del Anexo de la propuesta se refería al **intercambio y comunicación de información.** El Anexo contemplaba intercambios sistemáticos de información y datos relacionados a través de medios electrónicos, referidos especialmente a los participantes en los programas.

Tanto la Directiva 95/46/CE en sus artículos 25 y 26, como el Reglamento (CE) nº 45/2001 en su artículo 9, contienen disposiciones análogas en relación con los flujos transfronterizos de datos personales. El principio definido en estas disposiciones implica que **no se pueden transferir datos personales** de un Estado miembros a un tercer país, salvo que este último garantice un **nivel de protección suficiente** (o bien que se adopten las salvaguardias precisas, o que sea de aplicación alguna de las excepciones previstas).

A pesar de que el proyecto de exposición de motivos de la propuesta declaraba que el régimen japonés de protección de datos era adecuado, no se había observado el procedimiento definido en la Directiva para determinar si el tercer país garantizaba un nivel de protección suficiente. Como resultado, la declaración formulada en el proyecto de exposición de motivos constituía una infracción de la Directiva.

El SEPD recomendaba, por tanto, la supresión de la declaración sobre la adecuación del régimen japonés incluida en el punto 5(1) del proyecto de exposición de motivos, desde el momento que no se ajustaba a los requisitos del Reglamento (CE) nº 45/2001 y de la Directiva 95/46/CE. Recomendaba, además, que se examinasen las diversas posibilidades ofrecidas por el Reglamento y la Directiva, con el fin de garantizar el respeto de las normas sobre las transferencias internacionales de datos.

([14]) COM(2010) 55 final.

3.8. Acceso público, incluidos los asuntos judiciales

3.8.1. Acceso público a los documentos que contienen datos personales

Desde el inicio de sus actividades, el SEPD no ha dejado de ocuparse de la relación, a menudo complicada, que existe entre las normas comunitarias sobre el **acceso público a los documentos y** las que regulan la **protección de los datos**. Esta labor se reflejó, en primer lugar, en el asesoramiento prestado a las instituciones de la UE. En 2005, por ejemplo, el SEPD publicó un documento de base sobre este tema, bajo el título «El acceso del público a los documentos y la protección de datos», que contiene directrices para las instituciones y organismos de la UE.

El SEPD defendió igualmente este planteamiento en calidad de parte en el caso judicial más notorio en esta materia, *Bavarian Lager contra la Comisión,* que versaba sobre una solicitud de acceso del público a las actas de una reunión de la Comisión y a los nombres de los participantes y sobre la denegación de ese acceso por aplicación de las normas de protección de datos. Mientras que el tribunal de primera instancia convalidó la posición del SEPD, el Tribunal de Justicia, en su sentencia de 29 de junio de 2010 sobre el recurso presentado, revocó la resolución en primera instancia e interpretó de manera distinta la vigente legislación de la UE.

Una parte del análisis presentado en el documento de base de 2005 ha dejado de tener validez a la luz de esta última sentencia del Tribunal. En consecuencia, el SEPD elaboró un breve documento adicional sobre este tema, que finalizó y publicó en los primeros meses de 2011.

En este documento adicional, el SEPD insiste en la necesidad de un **enfoque anticipativa** de la materia. En síntesis, esto significa que las instituciones deben explicar claramente a los interesados, antes de obtener sus datos personales o a lo sumo en el momento de obtenerlos, hasta qué punto el tratamiento de tales datos incluye o puede incluir su revelación pública. El SEPD sostiene que las instituciones están obligadas a hacerlo en virtud de las buenas prácticas.

El enfoque anticipativo reduce el número de casos en los que las instituciones han de decidir si permiten la revelación de los datos cuando se solicita el acceso público a ellas, como ocurrió en el asunto *Bavarian Lager*. El documento formula recomendaciones sobre la forma de lograr un equilibrio justo, tanto en situaciones de anticipación como de reacción.

Diversos asuntos judiciales pendientes quedaron suspendidos en espera de la sentencia del juicio *Bavarian Lager*. Todos ellos se reactivaron una vez que el Tribunal dictó su sentencia en junio de 2010, y el SEPD intervino en algunos de ellos. Cuando lo estimó procedente, el SEPD aprovechó tales ocasiones para manifestar su punto de vista sobre la aplicabilidad de la sentencia en el asunto *Bavarian Lager* a estas otras situaciones. También aportó estos mismos argumentos en un caso promovido recientemente sobre el mismo tema.

Otra consecuencia de la sentencia *Bavarian Lager* fue la desestimación de la primera demanda presentada contra el SEPD ante un tribunal de primera instancia.

3.8.2. Otras cuestiones judiciales

Otra sentencia que afectó al SEPD fue la dictada el 15 de junio de 2010 por el Tribunal de la Función Pública en el asunto *Pachtitis contra Comisión*. Una de las cuestiones que se dilucidaban era la negativa de la Comisión a permitir al solicitante el acceso a las preguntas de un examen de admisión en el que había participado. Dado que se habían invocado a este respecto las normas sobre protección de datos, y que el asunto planteaba una interesante pregunta sobre si el alcance del derecho de acceso incluía los propios datos personales, el SEPD se personó en el proceso apoyando al solicitante. Aunque la demanda de este último fue aceptada, no se abordó el problema de la protección de datos, por cuyo motivo el SEPD se abstuvo de intervenir en el recurso planteado posteriormente por la Comisión ante el tribunal de primera instancia.

En julio de 2010, el Tribunal de la Función Pública invitó al SEPD a participar en un asunto judicial relativo a la transmisión de datos médicos entre dos instituciones de la UE. Era la primera vez que le invitaba el Tribunal a intervenir de tal forma. El SEPD aceptó la invitación y redactó una declaración en la que explicaba las correspondientes disposiciones del Reglamento sobre protección de datos.

3.9. Otras cuestiones

3.9.1. Sistema de Información del Mercado Interior

En julio de 2010, el SEPD envió un escrito a la Dirección General de Mercado Interior y Servicios (DG MARKT) de la Comisión, recapitulando los logros obtenidos y señalando las metas que aún quedaban por alcanzar en relación con los temas planteados en el Informe de la Comisión relativo a la situación de la protección de datos en el Sistema de Información del Mercado Interior (IMI).

IMI es una aplicación en línea que permite a los Estados miembros cooperar mutuamente para mejorar la aplicación de la legislación sobre el mercado interior. También implica el registro y comunicación de los datos personales correspondientes. En particular, el IMI permite a las autoridades nacionales, regionales y locales de los Estados miembros de la UE comunicarse de forma rápida y fácil con sus homólogos de otros países europeos. Este sistema ayuda a los usuarios a encontrar el organismo apropiado de otro país con el que deben ponerse en contacto, y a comunicarse con éste mediante conjuntos pretraducidos de preguntas y respuestas normalizadas. Está diseñado como sistema flexible, capaz de ser utilizado en relación con muchas de las normas que componen la legislación en materia de mercado único.

El SEPD acogió con satisfacción los progresos realizados hasta el momento y animó a la Comisión a exigir **garantías adicionales,** aplicando el principio de **privacidad por diseño**, y a continuar cooperando en todo lo necesario con las autoridades de protección de datos de los Estados miembros. Es importante destacar que invitó también a la Comisión a adoptar una nueva norma legal, preferiblemente a través del procedimiento legislativo ordinario, para aplicar al IMI unos requisitos de protección de datos más estrictos, con el fin de proporcionar una mayor seguridad jurídica y un nivel de protección superior.

A medida que se expande lel IMI, se necesita un fundamento jurídico sólido y nuevas garantías de protección de datos.

3.9.2. Escáneres de seguridad

En febrero de 2010, un representante del SEPD asistió a los ensayos del escáner de seguridad instalado en el aeropuerto de Schiphol, en los Países Bajos. La visita tenía como objetivo obtener información adicional sobre la denominada «segunda generación de sistemas», con la que se ha intentado mejorar la protección de datos y aplicar el principio de «privacidad por diseño».

En julio de 2010, el SEPD publicó sus comentarios([15]) sobre la Comunicación relativa al uso de escáneres de seguridad en los aeropuertos, adoptada por la Comisión en el mes de junio([16]).

> En estos comentarios, el SEPD hizo hincapié en que el **consentimiento no podía ser utilizado** para legitimar el tratamiento de los datos personales cuando no existía un fundamento jurídico para ello.

Señaló igualmente que, en lo relativo a los escáneres de seguridad, las «**mejores técnicas disponibles**» significan la fase más avanzada y eficaz del desarrollo de las actividades y métodos operativos, concretada en la idoneidad práctica de determinadas técnicas para ofrecer un umbral de detección definido y conforme con el marco europeo en materia de intimidad y protección de datos.

El SEPD seguirá vigilando de cerca los desarrollos legislativos y técnicos relacionados con los escáneres de seguridad y contribuirá de la forma más apropiada a los próximos pasos que la Comisión tiene previsto dar en 2011.

([15]) http://www.edps.europa.eu/edpsweb/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-07-01_Security_scanners_EN.pdf

([16]) Véase COM(2010) 311 final.

Tanto para los escáneres corporales como para los de seguridad, la solución consiste en implantar el principio de la privacidad por diseño.

3.9.3. Programas de garantía de depósitos

Los programas de garantía de depósitos permiten reembolsar los fondos de los depositantes, hasta un máximo de 100 000 euros, en caso de quiebra de la entidad financiera. En Europa existen normas que regulan estos programas desde 1994, y poco después de iniciada la crisis financiera de 2008 se procedió a reforzar estos mecanismos. En julio de 2010, la Comisión presentó otra propuesta para simplificar y armonizar las normas nacionales aplicables en la materia.

El reembolso de los depósitos a través de estos programas de garantía requiere el tratamiento de los datos de los depositantes. Por consiguiente, son de aplicación las normas de protección de datos, siempre que los titulares de los depósitos sean personas físicas. Los datos no sólo se intercambian entre la institución de crédito y el programa de garantía de depósitos, sino también entre estos últimos, ya sea dentro de un Estado miembro o entre Estados miembros distintos.

En 2010, el SEPD emitió un breve dictamen sobre esta propuesta, en el que se declaró satisfecho en general con el tratamiento dado en ella a los aspectos de protección de datos. Por ejemplo, la propuesta garantiza que los datos personales en cuestión solamente se utilicen para los fines que motivan su comunicación, es decir, para el reembolso de los depósitos.

El SEPD se mostró especialmente satisfecho al comprobar que los datos únicamente se pueden utilizar, con un formato anónimo, para llevar a cabo las denominadas «pruebas de resistencia» (*stress tests*). En efecto, durante la fase de elaboración de la propuesta el SEPD había puesto en duda la necesidad de utilizar datos personales para la realización de dichas pruebas.

3.9.4. Iniciativa ciudadana

La iniciativa ciudadana es una de las innovaciones introducidas por el Tratado de Lisboa. Gracias a ella, un grupo de al menos un millón de ciudadanos de la Unión, que sean nacionales de un número significativo de Estados miembros, pueden invitar a la Comisión a que presente una propuesta legislativa sobre una materia de su interés. La reunión de un millón como mínimo de adhesiones implica la recogida de datos personales.

> En su dictamen de abril de 2010, el SEPD destacó que el pleno respeto de las normas de protección de datos contribuiría de manera significativa a la fiabilidad, fortaleza y éxito de este nuevo e importante instrumento.

Una de las recomendaciones se refería a la obligación que incumbe al promotor de una iniciativa en la que se prevea utilizar un sistema de recogida por Internet de solicitar a la autoridad competente que certifique la seguridad de dicho sistema. Por cuanto se refiere al momento en que debe solicitarlo, el SEPD sugirió que se obligue a los promotores a hacerlo *antes* de comenzar la recogida de adhesiones, y no después. Propuso igualmente que el legislador garantizase lo siguiente:

- que los datos personales recogidos por el promotor no puedan ser utilizados para otra finalidad distinta que el apoyo expresado a la iniciativa ciudadana concreta;

- que los datos recibidos por la autoridad competente solo puedan utilizarse para verificar la autenticidad de las declaraciones de apoyo a una iniciativa ciudadana determinada.

3.9.5. Investigación y prevención de accidentes e incidentes en la aviación civil

El Dictamen de SEPD se centró en los aspectos de la propuesta referidos a la protección de los datos personales, incluido el **tratamiento de los datos de las listas de pasajeros, de las víctimas, familias y testigos** durante las distintas fases de la investigación y en el contexto del intercambio de información entre las autoridades de investigación.

El SEPD comprobó con satisfacción que los aspectos relativos a la protección de datos se habían tenido en cuenta en la propuesta. Sin embargo, considerando el **contexto específico** en que se tratan los datos personales – la investigación de accidentes para mejorar la seguridad de la aviación – **se deben introducir garantías adicionales para salvaguardar su confidencialidad.** Habría que adoptar, por tanto, disposiciones para la eliminación o anonimización de los datos personales lo antes posible, una vez que dejen de ser necesarios para una investigación.

A juicio del SEPD, se necesitan unas garantías más estrictas para proteger a las personas afectadas, directa o indirectamente, por un accidente grave o por la pérdida de familiares.

Algunas de las recomendaciones del SEPD fueron las siguientes:

- mantener por principio la confidencialidad de las listas de pasajeros, admitiendo la posibilidad de que los Estados miembros puedan decidir de manera diferente, en casos específicos, por motivos justificados y con el consentimiento de los familiares;

- establecer un plazo limitado para el almacenamiento de datos personales;

- supeditar la transmisión de datos personales a terceros países a la condición de que éstos garanticen un nivel adecuado de protección;

- aclarar las funciones y responsabilidades de la Comisión Europea y de la Agencia Europea de Seguridad Aérea en la aplicación de la legislación sobre protección de datos.

3.10. ¿Qué nos depara el futuro?

3.10.1. Avances tecnológicos

En anteriores informes anuales([17]) el SEPD ya destacó la **creciente convergencia** entre el **«mundo físico»** y el «mundo de Internet o digital», es decir, la **sociedad de la información**. Como consecuencia, la distinción entre el mundo físico y el mundo digital tiende a difuminarse. En 2010 se aceleró esta tendencia, al estimularse la convergencia con la introducción a gran escala de nuevas e innovadoras herramientas. Hasta ahora las personas han podido vivir en los dos universos en paralelo, y han sido capaces de diferenciar entre su yo virtual y su yo real. Pero tal cosa resulta cada vez más difícil y, lo quiera o no, la persona se adentra progresivamente en un universo que engloba, sin solución de continuidad, el mundo electrónico y el real, aunque uno y otro estén sujetos a marcos reguladores distintos.

Esta tendencia se ha materializado, en particular, en las **redes sociales,** que continúan expandiéndose. En estos momentos, la población mundial dedica 110 000 millones de minutos al año a conectarse a estas redes([18]), y en Estados Unidos una red social se ha convertido por primera vez en el sitio web más visitado([19]), por delante de los buscadores de Internet.

([17]) Informe anual 2007, página 56; Informe anual 2009, página 69.

([18]) http://blog.nielsen.com/nielsenwire/global/social-media-accounts-for-22-percent-of-time-online/#

([19]) http://www.hitwise.com/us/press-center/press-releases/facebook-was-the-top-search-term-in-2010-for-sec/

Las siguientes innovaciones han contribuido a potenciar más aún este fenómeno:

- **Los dispositivos móviles inteligentes([20])** constituyen uno de los pilares principales que sustentan los nuevos puentes tendidos ente el mundo físico y el digital. Están permanentemente conectados, se encuentran en todas partes y permiten compartir, modificar y tratar la información en tiempo real. Su capacidad de tratamiento es impresionante, y permiten aprovechar los recursos prácticamente ilimitados que están disponibles «en la nube». Son capaces de grabar imágines y vídeos de alta definición, de etiquetar de forma individual objetos y personas y de vincular unas coordenadas geográficas a material multimedia que contenga lugares, sucesos y personas. Los usuarios están conectados permanentemente a la red, manejando los datos personales de otros o permitiendo que éstos manejen los suyos.

- **La tecnología de reconocimiento facial,** limitada hasta ahora a entornos perfectamente controlados, está recibiendo un nuevo impulso al ser utilizada en las redes sociales y en los teléfonos inteligentes. El enorme potencial de millones de usuarios de las redes sociales «armados» con dispositivos móviles inteligentes y subiendo a la Red imágenes donde se etiquetan los rostros de las personas amplía de manera espectacular el alcance de la tecnología de reconocimiento facial y contribuye, al mismo tiempo, a su mejora. Esta nueva tendencia emergente podría permitir igualmente la creación de bancos de datos biométricos de un tamaño sin precedentes, basados en las redes sociales.

El concepto de **realidad aumentada,** apoyado en plataformas tales como los teléfonos inteligentes, hará posible la introducción de datos adicionales tomados de Internet en el mundo real del individuo. Ya es posible visitar una ciudad y recibir información sobre monumentos «identificados» por un dispositivo móvil inteligente. En combinación con el reconocimiento facial y de las redes sociales que acabamos de mencionar, será posible técnicamente, en un futuro próximo, tomar un fotografía de una persona en la calle y acceder en tiempo real a información detallada sobre ella.

En el futuro, la **tecnología «integrada en la ropa»** representará otro puente para enlazar la vida diaria de una persona con unos paisajes digitales que no se rigen necesariamente por los mismos principios. Permitirá insertar datos individuales sensibles (temperatura, presión arterial, latido cardíaco, nivel de glucemia, etc.) en aplicaciones y servicios en línea.

Estos dos mundos íntimamente entrelazados ofrecen unas ventajas sin precedentes a los ciudadanos, empresas y administraciones públicas, pero también presentan **amenazas inéditas** que deben ser abordadas adecuadamente. En particular, el **robo de identidad en el mundo virtual** pronto tendrá consecuencias similares al robo de identidad en el mundo real. A la luz de todo esto, la disponibilidad en una red de volúmenes masivos de datos personales, la insuficiente atención a las infracciones de las normas en esta materia (muchas de las cuales tienen lugar cabo sin que nos percatemos de ello) y el número creciente de servicios comerciales, públicos y sociales a los que podemos acceder mediante la identificación virtual en el mundo de Internet, constituyen una combinación potencialmente peligrosa. Las identidades basadas en documentos, de corte tradicional, ya no representan un respaldo satisfactorio o una solución de emergencia cuando la identidad electrónica se encuentra comprometida, porque ambas están cada vez más interrelacionadas.

A pesar de esta confusión de fronteras entre el universo virtual y el real, las normas aplicables en uno y otros no son similares. Tomemos como ejemplo el contador inteligente. La fabricación, comercialización y uso de los contadores eléctricos están sujetos a toda una serie de normas específicas orientadas a la protección del consumidor, pero en el momento en que ese mismo contador se conecta a Internet y comienza a transmitir información sobre los hábitos de una persona, convirtiéndose en un contador inteligente – ya que mediante el registro y almacenamiento de las horas en que se consume electricidad es posible saber, por ejemplo, si una persona está o no en casa -, tales normas dejan de ser aplicables. La **revisión del marco jurídico de la protección de datos** podría ser la ocasión adecuada para abordar tales cuestiones. El nuevo marco deberá contribuir a definir las garantías necesarias que los ciudadanos esperan encontrar en este nuevo entorno, para poder confiar en él.

([20]) http://www.enisa.europa.eu/media/news-pictures/smartphones-video-clip

3.10.2. Prioridades para 2011

En diciembre de 2010, el SEPD publicó su quinto inventario oficial como asesor en relación con las propuestas legislativas previstas, definiendo sus prioridades en el ámbito de las actividades de consulta para el período siguiente. Como en años anteriores, el SEPD tiene intención de emitir un dictamen sobre todas las propuestas legislativas que afecten de manera importante a la protección de datos. También examinará aquellas otras medidas que, sin tener carácter legislativo, planteen dudas importante en esta materia.

Las principales prioridades del SEPD enumeradas en el inventario son las siguientes:

- *La **revisión del marco jurídico de la protección de datos**, una de sus principales prioridades para 2011.*
- *Las diferentes iniciativas referentes a la **ejecución del Programa de Estocolmo para el espacio de libertad, seguridad y justicia**, tales como la creación de un sistema de entrada y salida y el Programa de Registro de Pasajeros, la Directiva prevista sobre el uso del registro de nombres de pasajeros para fines policiales y la introducción de un Programa europeo de seguimiento de la financiación del terrorismo. El SEPD también hará un seguimiento minucioso de las negociaciones encaminadas a la celebración de acuerdos con terceros países. Por último, aunque no por ello menos importante, participará activamente en la revisión de la Directiva sobre conservación de datos.*
- *El SEPD también analizará atentamente todas aquellas **iniciativas tecnológicas** de las que pudieran derivarse consecuencias para la intimidad y la protección de datos. Seguirá prestando atención a la ulterior aplicación de la **Agenda digital** para Europa.*
- *Y finalmente, vigilará **cualquier otra innovación** que pueda afectar de manera significativa la protección de datos, por ejemplo en el área del **transporte** (uso de escáneres corporales en los aeropuertos, paquete de movilidad electrónica) y en los intercambios de datos a gran escala realizados en el marco del **Sistema de Información del Mercado Interior**.*

4 COOPERACIÓN

4.1. Grupo de trabajo del artículo 29

El Grupo de trabajo del artículo 29 es un órgano consultivo independiente constituido al amparo del artículo 29 de la Directiva sobre protección de datos (95/46/CE). El Grupo presta a la Comisión Europea asesoramiento independiente sobre temas de protección de datos y contribuye al desarrollo de políticas armonizadas en esta materia en los Estados miembros de la UE.([21])

Sus funciones se establecen en el artículo 30 de la Directiva y pueden resumirse como sigue:

- prestar a la Comisión Europea asesoramiento especializado, en nombre de los Estados miembros, sobre cuestiones relacionadas con la protección de datos;
- promover la aplicación uniforme de los principios generales de la Directiva en todos los Estados miembros, mediante la cooperación entre las autoridades de control competentes en materia de protección de datos;
- asesorar a la Comisión sobre cualquier medida que afecte a los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales;
- dirigir recomendaciones a la población en general, y a las instituciones comunitarias en particular, sobre cuestiones relacionadas con la protección de las personas en lo que respecta al tratamiento de datos personales en la UE.

El SEPD es miembro del Grupo de trabajo del artículo 29 desde principios de 2004 y considera que constituye una plataforma muy importante para la cooperación con las autoridades nacionales de control. Naturalmente, el Grupo debe desempeñar también una función primordial en la aplicación uniforme de la Directiva y en la interpretación de sus principios generales.

En 2010, el Grupo concentró sus actividades en los cuatro principales temas estratégicos identificados en el programa de trabajo 2010-2011, a saber:

- aplicar de la Directiva y elaborar un amplio marco jurídico para el futuro;
- abordar la globalización;
- reaccionar ante los retos tecnológicos;
- mejorar la eficacia del propio Grupo y de las autoridades de protección de datos.

El Grupo de trabajo redactó diversos documentos a este respecto, entre ellos los siguientes:

([21]) El Grupo de trabajo está formado por los representantes de las autoridades de control de cada Estado miembro, por un representante de la autoridad designada por las instituciones y organismos de la UE (es decir, el SEPD), y por un representante de la Comisión, que también desempeña las labores de secretaría. Las autoridades de control de Islandia, Noruega y Lichtenstein (como miembros del EEE) están representadas a través de observadores.

- Dictamen 2/2010 sobre **publicidad comportamental en línea** (WP 171);

- Dictamen 5/2010 relativo a la propuesta de la industria para un marco de evaluación del impacto sobre la protección de datos y la intimidad en las **aplicaciones basadas en la identificación por radiofrecuencia (RFID)** (WP 175);

- Dictamen 7/2010 relativo a la Comunicación de la Comisión Europea sobre el **enfoque global de las transferencias de datos de los registros de nombres de los pasajeros** (PNR) a terceros países (WP 178).

El Grupo de trabajo y el SEPD colaboraron estrechamente en los problemas relacionados con la aplicación de la Directiva 95/46/CE y la interpretación de algunas de sus disposiciones principales. El SEPD también prestó una contribución activa en otros temas, como por ejemplo:

- Dictamen 1/2010 sobre los **conceptos de «responsable del tratamiento» y «encargado del tratamiento»** (WP 169);

- Dictamen 3/2010 sobre el **principio de responsabilidad** (WP 173);

- Dictamen 8/2010 sobre el **Derecho aplicable** (WP 179).

Por otra parte, el SEPD coopera con las autoridades de control nacionales en la medida necesaria para el ejercicio de sus correspondientes funciones, en particular intercambiando toda la información que pueda resultar útil y pidiendo o prestando asistencia para el desempeño de sus funciones [artículo 46, letra f), inciso i), del Reglamento]. Esta cooperación se lleva a cabo caso por caso.

La cooperación directa con las autoridades nacionales adquiere cada vez mayor importancia en el contexto de los grandes sistemas internacionales como Eurodac, que requieren un planteamiento coordinado de la supervisión (véanse las secciones 4.2 y 4.3).

4.2. Supervisión coordinada de Eurodac

La supervisión eficaz de Eurodac se basa en una estrecha cooperación entre las autoridades nacionales de protección de datos y el SEPD.

El Grupo de Coordinación de la Supervisión de Eurodac, compuesto por autoridades nacionales de protección de datos y el SEPD, desarrolló sus actividades de acuerdo con el programa de trabajo 2010-2011, aprobado a principios de 2010.

Aunque este programa de trabajo engloba una variedad de temas, se centra preferentemente en los de carácter común o sensible, en los que el Grupo puede aportar un valor añadido que suponga una diferencia. Sin embargo, diversas actividades están pendientes de la adopción de los nuevos Reglamentos de Eurodac y de Dublín, por lo que se llevarán a cabo en el momento oportuno.

En la actualidad, las actividades del Grupo están organizadas en función de un calendario, lo que permite una mejor planificación. Las tareas para los próximos años se han dividido en:

- actividades cuatrienales: por ejemplo, la realización por las autoridades nacionales de protección de datos de una auditoría de seguridad completa, tanto a nivel nacional como de la UE. La preparación de la misma, coordinada por el Grupo, permitirá lograr una mayor eficacia y comparabilidad de los resultados;

- actividades bianuales: por ejemplo, las inspecciones coordinadas, es decir, la definición y realización de este tipo de inspecciones a intervalos regulares;

- actividades anuales: se trata de investigaciones de corta duración, con un alcance más limitado que las inspecciones coordinadas, y que se llevan a cabo en función de las necesidades identificadas por el Grupo;

- actividades permanentes: incluyen sobre todo las actividades de seguimiento requeridas a nivel institucional, como el análisis de las iniciativas de tipo legislativo y político, y también las investigaciones especiales y las actuaciones derivadas de las recomendaciones previamente realizadas.

Dentro de estas categorías, se seleccionaron diversas actividades para su inicio en 2010.

El Grupo celebró tres reuniones en Bruselas, en los meses de marzo, octubre y diciembre de 2010. En la reunión de marzo fue reelegido Presidente Peter Hustinx (SEPD), designándose Vicepresidenta a Elizabeth Wallin (de la autoridad sueca de protección de datos).

El Grupo comenzó a trabajar en los **preparativos de la auditoria de seguridad completa**. Se designó un subgrupo que dio comienzo a sus tareas identificando los temas de interés, como la elaboración de una lista de objetivos de seguridad, y los problemas planteados por el requisito de comparabilidad de los resultados. Esta tarea proseguirá en 2011.

A finales de 2010 se puso en marcha una **nueva inspección coordinada,** para la cual el Grupo seleccionó el tema de la eliminación anticipada de los datos, elaborando el cuestionario y la metodología correspondientes, y cuyos resultados se espera conocer en 2011. La eliminación anticipada de los datos se consideró importante debido a sus consecuencias para la calidad de los datos en el sistema Eurodac, y para la protección de las personas que no deberían seguir registradas en su base de datos.

La **interacción con las partes interesadas** se inició, bajo los mejores auspicios, en la reunión de diciembre, a la que asistieron representantes del Alto Comisionado de las Naciones Unidas para los Refugiados y del Consejo Europeo sobre Refugiados y Asilados. Las partes interesadas externas presentaron sus trabajos y prioridades y expusieron sus puntos de vista sobre temas tales como el futuro del Sistema de Dublín, la información que se debe facilitar a los solicitantes de asilo y la defensa de los derechos de estos últimos. También plantearon sus objeciones a la posibilidad de permitir el acceso a Eurodac para fines policiales. Este intercambio de opiniones resultó extremadamente útil y deberá repetirse de forma regular.

La supervisión coordinada de Eurodac resulta esencial para garantizar los derechos de las personas vulnerables, como los demandantes de asilo.

4.3. Supervisión del Sistema de Información Aduanera (SIA)

La finalidad del Sistema de Información Aduanera (SIA) es la creación de un **mecanismo de alerta** en el marco de la **lucha contra el fraude,** en virtud del cual cualquier Estado pueda introducir una solicitud dirigida a otro Estado miembro para éste realice inspecciones y notificaciones, lleve a cabo una vigilancia encubierta o proceda a comprobaciones específicas o a análisis operativos y estratégicos.

El SIA almacena información sobre mercancías, medios de transporte, personas y empresas, productos y dinero aprehendidos o confiscados, con el fin de ayudar a la prevención, investigación y enjuiciamiento de las actividades que contravengan la legislación aduanera o agrícola (el antiguo «tercer pilar»). Esta última actividad está sometida una Autoridad Común de Control compuesta por representante de las autoridades nacionales de protección de datos.

El Grupo de Coordinación de la Supervisión del SIA constituye una plataforma para que las autoridades de protección de datos, responsables del control del SIA en virtud del Reglamento (CE) nº 766/200([22]) – es decir, el SEPD y las autoridades nacionales de protección de datos – ,puedan cooperar en el marco de sus competencias a fin de garantizar una supervisión coordinada del SIA.

([22]) Reglamento (CE) nº 766/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se modifica el Reglamento (CE) nº 515/97 del Consejo, relativo a la asistencia mutua entre las autoridades administrativas de los Estados miembros y a la colaboración entre estas y la Comisión con objeto de asegurar la correcta aplicación de las reglamentaciones aduanera y agraria.

El Grupo de Coordinación debe:

a) estudiar los problema de ejecución relacionados con las actividades del SIA;

b) analizar las dificultades encontradas durante las comprobaciones efectuadas por las autoridades de control;

c) examinar las dificultades de interpretación o aplicación del Reglamento del SIA;

d) elaborar recomendaciones sobre soluciones comunes a los problemas existentes, y

e) esforzarse por mejorar la cooperación entre las autoridades de control.

En 2010, el SEPD convocó dos reuniones del Grupo de Coordinación de la Supervisión del SIA (en marzo y diciembre respectivamente). En ellas participaron representantes de las autoridades nacionales de protección de datos, de la Autoridad Común de Control Aduanero y de la Secretaría de Protección de Datos.

En su reunión de diciembre, el Grupo aprobó el reglamento interno por el que se regirá su futura colaboración con el SIA, y debatió las posibles medidas que se han de adoptar en el período 2011-2012 para lograr una supervisión integral de la protección de los datos en este sistema.

4.4. Cooperación policial y judicial: cooperación con las ACC y con el WPPJ

El SEPD coopera asimismo con las autoridades encargadas de la supervisión de organismos específicos o de determinados sistemas informáticos europeos a gran escala, como la Autoridad Común de Control (ACC) de Europol y de Eurojust, y la Autoridad Común de Control (ACC) del Sistema de Información de Schengen (SIS) y de los aspectos relativos al «antiguo tercer pilar» del Sistema de Información Aduanera (SIA). Esta cooperación reviste la forma de información mutua sobre temas de interés común, como aquellos en los que el SEPD y las ACC supervisan respectivamente distintas partes de un mismo sistema.

En 2010 la cooperación giró principalmente en torno al SIA. Puesto que el SEPD y la ACC del SIA comparten la función de supervisar el mismo sistema, es

lógico que actúen de la forma más coordinada posible. En este sentido, el SEPD invitó a representantes de las ACC a participar en las reuniones organizadas para tratar sobre la supervisión coordinada del SIA (véase la sección 4.3).

Participó igualmente en los encuentros y actividades del Grupo de trabajo sobre policía y justicia (WPPJ). El WPPJ estudió diversos asuntos en 2010, entre ellos el desarrollo de una política de supervisión común para los acuerdos «de tipo Prüm» (acuerdos bilaterales sobre el intercambio de datos). Por otro lado, trabajó conjuntamente con el Grupo de trabajo del artículo 29 (WP29) para elaborar una «contribución común de las autoridades europeas de protección de datos», representadas en estos organismos, en relación con el acuerdo sobre protección de datos EU-EE.UU. Este ejemplo ilustra la necesidad de una amplia cooperación entre ambos grupos, en un contexto en el que la distinción entre los pilares primero y tercero es cada vez menos relevante.

Por último, el WPPJ abordó el tema de su propio futuro a la luz de los cambios antes mencionados, teniendo presente la creciente implicación del WP29 en las áreas que tradicionalmente le correspondían a él.

4.5. Conferencia Europea

Las autoridades de protección de datos de los Estados miembros y el Consejo de Europa se reúnen anualmente en una conferencia de primavera para debatir materias de interés común e intercambiar información y experiencias en diversos campos.

La Conferencia Europea de Comisarios de Protección de Datos se celebró en **Praga los días 29-30 de abril de 2010** bajo el lama «Sopesar el pasado, pensar en el futuro», actuando como anfitrión la Autoridad Checa de Protección de Datos.

La conferencia incluyó sesiones dedicadas a diversos temas, entre ellos los siguientes: 1) Internet de los objetos: controles omnipresentes en el espacio y en el tiempo, con una presentación del Supervisor adjunto; 2) Los niños en la telaraña de las redes; 3) La protección de datos personales en la encrucijada, una presentación del SEPD; 4) El sector público: ¿un socio respetado o un encargado del tratamiento con privilegios?

No es sorprendente que **el futuro marco de la protección de datos,** actualmente en curso de elaboración por la Comisión Europea, fuera un elemento central del debate. Se aprobaron varias resoluciones, en particular acerca de:

- el proyectado acuerdo entre Estados Unidos y la UE sobre las normas de protección de datos en el ámbito de la cooperación policial y judicial en materia penal;
- los escáneres corporales;
- la protección de los menores, y
- el futuro de la intimidad.

4.6. Conferencia internacional

Las autoridades responsables de la protección de datos y los comisarios encargados de la protección del derecho a la intimidad de Europa y de otras regiones del mundo, en concreto Canadá, América Latina, Australia, Nueva Zelanda, Hong Kong y Japón, además de otras entidades políticas de la región Asia-Pacífico, han venido organizando desde hace tiempo encuentros anuales en una conferencia que se celebra en otoño.

Este año, la Conferencia Internacional de Comisarios de Protección de Datos fue organizada en Jerusalén por la Autoridad de Protección de Datos de Israel, **los días 26-29 de noviembre de 2010**. Su lema principal fue «La intimidad y las generaciones».

Se celebraron varias sesiones plenarias, en las que se debatieron los temas siguientes:

- ¿Dónde estamos? El cambio intergeneracional en la percepción de la intimidad;
- El contenido del programa de elaboración de normas: la voz de los legisladores;
- Privacidad por diseño;
- La intimidad en el futuro: de qué modo las normas sobre intimidad pueden inspirar a la reglamentación.

La Conferencia siguió estudiando las perspectivas de las diferentes generaciones sobre la intimidad y la protección de datos. Uno de los temas más

destacados fue la forma en que las leyes y los mecanismos de autorregulación influyen en la tecnología y viceversa. El creciente uso de las redes sociales fue asimismo uno de los focos de interés de la conferencia.

El SEPD y el Supervisor adjunto ofrecieron sus presentaciones y presidieron diversas sesiones de la conferencia.

La sesión de los Comisarios, celebrada a puerta cerrada, adoptó varias resoluciones, la más importante de las cuales fue la invitación a celebrar una conferencia intergubernamental para la elaboración de un instrumento jurídico internacional de carácter vinculante en materia de protección de la intimidad y los datos personales.

La 33ª Conferencia Internacional tendrá lugar en México en noviembre de 2011.

4.7. Organizaciones internacionales (taller de Florencia)

El SEPD, en colaboración con el Instituto Universitario Europeo, organizó el tercer taller sobre protección de datos en las organizaciones internacionales. Se celebró en Florencia los días 27-28 de mayo de 2010 y contó con la participación de relevantes organizaciones internacionales, como la ACNUR, la OMA, la OIM, el CIC y otras muchas. En los debates se analizaron los diversos desafíos con que se enfrentan las organizaciones internacionales que tratan de garantizar un nivel adecuado de protección de datos, en contextos frecuentemente difíciles y sin disponer de un fundamento jurídico claro. Las organizaciones que ya han alcanzado un buen nivel en este ámbito destacaron los múltiples beneficios que pueden reportar para sus actividades esenciales (en particular la seguridad y legitimidad de los datos).

Como continuación del taller, el SEPD distribuyó un cuestionario con el fin de hacer un inventario de los regímenes de protección de datos (o de la ausencia de ellos) en las organizaciones internacionales participantes. Se hizo hincapié en los métodos para asegurar una protección de datos real y eficaz, más que en los sistemas legislativos específicos.

Por lo tanto, el cuestionario trataba de registrar los logros obtenidos en materia de protección de datos por las organizaciones internacionales, la aplicación del principio de asunción de responsabilidades para reducir el riesgo de incumplimiento, y la introducción de mecanismos prácticos para lograr una protección de datos eficaz. Estos conceptos son especialmente adecuados en el contexto de las organizaciones internacionales, ya que pueden aplicarse al margen del entorno legislativo en que se realiza el tratamiento de los datos.

Las respuestas servirán de base para las futuras acciones en este ámbito. Muchos de los participantes expresaron su deseo de que estos talleres se sigan organizando en el futuro de forma regular.

5 COMUNICACIÓN

5.1. Introducción

La información y la comunicación desempeñan un papel esencial para conferir **visibilidad** a las principales actividades del SEPD y **mejorar la sensibilización** tanto sobre el trabajo de éste como sobre la protección de datos en general. Se trata de un aspecto importante, debido a la necesidad de dar a conocer mejor las funciones y la misión del SEPD a nivel europeo, aunque ya se han registrado avances importantes en esta dirección. Indicadores como el mayor volumen de solicitudes de información recibidas de los ciudadanos de la UE, el incremento de las consultas recibidas de los medios de comunicación, el mayor número de abonados del boletín y de invitaciones para intervenir en conferencias, así como el tráfico cada vez más intenso en el sitio web, refuerzan la convicción de que el SEPD se ha convertido en un punto de referencia para las cuestiones relacionadas con la protección de datos.

La presencia cada vez más acusada del SEPD en el paisaje institucional es especialmente relevante para sus tres funciones principales, a saber: la supervisión de todas las instituciones y organismos comunitarios que participan en el tratamiento de datos personales, el asesoramiento a las instituciones que participan en la elaboración y la adopción de nueva legislación y de políticas que pueden afectar a la protección de datos personales (Comisión, Consejo y Parlamento) y la cooperación con las autoridades nacionales de supervisión y los diversos organismos en el ámbito de la seguridad y justicia.

En 2010 continuaron las actividades de mejora de las actividades y herramientas de comunicación del SEPD. Una novedad importante fue la incorporación del alemán como tercera lengua, además del inglés y francés, en las relaciones con la prensa y en otras actividades de comunicación. La relevancia de este hecho estriba en que el alemán es la lengua de la UE que cuenta con mayor número de hablantes nativos. Por lo tanto, el objetivo consiste en alcanzar una audiencia más amplia y dar a la prensa y a los ciudadanos germanohablantes la posibilidad de seguir las actividades del SEPD en su propia lengua.

5.2. Características de la comunicación

Es preciso configurar la política de comunicación del SEPD de acuerdo con características específicas pertinentes, teniendo en cuenta la antigüedad de la institución, su tamaño y su mandato. Esto requiere un planteamiento a la medida, que utilice las herramientas más apropiadas para dirigirse a las audiencias adecuadas y que al mismo tiempo pueda adaptarse a las diversas limitaciones y requisitos.

5.2.1. Principales audiencias y grupos destinatarios

A diferencia de la mayor parte de las demás instituciones y organismos de la UE, cuyas políticas y actividades de comunicación se desarrollan a nivel general y se dirigen a los ciudadanos de la UE en su conjunto, la esfera de acción directa del SEPD está

mucho más delimitada. Se centra fundamentalmente en las instituciones y organismos comunitarios, los titulares de los datos en general y el personal de la UE en particular, las partes interesadas en las políticas de la UE y «los homólogos de la protección de datos». Como resultado, la política de comunicación del SEPD no tiene motivos para embarcarse en una estrategia de «comunicación de masas». La sensibilización sobre los problemas de protección de datos entre los ciudadanos de los Estados miembros dependerá más bien, en lo fundamental, de un planteamiento más indirecto, por ejemplo a través de las autoridades responsables de la protección de datos a nivel nacional.

Con todo, el SEPD también asume la parte que le corresponde en la mejora de su perfil entre el público en general, en especial aplicando las diversas herramientas de comunicación (sitio web, boletín, actividades de mejora de la sensibilización), atendiendo con regularidad a las partes interesadas (por ejemplo, a las visitas de estudio a su oficina) y participando en actividades, reuniones y conferencias públicas.

5.2.2. Política relativa al lenguaje utilizado para la comunicación

La política de comunicación del SEPD debe tener en cuenta además la naturaleza específica del medio en el que se desarrolla su actividad. Para los profanos en la materia, los problemas ligados a la protección de datos pueden parecer un tanto técnicos y oscuros, por lo que el lenguaje utilizado por el SEPD debe adaptarse en consecuencia. Cuando se trata de herramientas de información y de comunicación dirigidas a una audiencia heterogénea, es preciso utilizar un lenguaje claro y comprensible que evite toda terminología especializada innecesaria. Se hacen, por tal motivo, esfuerzos constantes en esta dirección, en particular en la comunicación con el público y los medios generalistas, con el objetivo de corregir la imagen excesivamente «jurídica» que tiene la protección de datos.

Cuando se trata de audiencias más informadas (por ejemplo, expertos en protección de datos, partes interesadas de la UE) está más justificado el uso de un lenguaje especializado. Por consiguiente, posiblemente será necesario utilizar diferentes estilos de comunicación y pautas lingüísticas para comunicar las mismas noticias.

5.3. Relaciones con los medios de comunicación

El SEPD aspira a mantener las relaciones más fluidas posible con la prensa, de manera que la ciudadanía pueda estar al corriente de sus actividades. El SEPD informa regularmente a los medios a través de comunicados de prensa, entrevistas, debates de fondo y conferencias de prensa. La gestión de las consultas procedentes de los medios de comunicación permite un mayor contacto con ellos.

5.3.1. Comunicados de prensa

En 2010, el servicio de prensa publicó 19 comunicados. La mayoría de ellos se referían a la labor del SEPD en el ámbito consultivo y, más específicamente, a los **dictámenes legislativos** directamente relevantes para el público en general. Entre los temas tratados estaban la estrategia para la reforma de la protección de datos de la UE, las negociaciones sobre el Acuerdo Comercial de Lucha contra la Falsificación (ACTA), el acuerdo UE-EE.UU. sobre el Programa de Seguimiento de la Financiación del Terrorismo (TFTP), la gestión de la información en el espacio de libertad, seguridad y justicia, la intimidad y la confianza en la sociedad de la información, la estrategia externa de la UE en relación con el registro de nombres de los pasajeros, el proceso de evaluación de la Directiva sobre conservación de datos y la Estrategia de Seguridad Interior de la UE. También se publicaron comunicados de prensa sobre la sentencias más relevantes del Tribunal de Justicia de la Unión Europea, como la dictada en el asunto *Bavarian Lager* o la relativa a la independencia de las autoridades responsables de protección de datos.

También se distribuyeron comunicados en prensa en relación con las **principales actividades en el ámbito de la supervisión,** en particular las relativas a la adopción de la directrices sobre videovigilancia o de una política de amplio alcance en materia de control del cumplimiento y aplicación.

Los comunicados de prensa se publican en el sitio web del SEPD y en la base de datos interinstitucional de comunicados de prensa de la Comisión Europea (RAPID), en inglés y francés. En 2010 se añadió una versión en alemán, para reflejar la introducción de esta tercera lengua en las actividades de comunicación del SEPD. Los comunicados se distribuyen a una red de periodistas e interlocutores que se actualiza periódicamente. Habitualmente generan una cobertura significativa por parte de los medios de comunicación, tanto de información general

como especializados. Se publican además en una serie de sitios web, tanto institucionales como de otro tipo, que van desde las páginas de las instituciones y organismos de la UE hasta las de organizaciones no gubernamentales, instituciones académicas y empresas relacionadas con las tecnologías de la información.

5.3.2. Entrevistas de prensa

En 2010, el SEPD concedió alrededor de 20 entrevistas a periodistas de la prensa impresa, de la radiotelevisión y de los medios electrónicos de toda Europa, en respuesta a un considerable número de peticiones procedentes de medios alemanes, austriacos, neerlandeses y estadounidenses.

Ello dio lugar a varias apariciones en medios nacionales, europeos e internacionales, por ejemplo en publicaciones especializadas sobre temas de tecnologías de la información y en entrevistas en emisoras de radio y TV, como la televisión nacional austríaca o la radio neerlandesa y austríaca.

Las entrevistas abarcaron cuestiones horizontales tales como la seguridad de los datos europeos, la tendencia a una sociedad de la vigilancia y los retos actuales y venideros en el ámbito de la intimidad y la protección de datos. También se trataron otros temas más específicos que saltaron a los titulares en 2010, como el acuerdo TFTP con Estados Unidos, la revisión del marco jurídico de la UE para la protección de datos y los problemas de intimidad relacionados con las redes sociales, las aplicaciones de geolocalización y el uso de los escáneres corporales en los aeropuertos.

5.3.3. Conferencias de prensa

El 15 de noviembre de 2010 se organizó en Bruselas una conferencia de prensa sobre la revisión de las normas de la UE en materia de protección de datos e intimidad. En ella, Peter Hustinx y Giovanni Buttarelli comentaron, en particular, la Comunicación de la Comisión sobre una estrategia para el reforzamiento de las normas europeas de protección de datos, publicada a primeros de noviembre de 2010. La conferencia de prensa ofreció asimismo la oportunidad de presentar el Informe anual 2009 del SEPD y de describir las líneas principales de las actividades realizadas ese año en relación con sus tareas de control, asesoramiento y cooperación (véase la sección 5.7.1.).

5.3.4. Consultas de los medios

Se reciben con frecuencia consultas de los medios de comunicación que suelen incluir peticiones de comentarios del SEPD y solicitudes de aclaración o información. En 2010, la atención de los medios se

Conferencia de prensa del SEPD sobre la revisión del marco jurídico de protección de datos (Bruselas, 15 de noviembre de 2010)

centró principalmente en los problemas de la intimidad en Internet, particularmente en relación con las nuevas aplicaciones en línea, como la geolocalización, los motores de búsqueda y las redes sociales, siendo esta última área la que concentró en mayor número de consultas. También el acuerdo con Estados Unidos sobre el tratamiento y trasmisión de datos financieros en el marco del Programa de seguimiento de la financiación del terrorismo (TFTP) fue objeto de especial atención por la prensa.

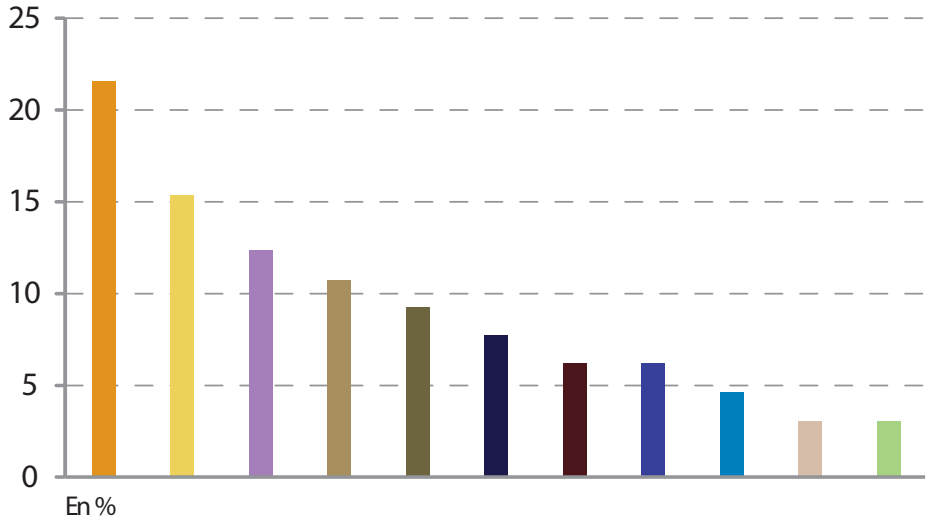
Los restantes temas de interés para los medios fueron la revisión del marco jurídico de la UE para la protección de datos, la Directiva sobre conservación de datos, la Directiva sobre privacidad electrónica y el tratamiento dado en ella a las filtraciones de datos, las actividades de supervisión del SEPD y sus directrices sobre videovigilancia, el problema de la seguridad de los datos, la identificación biométrica, tanto en los pasaportes como en el Sistema de Información de Schengen, las transferencias internacionales de datos y las decisiones de la Comisión sobre la adecuación de los acuerdos con terceros país y el uso de escáneres corporales en los aeropuertos.

5.4. Solicitudes de información y asesoramiento

El número de solicitudes de información o asesoramiento recibidas de los ciudadanos descendió ligeramente en 2010 (141 solicitudes, en comparación con las 174 de 2009). El principal motivo fue la disminución del número de solicitudes referidas a cuestiones de protección de datos a nivel nacional, para las que el SEPD carece de competencias. Esta evolución puede considerarse que es resultado de los esfuerzos realizados para explicar el ámbito de competencias del SEPD a través de sus distintos instrumentos de información y comunicación.

Las solicitudes procedían de un amplio abanico de personas y colectivos, desde las partes interesadas que operan en el entorno de la UE o que trabajan en el ámbito del derecho a la intimidad, la protección de datos y la tecnología de la información (despachos de abogados, consultorías, representantes de grupos de presión, organizaciones no

Temas principales de las consultas de la prensa en 2010



- Intimidad en Internet*
- Acuerdo SWIFT/TFTP
- Revisión del marco jurídico de la protección de datos en la UE
- Directiva sobre conservación de datos
- Directiva sobre privacidad electrónica
- Actividades de supervisión del SEPD**
- Seguridad de los datos
- Datos biométricos***
- Transferencias internacionales de datos****
- Escáneres corporales
- Acuerdo ACTA

* incluyendo las nuevas aplicaciones en línea, los motores de búsqueda y las redes sociales

** incluyendo las directrices sobre videovigilancia.

*** incluyendo el Sistema de Información de Schengen

**** incluyendo las decisiones de la Comisión sobre adecuación

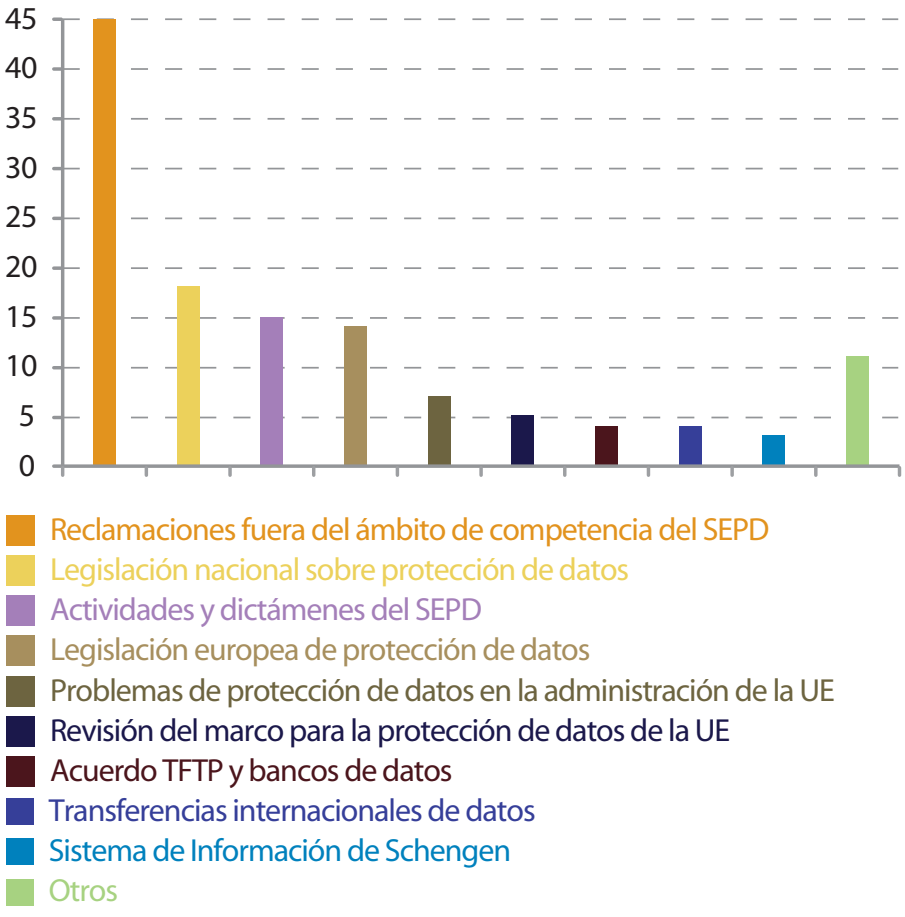
gubernamentales, asociaciones, universidades, etc.) hasta los ciudadanos que necesitan más información sobre el derecho a la intimidad o que solicitan ayuda para solucionar los problemas con que se enfrentan.

La primera categoría de solicitudes recibidas en 2010 comprende las reclamaciones formuladas por ciudadanos de la UE en relación con asuntos que no son competencia del SEPD. La mayoría de estas reclamaciones se referían a presuntas infracciones en materia de protección de datos por parte de autoridades públicas, empresas públicas o privadas y servicios y tecnologías relacionados con Internet, como juegos en línea, *blogs,* servicios de geolocalización, redes sociales y herramientas de mensajería. Otras estaban relacionadas con la seguridad de los datos bancarios, el derecho de acceso a los documentos en poder de las administraciones nacionales, la divulgación de los datos personales a terceros sin el consentimiento del interesado y los recursos contra las resoluciones de las autoridades nacionales de protección de datos. Dado que este tipo de reclamaciones no son competencia del SEPD, se responden describiendo el mandato del SEPD y aconsejando al reclamante que se dirija a la autoridad competente, que por lo general es la autoridad nacional responsable de protección de datos del Estado miembro de que se trate.

La segunda categoría de solicitudes recibidas en 2010 corresponde a la legislación sobre protección de datos en los Estados miembros de la UE, o a su aplicación. En estos casos, el SEPD aconseja al interesado que se ponga en contacto con la autoridad competente responsable de la protección de datos y, en su caso, con la Unidad de Protección de Datos de la Comisión Europea.

La mayor parte de las solicitudes de información restantes eran competencia del SEPD, por lo que obtuvieron respuestas puntuales. Se trataba, por regla general, de consultas sobre la actividades del SEPD, en particular las relacionadas con las políticas y el asesoramiento, así como sobre la legislación europea en materia de protección de datos, los problemas de protección de datos en la administración de la UE, la revisión del marco jurídico correspondiente,

Temas principales de las solicitudes de información del público en 2010



el acuerdo TFTP y los datos financieros, las transferencias internacionales de datos y el acceso al Sistema de Información de Schengen.

5.5. Visitas de grupos de estudiantes

En el marco de sus esfuerzos por mejorar tanto la sensibilización sobre la protección de datos como la interacción con el mundo académico, el SEPD recibe con regularidad visitas de grupos de estudiantes de especialidades relacionadas con la legislación europea, la protección de los datos y/o los problemas de seguridad de las tecnologías de la información. En 2010, el SEPD recibió la visita de siete grupos de estudiantes de diversos países europeos. Por ejemplo, en octubre de 2010, acogió a un grupo de estudiantes de Derecho internacional y europeo de la Fundación Friedrich Ebert de Alemania, a los que presentó sus funciones y actividades y con los que debatió sobre asuntos relacionados con la protección de datos en el marco del Programa de Estocolmo. También dio la bienvenida a otros visitantes, entre ellos estudiantes austríacos de MBA en gestión pública, de la Universidad de Tilburg en los Países Bajos, de la Fundación Rosa Luxemburg de Alemania y la Universidad de Grenoble en Francia.

En sus esfuerzos por llegar a un público más joven, el personal del SEPD recibió a un grupo de alumnos austríacos de enseñanza secundaria, con los cuales se comentaron los temas relacionados con la protección de datos que les interesaban especialmente, como las cuestiones de intimidad en las redes sociales de Internet.

5.6. Herramientas de información en línea

5.6.1. Sitio web

El sitio web es el canal de comunicación y herramienta de información más importante del SEPD. Se actualiza casi a diario. Es también el medio de comunicación a través del cual los visitantes pueden acceder a los diversos documentos presentados como consecuencia de las actividades del SEPD (por ejemplo, dictámenes sobre controles previos y sobre propuestas de legislación de la UE, prioridades de trabajo, publicaciones, alocuciones del Supervisor y el Supervisor adjunto, comunicados de prensa, boletines e información sobre actividades).

Cambios en la web

En 2010, el cambio más importante en el sitio web fue la introducción de la versión alemana, además de la inglesa y la francesa ya existentes. Esta iniciativa fue consecuencia de la decisión de publicar todos los materiales de comunicación externa en estas tres lenguas como mínimo, con el fin de responder mejor a las necesidades de información del público y de las partes interesadas.

Se reorganizó asimismo la página principal para resaltar mejor las últimas noticias relacionadas con las actividades del SEPD.

Entre las ulteriores mejoras del sitio web previstas se incluyen las siguientes:

- la introducción de un formulario de reclamación en línea para facilitar la presentación de reclamaciones y acelerar la tramitación de las mismas por parte de los servicios del SEPD;
- la renovación de la sección sobre dictámenes de control previo, al objeto de completar las opciones de búsqueda y la navegabilidad entre las distintas categorías temáticas;
- una presentación más simplificada del registro de notificaciones, y
- la introducción de una sección de informes de prensa, destinada a facilitar a los profesionales documentación y recursos que puedan utilizar en sus artículos, noticias y entrevistas informativas.

Tráfico y navegación

En el marco de los esfuerzos por mejorar el funcionamiento del sitio web, en 2009 se mejoraron diferentes características (como la herramienta de búsqueda avanzada), unas más visibles que otras.

Un análisis de los datos sobre tráfico y navegación muestra que en 2010 el sitio web recibió un total de 108 215 visitas únicas, con más de 12 000 mensuales en febrero y marzo. Estas cifras suponen un notable incremento respecto a 2009. Después de la página principal, las más visitadas fueron «Contacto», «Supervisión» y «Consulta», aunque también las páginas de «Noticias», «Publicaciones» y «Eventos» han gozado de gran popularidad. Las estadísticas muestran asimismo que la mayor parte de los visitantes acceden al sitio web a través de una

dirección directa, un marcador, un vínculo en un correo electrónico o un vínculo en otro sitio web, como el portal Europa o el sitio web de una autoridad nacional de protección de datos. Solo un número muy reducido de visitantes acceden al sitio web a través de un motor de búsqueda. Estas cifras nos dan a entender que el sitio web del SEPD es consultado por un núcleo de visitantes regulares que confían en su contenido.

5.6.2. Boletín digital

El boletín del SEPD sigue siendo una herramienta útil para informar sobre sus actividades más recientes y para llamar la atención sobre las últimas novedades incluidas en el sitio web. Ofrece noticias relacionadas con los últimos dictámenes del SEPD sobre las propuestas legislativas de la UE y sobre los controles previos. Incluye asimismo información sobre las próximas conferencias y otras actividades, y sobre las alocuciones recientes del Supervisor y el Supervisor adjunto. Los boletines se encuentran disponibles en el sitio web del SEPD, y también se ofrece un formulario de suscripción en la página correspondiente.

En 2010 se publicaron cinco números del boletín, con una frecuencia media bimestral. Hasta 2010, el boletín se publicaba en inglés y francés. A partir de ese año se añadió también una versión alemana, para ampliar la audiencia y para reflejar el uso de las tres lenguas de trabajo en el servicio de prensa del SEPD.

El número de abonados se incrementó, pasando de 1 200 a finales de 2009 a unos 1 500 al finales de 2010. Entre los abonados figuran diputados al Parlamento Europeo, personal de las instituciones europeas y de las autoridades nacionales de protección de datos, así como periodistas, personalidades del mundo académico, empresas de telecomunicación y despachos de abogados.

5.6.3. Intranet

Con vistas a mejorar la comunicación interna y simplificar el intercambio de información entre los diversos sectores de la oficina del SEPD, se ha desarrollado una intranet con la ayuda del servicio responsable del Parlamento Europeo. Este nuevo portal interno será plenamente operativo a comienzos de 2011.

5.7. Publicaciones

5.7.1. Informe anual

El Informe anual es la publicación principal del SEPD. Ofrece una descripción general de las actividades en sus grandes esferas operativas de la supervisión, el asesoramiento y la cooperación durante el año de referencia, y define sus principales prioridades para el año siguiente. También describe lo logrado en términos de comunicación exterior, así como las incidencias relativas a la administración, al presupuesto y al personal.

El Informe anual puede ser de especial interés para diversos grupos y particulares a nivel internacional, europeo y nacional: los titulares de los datos en general y el personal de la UE en particular, la estructura institucional de la UE, las autoridades de protección de datos, los especialistas en esta materia, los grupos de interesados y las organizaciones no gubernamentales activas en este ámbito, los periodistas y cualquier persona que busque información sobre la protección de datos personales a nivel de la UE.

En 2010 se introdujeron diversas mejoras tanto en la forma como en el fondo, destinadas a conseguir una publicación más fácil de utilizar por el lector y a destacar con mayor claridad los principales resultados y conclusiones del informe.

El 15 de noviembre de 2010, el Supervisor y el Supervisor adjunto presentaron el Informe anual 2009 del SEPD a la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento

Informe anual 2009 del SEPD

Europeo. También se presentaron a la prensa los aspectos más destacados del informe en ocasión de una conferencia organizada ese mismo día sobre el futuro del marco jurídico de la UE para la protección de datos (véase la sección 3.3.).

5.7.2. Publicaciones temáticas

Se iniciaron los preparativos para la publicación de las «hojas informativas» temáticas sobre las cuestiones de importancia estratégica en el ámbito de la protección de datos. Su finalidad consiste en facilitar directrices específicas dirigidas tanto al público en general como a los grupos interesados. El primer conjunto de hojas informativas abordará temas como la Directiva sobre la privacidad en las comunicaciones electrónicas, el acuerdo SWIFT/TFTP y el registro de los nombres de los pasajeros.

5.8. Actividades de mejora de la sensibilización

El SEPD trata de aprovechar todas las oportunidades para poner de relieve la importancia creciente de la intimidad y la protección de datos, y mejorar la sensibilización de los interesados sobre los derechos que les protegen y de las administraciones europeas sobre las obligaciones que les conciernen en esta materia.

5.8.1. Día de la Protección de Datos

El 28 de enero de 2010, los Estados miembros del Consejo de Europa y las instituciones europeas conmemoraron el cuarto Día Europeo de la Protección de Datos. Esta fecha señala el aniversario del Convenio para la protección de los datos de carácter personal del Consejo de Europa (Convenio 108), el primer instrumento internacional jurídicamente vinculante en la materia.

Como en años anteriores, el SEPD utilizó esta ocasión para insistir en la importancia del derecho a la intimidad y la protección de datos, y en particular para mejorar la sensibilización del personal de la UE sobre sus derechos y obligaciones en este ámbito. Cada vez que se conmemora el Día de la Protección de Datos, el SEPD instala un stand informativo en las sedes del Parlamento, de la Comisión y del Consejo, en colaboración con el responsable de la protección de datos de cada una de estas instituciones. Los visitantes tienen la posibilidad de plantear preguntas al personal del SEPD y al propio responsable de la protección de datos, pudiendo comprobar sus conocimientos sobre las normas europeas mediante un juego de preguntas.

En 2010, el SEPD repitió esta acción específica y dedicó además nuevos esfuerzos a mejorar la sensibilización entre los funcionarios de la UE. Bajo el título «Intimidad y protección de datos: ¿cómo te afectan?», organizó el 28 de enero de 2010 un almuerzo-coloquio en la sede de la Comisión Europea, durante el cual Peter Hustinx ofreció una presentación al personal de la Comisión y respondió a las preguntas sobre sus derechos relativos a la protección de datos y sobre la forma de ejercerlos en el marco de la administración de la UE.

También se distribuyó un mensaje grabado en vídeo del Supervisor y el Supervisor adjunto entre las partes interesadas institucionales, disponible asimismo en el sitio web, en el que se explican las funciones del SEPD y se resumen sus retos futuros.

El SEPD participó igualmente en los diversos actos organizados en Bruselas con ocasión del Día de la Protección de Datos, como la conferencia y ceremonia de entrega de premios con la que se clausuró la campaña «Piensa en la intimidad» promovida por la red escolar europea (European Schoolnet) y por Microsoft. Esta campaña incluyó un concurso a escala europea en el que se invitó a jóvenes de 15 a 19 años a crear y exponer una presentación multimedia sobre el tema «La intimidad es un derecho humano: trátala con cuidado».

Los días 29-30 de enero de 2010, el SEPD participó en la conferencia internacional «Ordenadores, intimidad y protección de datos», que trata de tender un puente entre los responsables de la formulación de políticas, el mundo académico, los profesionales y los activistas para establecer un diálogo sobre los nuevos problemas surgidos en el ámbito de la intimidad, la protección de datos y las tecnologías de la información. En esta cuarta edición, el lema de la conferencia fue «El problema de elegir» en referencia a las múltiples opciones posibles en la política de protección de datos. Miembros de la secretaría del SEPD participaron en el debate del grupo de expertos, y Peter Hustinx pronunció el discurso de clausura de la conferencia.

Peter Hustinx, SEPD, durante su alocución en la conferencia y ceremonia de entrega de premios sobre el tema «Piensa en la intimidad» (Bruselas, 28 de enero de 2010)

5.8.2. Jornada de Puertas Abiertas de la UE

El 8 de mayo de 2010, la oficina del SEPD participó, como ya es habitual cada año, en la Jornada de Puertas Abiertas de las Instituciones Europeas, organizada en el Parlamento Europeo en Bruselas.

Se trata de una oportunidad excelente para mejorar la sensibilización del público en general sobre la necesidad de proteger su intimidad y su información personal.

El SEPD dispuso de un espacio de información situado en el edificio principal del Parlamento Europeo, y colaboradores de su secretaría estuvieron presentes para contestar a las preguntas de los visitantes. Como en el Día de la Protección de Datos, el SEPD distribuyó material informativo entre los visitantes de su stand, a quienes propuso también un juego de preguntas sobre derecho a la intimidad y protección de datos.

Los visitantes rellenan el juego de preguntas sobre protección de datos durante la Jornada de Puertas Abiertas de la UE.

6 ADMINISTRACIÓN, PRESUPUESTO Y PERSONAL

6.1. Introducción

Monique Leens, Jefa de Administración de la Secretaría del SEPD desde su fundación, se jubiló en junio de 2010. Su contribución a la organización del SEPD durante los últimos seis años ha sido crucial, y le deseamos lo mejor para su merecida jubilación. A raíz de su marcha, Christopher Docksey, funcionario del Servicio Jurídico de la Comisión Europea, asumió interinamente el puesto de Director del SEPD, y la Secretaría fue reforzada con la incorporación de Leonardo Cervera Navas, también de la Comisión Europea, como Jefe de RR.HH., Presupuesto y Administración.

La plantilla aumentó de forma importante en 2010. Después de publicadas las listas de reserva de los concursos generales organizados por el SEPD para puestos relacionados con la protección de datos, se contrataron doce nuevos funcionarios. Para ello fue preciso no solo encontrar nuevo espacio de oficinas, sino también adoptar un nuevo organigrama que permitiera responder a las necesidades de una organización de mayor tamaño, responsable de nuevas y complejas tareas.

La reorganización del SEPD, iniciada con una nota interna en abril de 2010, continuó a lo largo del año, con la colaboración de un consultor de dirección externo. Se prevé que estos trabajos continuarán a lo largo de 2011, incorporando al contenido de los mismos la estrategia y la gestión del rendimiento.

6.2. Presupuesto

La autoridad presupuestaria asignó al SEPD un presupuesto de 7 104 351 euros, lo que representa un incremento del 6,62 % en comparación con el ejercicio anterior.

Este incremento es el correspondiente a las necesidades de una organización mayor, con más personal, nuevas actividades y responsabilidad añadidas como consecuencia de la entrada en vigor del Tratado de Lisboa. Además de los gastos de personal y inmuebles, una parte importante del presupuesto del SEPD se destina a traducciones, ya que sus dictámenes sobre propuestas legislativas deben traducirse a todas lenguas oficiales y publicarse en el *Diario Oficial de la Unión Europea* Los dictámenes de control previo y demás documentos publicados se traducen igualmente a las lenguas de trabajo del SEPD (inglés, francés y alemán).

La Declaración de fiabilidad 2009 del Tribunal de Cuentas Europeo no instó a realizar cambios importantes. El informe final incluía solamente dos recomendaciones: la mejora de las normas de control interno mediante la adopción de un sistema de verificación *ex-post* y la creación de un registro centralizado de excepciones a los procedimientos financieros ordinarios.

La Comisión siguió prestando asistencia en 2010 al SEPD en los temas financieros, en concreto en los servicios de contabilidad, ya que su contable actúa asimismo como contable del SEPD. En este contexto, la Dirección General de Presupuestos de la Comisión realizó una validación de los sistemas de

contabilidad, informando positivamente sobre ellos. La principal recomendación del informe fue el nombramiento de un corresponsal contable.

Todas las recomendaciones del Tribunal de Cuentas Europeo y de la Comisión se han aplicado de la manera siguiente:

a) se ha introducido un nuevo sistema de verificación financiera interna en el flujo de trabajo relativo a las finanzas;

b) se ha designado un contable;

c) se ha creado un registro centralizado de excepciones, y

d) se está adoptando un sistema de verificación *ex-post*.

Como consecuencia de la reorganización del SEPD, Christopher Docksey, Director interino del SEPD, ha sido nombrado ordenador de pagos delegado, y Leonardo Cervera Navas, Jefe de RR.HH., Presupuesto y Administración, ordenador de pagos subdelegado. Esta nueva estructura proporciona una mayor flexibilidad y refuerza el proceso de autorización de las transacciones financieras del SEPD.

Siempre que no se hayan establecido disposiciones específicas, el SEPD aplica en su ejecución presupuestaria las normas internas de la Comisión.

6.3. Recursos humanos

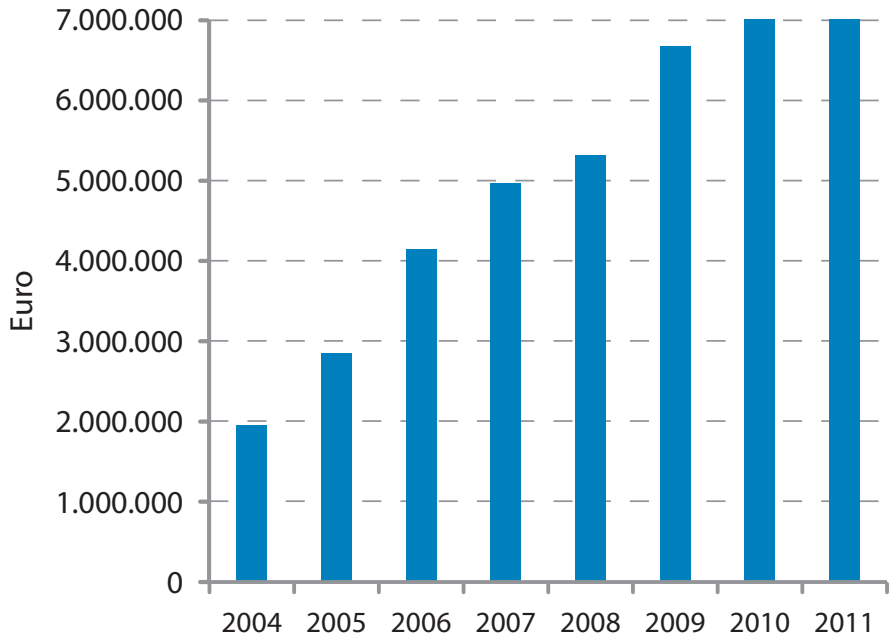
6.3.1. Contratación de personal

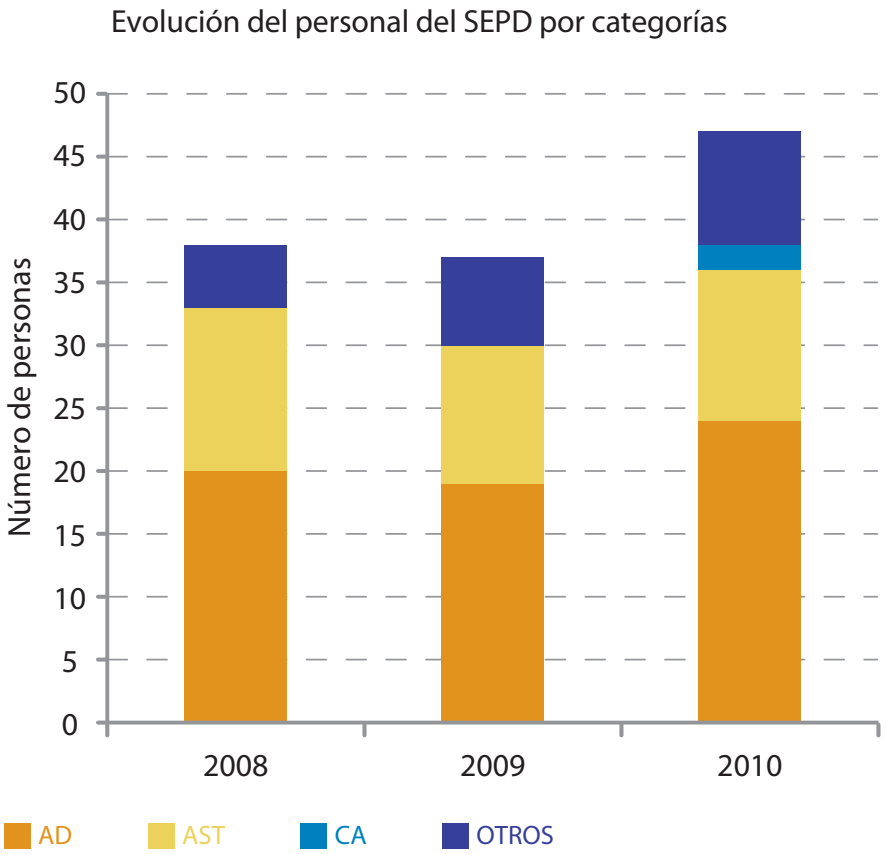
Al igual que en años anteriores, y como queda reflejado en los capítulos precedentes del presente Informe, la creciente visibilidad pública del SEPD está generando una mayor carga de trabajo y una expansión de sus actividades que ha de ser abordada desde la perspectiva de los recursos humanos.

Gracias a un acuerdo de nivel de servicio, el SEPD se benefició de los servicios de la Oficina Europea de Selección de Personal (EPSO), participando en su Consejo de Administración en calidad de observador. Por ese motivo, en estrecha cooperación con la EPSO, el SEPD convocó en 2009 una oposición para seleccionar personal especializado en protección de datos. En el verano de 2010 estuvieron disponibles las tres listas de reserva correspondientes a los niveles AD9, AD6 y AST3. La validez de estas listas de reserva ha sido prorrogada hasta finales de 2011 como mínimo.

A raíz de la publicación de estas listas, el SEPD emprendió un importante proceso de selección, entrevistando a los candidatos incluidos en ellas y a funcionarios de otras instituciones, de conformidad con el artículo 29 del Estatuto de los funcionarios. A lo largo de 2010, el SEPD contrató a doce funcionarios e introdujo por primera vez una nueva

Evolución del presupuesto del SEPD 2004-2011





categoría de personal, los agentes contractuales En el contexto del proceso de selección de candidatos elegidos de las listas CAST, se incorporaron asimismo dos nuevos agentes contractuales. Para atender necesidades temporales, en 2010 se contrató además a una secretaria interina. En total, el SEPD contrató a 15 personas durante el año.

Finalmente, la vacante para el puesto de Director del SEPD se publicó a finales de 2010 en el sitio web interinstitucional, y se prevé que este procedimiento de selección para altos directivos esté concluido en el primer semestre de 2011.

6.3.2. Programa de prácticas

En 2005 se creó un programa de prácticas con el objetivo de ofrecer a jóvenes titulados universitarios la posibilidad de aplicar sus conocimientos académicos y adquirir experiencia práctica en las actividades diarias del SEPD. También brinda al SEPD la oportunidad de aumentar su visibilidad entre los ciudadanos jóvenes de la UE, en particular entre los estudiantes universitarios y los titulados jóvenes que se han especializado en la protección de datos.

El programa principal permite ofrecer un contrato en prácticas a una media de dos personas por periodo, con dos periodos de cinco meses por año (de marzo a julio y de octubre a febrero). En situaciones excepcionales, y con sujeción a criterios de admisión estrictos, el SEPD puede acoger igualmente a doctorandos que deseen realizar prácticas no remuneradas. Todas las personas en prácticas, remuneradas o no, contribuyeron tanto al trabajo teórico como al práctico y adquirieron experiencia útil de primera mano.

Con arreglo a los acuerdos de nivel de servicio suscritos con la Comisión, el SEPD contó con la asistencia administrativa de la Oficina de Prácticas de la Dirección General de Educación y Cultura, que siguió prestando un valioso apoyo gracias a la dilatada experiencia de su personal.

6.3.3. Programa para expertos nacionales en comisión de servicios

El programa para expertos nacionales en comisión de servicios (ENCS) se puso en marcha en enero de 2006. Cada año se han recibido en comisión de servicios a una media de dos expertos enviados por

las autoridades nacionales responsables de la protección de datos de diferentes Estados miembros. Este sistema permitió al SEPD beneficiarse de las capacidades y la experiencia profesional de los expertos y aumentar su visibilidad a nivel nacional. Al mismo tiempo, brinda a los expertos nacionales la oportunidad de familiarizarse con asuntos de protección de datos en el entorno de la UE.

6.3.4. Organigrama

El organigrama del SEPD había permanecido inalterado desde su creación en 2004 hasta 2009, año en que se efectuó la primera reorganización con la creación del puesto de Director como Jefe de Secretaría.

En 2010 el organigrama fue objeto de una modificación importante, y su personal se distribuyó en cinco sectores: Supervisión y Aplicación, Política y Consulta, Registro y Apoyo Operativo, Información y Comunicación, y Recursos Humanos, Presupuesto y Administración. Como jefes de unidad fueron designados directivos de la escala intermedia. En la nueva estructura organizativa, el Director representa al SEPD en el ámbito de la gestión y garantiza la aplicación de las políticas y la coordinación horizontal de las actividades. El Supervisor y el Supervisor adjunto conservan la responsabilidad última de la gestión, pero ahora se pueden concentrar más en la formulación de políticas y en las relaciones interinstitucionales.

Estos cambios se han reflejado en un nuevo organigrama, que está disponible en el sitio web del SEPD.

6.3.5. Formación

Una de las prioridades de 2010 consistió en ofrecer al personal mejores oportunidades de formación y desarrollo profesional. Se suscribió una nuevo acuerdo de nivel de servicio con el Departamento de RR.HH. de la Comisión Europea, el cual permitirá acceder por vía electrónica al catálogo de cursos de formación de la Comisión a primeros de 2011. A partir de ese momento, los miembros del personal del SEPD podrán beneficiarse del sistema SYSLOG para disfrutar de las mismos oportunidades de formación que los funcionarios de la Comisión.

Muchos de los miembros del personal han asistido a cursos de idiomas y han tenido acceso a la formación organizada a nivel interinstitucional y a la formación externa en caso necesario. El curso titulado «Programa de Eficiencia Personal (PEP)», organizado específicamente para el SEPD, obtuvo un éxito notable. Fue impartido en 2010 a los funcionarios de los tres sectores, y los restantes miembros del personal podrán recibirlo durante el primer semestre de 2011.

Con motivo de la reorganización del SEPD, los nuevos directivos recibieron formación y entrenamiento específicos en temas de gestión, tanto a nivel individual como de equipo.

El SEPD siguió participando en los comités interinstitucionales (Grupo de trabajo interinstitucional y Grupo de evaluación de la formación de la Escuela Europea de Administración (EAS), Comité interinstitucional para la formación lingüística) con el fin de conjugar esfuerzos y obtener economías de escala en un área en la que las necesidades son básicamente las mismas en todas las instituciones de la UE. Al igual que en años anteriores, el SEPD suscribió, junto con otras instituciones, el protocolo sobre la armonización del coste de los cursos interinstitucionales de idiomas y el nuevo protocolo sobre la distribución entre las instituciones de los costes de los proyectos pedagógicos sobre terminología interinstitucional.

Durante 2011, el SEPD continuará realizando esfuerzos para mejorar las oportunidades de formación y desarrollo profesional de su personal. También se ha previsto actualizar la Decisión sobre formación de 18 de julio de 2007, en estrecha consulta con el personal.

6.3.6. Actividades sociales

El SEPD firmó un acuerdo de cooperación con la Comisión para facilitar la integración del nuevo personal mediante la prestación, por ejemplo, de asistencia jurídica para temas privados (contratos de alquiler, adquisición de vivienda, etc.) y el ofrecimiento de la posibilidad de participar en diversas actividades sociales y en red. El Supervisor, el Supervisor adjunto y el Director del SEPD dan personalmente la bienvenida al personal recién incorporado. Éste se reúnen, además de con su mentor, con responsables del sector de RR.HH., Presupuesto y Administración, quienes le entregan la guía administrativa del SEPD y otra información sobre los procedimientos específicos.

El SEPD continuó desarrollando la cooperación interinstitucional en el ámbito de la atención a la infancia: los hijos del personal del SEPD tienen

acceso a los jardines de infancia, las guarderías postescolares y los demás centros infantiles al aire libre de la Comisión, así como a las Escuelas Europeas. El SEPD participa como observador en el Comité consultivo de prevención y protección en el trabajo del Parlamento Europeo, cuyo objetivo es mejorar el entorno de trabajo.

En 2010, los sectores de nueva creación organizaron sus propias jornadas de convivencia para promover el espíritu de equipo y ayudar a los recién incorporados a integrarse. Se celebró una fiesta de Navidad para todos los miembros del personal, en la que los antiguos tuvieron ocasión de dar la bienvenida a los nuevos compañeros y de rememorar un año muy intenso, lleno de cambios.

6.4. Funciones de control

6.4.1. Control interno

El sistema de control interno, que funciona desde 2006, garantiza que los objetivos del SEPD se alcancen con eficacia y de conformidad con la normativa. El SEPD ha adoptado procedimientos de control interno específicos, acordes con sus necesidades, con su tamaño y con sus actividades. El sistema no está diseñado para eliminar el riesgo de incumplimiento de los objetivos institucionales, sino para gestionarlo.

El SEPD tomó conocimiento del Informe anual de actividad y de la declaración de fiabilidad firmada por el ordenador delegado. En general, el SEPD considera que los sistemas de control interno aplicados ofrecen una fiabilidad razonable de la legalidad y la regularidad de las operaciones de las que es responsable. No obstante, el 2010 se puso en marcha un planteamiento más ambicioso, ampliando la lista de medidas para la aplicación de las Normas de Control Interno (NCI) con el fin de garantizar un control interno más eficiente de los procesos aplicados.

A título de ejemplo, se elaboraron nuevos manuales de casos prácticos que permiten una mejor gestión de procesos tales como los relacionados con el control previo, las reclamaciones o los asuntos judiciales. Se desarrollaron medidas como la mejora de la sensibilización sobre los aspectos éticos, la adopción de unas descripciones más detalladas de los puestos de trabajo, la elaboración de normas internas adicionales y el establecimiento de un nuevo sistema de mentoría, tras intensas consultas con el personal y contando con el pleno apoyo de los Supervisores.

6.4.2. Auditoría interna

El auditor interno de la Comisión es también el auditor interno del SEPD. Para garantizar la gestión eficaz de los recursos, el auditor interno lleva a cabo verificaciones periódicas de los sistemas de control interno de la institución, así como de sus operaciones financieras.

A raíz de una visita de auditoría de seguimiento realizada en diciembre de 2008 por el Servicio de Auditoría Interna (SAI), un informe emitido en mayo de 2009 confirmó que el SEPD había logrado sus objetivos, aunque identificó asimismo algunas cuestiones susceptibles de mejora. Algunas de ellas ya han sido resueltas, y otras son objeto de revisión a medida que avanza el proceso de reorganización del SEPD.

El SAI ha programado una evaluación de riesgo para los primeros meses de 2011, con vistas a la realización de una auditoría en el transcurso del año.

6.4.3. Seguridad

En diciembre de 2010, el SEPD decidió nombrar a dos miembros del personal, respectivamente, responsable local de seguridad (LSO) y responsable local de seguridad de la información (LISO), además de los correspondientes LSO y LISO adjuntos, en ambos casos en régimen de trabajo a tiempo parcial. Se han establecido los contactos iniciales con los servicios de la Comisión Europea y del Parlamento Europeo, habiéndose convenido un primer ámbito de cooperación. Se ha iniciado el proceso para obtener la correspondiente habilitación. Las medidas ulteriores estarán centradas en la seguridad de la información y de las tecnologías de la información (TI), y en particular en el desarrollo del sistema interno de gestión de casos del SEPD.

En 2011 el SEPD seguirá desarrollando la Decisión sobre seguridad adoptada a finales de 2008, que incluye medidas relativas a la administración de la información confidencial y de la seguridad informática, así como a las condiciones de salud y seguridad del personal y de las instalaciones.

6.5. Infraestructuras

En cumplimiento del acuerdo de cooperación administrativa, el SEPD ocupa locales del Parlamento Europeo, el cual presta además ayuda adicional, principalmente en materia de tecnologías de la información e infraestructura. Como consecuencia del significativo aumento de la plantilla registrado en 2010, se consiguió espacio de oficina suplementario con la colaboración del Parlamento Europeo.

El edificio que alberga al SEPD fue renovado parcialmente en 2010. Esta renovación, realizada bajo la supervisión del Parlamento Europeo, ha mejorado notablemente el nivel de comodidad y bienestar en el trabajo. Sin embargo, las limitaciones de espacio constituyen un serio problema para el SEPD, habiendo sido objeto de diversas reuniones con el Parlamento Europeo.

El SEPD siguió gestionando de modo independiente su inventario de mobiliario y equipos informáticos, asistido por los servicios del Parlamento Europeo.

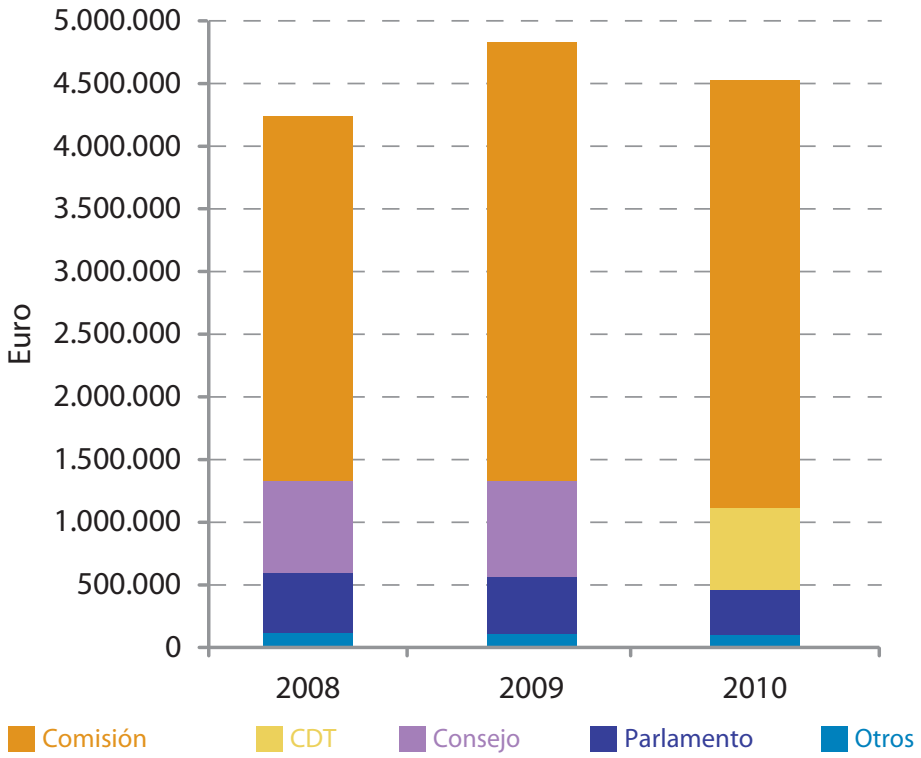
6.6. Entorno administrativo

6.6.1. Asistencia administrativa y cooperación interinstitucional

El SEPD se beneficia de la cooperación institucional en muchas áreas, como consecuencia del acuerdo suscrito en 2004 con el Secretario General de la Comisión, el Parlamento y el Consejo, prorrogado en 2006 (por un plazo de tres años) y en 2010 (por un plazo de dos años). Esta cooperación resulta esencial para el SEPD, ya que mejora su eficiencia y le permite alcanzar economías de escala.

Durante 2010 continuó la cooperación interinstitucional con diversas Direcciones Generales de la Comisión (Personal y Administración, Presupuestos, Servicio de Auditoría Interna y Educación y Cultura), la Oficina de Gestión y Liquidación de los Derechos Individuales, la Escuela Europea de Administración (EAS), distintos servicios del Parlamento Europeo (servicios informáticos, particularmente en lo que se refiere al mantenimiento y desarrollo del sitio web del SEPD, adaptación de los locales, seguridad

Ejecución presupuestaria del SEPD
a través de la cooperación interinstitucional



de los edificios, imprenta, correo, teléfono, material de oficina, etc.). En muchos casos, esta cooperación reviste la forma de acuerdos de nivel de servicio que se actualizan periódicamente. El SEPD siguió participando en las licitaciones interinstitucionales, lo que permitió a la institución aumentar su eficiencia en muchas áreas administrativas y avanzar hacia una mayor autonomía.

El acuerdo con el Consejo Europeo sobre los servicios de traducción venció en enero de 2010, firmándose un nuevo acuerdo con el Centro de Traducción de los Órganos de la Unión Europea, que ha asumido los trabajos de traducción a partir de 2010.

El SEPD es miembro de diversos comités interinstitucionales, como el Colegio de Jefes de Administración, el Comité de Gestión del Seguro de Enfermedad, el Comité de Preparación de las Cuestiones Estatutarias, el Comité del Estatuto, el Grupo de trabajo interinstitucional/EAS, el Consejo de Administración y el grupo de trabajo de la EPSO y la Comisión Paritaria Común. Es miembro asimismo del Comité de preparación de los asuntos sociales y participa en el grupo de trabajo *ad hoc* dedicado a la aplicación en las instituciones europeas de la Convención de las Naciones Unidas sobre los derechos de las personas con discapacidades. Esta participación le permitió aumentar su visibilidad entre otras instituciones y propició el intercambio de buenas prácticas.

6.6.2. Normas internas

La adopción de normas internas para el funcionamiento sin problemas del SEPD es un proceso continuo. En las áreas en que el SEPD cuenta con la asistencia de la Comisión o del Parlamento Europeo, las normas son similares a las aplicadas en ambas instituciones, aunque con ciertas adaptaciones para atender a las características particulares del SEPD.

El SEPD es una institución relativamente joven que ha crecido rápidamente. En consecuencia, las normas y procedimientos que resultan apropiados durante los primeros años de actividad pueden llegar a ser menos efectivos en el futuro, en el marco de una estructura más grande y compleja. Por este motivo se someten las normas a una evaluación permanente, que puede llevar a su modificación durante los próximos años. Esta labor se inició en 2010 con el objetivo de modificar el Código de buena conducta del SEPD.

6.6.3. Gestión documental

Con la ayuda de los servicios del Parlamento Europeo, en enero de 2009 se implantó un nuevo sistema de gestión del correo electrónico (GEDA) para las tareas administrativas. Tras este primer paso, se realizaron estudios dirigidos al establecimiento de un sistema apropiado de gestión de documentos y expedientes para el departamento de protección de datos.

A lo largo de 2010 se elaboró un conjunto detallado de requisitos para un sistema adecuado de gestión documental y de expedientes que incluyera la gestión de casos del SEPD. Se encargó a consultores externos la realización de un análisis de mercado basado en estos requisitos, con el fin de identificar las posibles soluciones. La DG de Innovación y Apoyo Tecnológico del Parlamento Europeo (ITEC) sigue respaldando y colaborando con el SEPD en este proceso. Se ha formado un equipo interno de proyecto, dirigido por el Jefe de Registro y Apoyo Operativo. Los miembros de este equipo multidisciplinario representan a los cinco sectores de la oficina.

Paralelamente a estos cambios tecnológicos, el sector de Registro y Apoyo Operativo ha seguido con su gestión precisa de los expedientes. Se ha adoptado un plan de archivo para cuatro de los cinco sectores, y se han simplificado los procedimientos para el registro del correo, en consonancia con el nuevo organigrama del SEPD. Se ha prestado una atención especial a las necesidades de la Dirección del SEPD en materia de informes. Todos los sectores han definido y recopilado la información específica relativa a los expedientes, al objeto de mejorar el seguimiento de los mismos.

7 EL RESPONSABLE DE PROTECCIÓN DE DATOS DEL SEPD

7.1. Un nuevo equipo del RPD en el SEPD

Al igual que las restantes instituciones europeas, el SEPD se encuentra sometido a determinadas obligaciones legales relacionadas con la protección de datos. Tales obligaciones son las definidas en el Reglamento sobre protección de datos (Reglamento (CE) nº 45/2001).

Además de describir los principios jurídicos que rigen el tratamiento de los datos personales por la administración de la UE, este Reglamento establece que todas las instituciones y organismos europeos deben designar como mínimo un responsable de la protección de datos (RPD).

En septiembre de 2010, el SEPD nombro un **nuevo RPD** y decidió nombrar también un **RPD adjunto**. Con estos nombramientos, el SEPD dedica esfuerzos adicionales a este tema, con el fin de elevar rápidamente los niveles de cumplimiento.

La función del RPD en el SEPD presenta múltiples desafíos: ser independiente dentro de de una institución independiente, estar a la altura de las elevadas expectativas de unos compañeros que están especialmente alerta y sensibilizados en relación con los problemas de la protección de datos y encontrar soluciones que puedan servir de referencia para otras instituciones.

7.2. Plan de acción y normas de aplicación

El equipo del RPD recién nombrado distribuyó entre el personal un exhaustivo **Plan de acción** en el que se señalan las prioridades correspondientes. En él se destacan las cuatro áreas de actuación en las que el equipo del RPD hará un hincapié especial: aspectos organizativos, función de asesoramiento, información y mejora de la sensibilización.

Un primer paso importante fue la adopción en octubre de 2010 de las **normas de aplicación del RPD,** que se basan en las normas similares de otras instituciones y en las directrices del SEPD, adaptadas a las características específicas del SEPD. Por ejemplo, la garantía de que el RPD solo puede ser despedido con la autorización del SEPD se ha adaptado para exigir la autorización tanto del Supervisor como del Supervisor adjunto. Por otro lado, inspirándose en el documento relativo a los RPD, las normas de aplicación insisten en la necesidad de conocer en profundidad la protección de datos, así como en la independencia del proceso de elaboración de informes.

7.3. Un registro de operaciones de proceso de datos de fácil acceso

El equipo del RPD hizo una verificación completa del **inventario de las operaciones de proceso de datos existentes** y mejoró la sensibilización del personal sobre ellas, con objeto de garantizar la notificación de todas las operaciones realizadas en el SEPD. Para ello se invitó a los responsables a informar sobre las operaciones no notificadas aún. El RPD prestó también el asesoramiento necesario para preparar las nuevas notificaciones o completar las pendientes.

Se ha puesto a disposición de los usuarios una versión en Internet del registro de operaciones de tratamiento. Esta versión electrónica contiene un hipervínculo con todas las notificaciones finales, lo que facilita el acceso de los usuarios que desean consultar dicho registro, de acuerdo con lo dispuesto en el artículo 26 del Reglamento sobre protección de datos.

El equipo del RPD también actualizó y mejoró los formularios de notificación utilizados en los informes sobre el tratamiento de datos personales por la secretaría del SEPD.

7.4. Ejercicio de primavera

El equipo del RPD continuó la secuencia de «ejercicios de primavera» (véase la sección 2.5.2.), para actualizar la información del SEPD relativa al cumplimiento de los preceptos de la protección de datos dentro de la institución. En un escrito dirigido al SEPD a comienzos de 2011 destacó los logros alcanzados y se reafirmó en su propósito de reforzar el cumplimiento y la sensibilización sobre la protección de datos a partir del plan de acción del RPD, especialmente en el área de recursos humanos.

7.5. Información y mejora de la sensibilización

El equipo del RPD atribuye una gran importancia a la mejora de la sensibilización y a la comunicación sobre el cumplimiento de la normativa de protección de datos por parte del SEPD, tanto en el plano externo como interno.

En el plano de la **comunicación externa,** se ha incluido una sección dedicada el RPD en el sitio web, con información básica sobre sus funciones y actividades. También se hallan disponibles en línea las normas de aplicación y el registro del operaciones de tratamiento del SEPD.

Por otro lado, el equipo del RPD participó en las **reuniones de la red de RPDs**, lo que representa una oportunidad singular para entrar en contacto, dialogar sobre los problemas comunes y compartir las buenas prácticas. Desempeñó asimismo un papel activo en las actividades organizadas en el marco del Día de la Protección de Datos.

En el plano de la **comunicación interna,** la intranet recientemente creada constituye también una oportunidad excelente para comunicarse con el personal. La sección dedicada al RPD en ella contiene información útil para todo el personal, siendo sus temas principales la función del RPD, las normas de aplicación, el Plan de acción del RPD y la información sobre sus actividades. El equipo del RPD tiene también la intención de utilizar este espacio virtual para mejorar la visibilidad de la información facilitada a los titulares de datos, con arreglo a lo establecido en los artículos 11 y 12 del Reglamento. A este respecto, comenzó a publicar en la intranet referencias a las declaraciones de intimidad relacionadas con las operaciones de tratamiento realizadas en el SEPD, al objeto de hacerlas fácilmente accesibles a todo el personal.

8 PRINCIPALES OBJETIVOS PARA 2011

Para 2011 se han seleccionado los siguientes objetivos. El año próximo se informará de los resultados que se obtengan.

8.1. Supervisión y aplicación

De acuerdo con el documento de orientación sobre cumplimiento y aplicación publicado en diciembre de 2010, el SEPD ha definido los objetivos siguientes en este ámbito:

- **Mejora de la sensibilización**

El SEPD seguirá dedicando tiempo y recursos a prestar asesoramiento y orientación en temas relacionados con la protección de datos. Esta labor de mejora de la sensibilización se realizará a través de documentos de orientación sobre asuntos seleccionados, así como de talleres o seminarios interactivos en los que el SEPD expondrá sus puntos de vista sobre alguna cuestión concreta.

- **Función de control previo**

Teniendo en cuenta que el número de controles previos *ex-post* pendientes de realización se ha reducido prácticamente a cero, el SEPD se concentrará en el análisis de los efectos que puedan derivarse de las nuevas actividades de tratamiento de datos. El SEPD continuará insistiendo en la aplicación de las recomendaciones incluidas en los dictámenes de control previo y garantizará un adecuado seguimiento de las mismas.

- **Seguimiento y presentación de informes**

El SEPD seguirá vigilando la aplicación de las normas de protección de datos por parte de las instituciones y organismos de la UE, tanto mediante un ejercicio de control general (primavera de 2011) como mediante ejercicios específicos de control en los casos en que el nivel de conformidad de determinadas instituciones u organismos sea motivo de preocupación.

- **Inspecciones**

Se realizarán inspecciones sobre el terreno en los casos en que el SEPD tenga sólidas razones para creer que los mecanismos que aseguran la conformidad están bloqueados. Dichas inspecciones constituyen la fase previa a la adopción de medidas formales de aplicación. También se llevarán a cabo inspecciones y auditorías en relación con los sistemas informáticos a gran escala que operen en el ámbito de competencias del SEPD.

8.2. Política y consulta

Los principales objetivos se ajustan a las prioridades establecidas para este ámbito en 2011 y publicadas en el sitio web. Además, se han definido objetivos dirigidos a la cooperación con las autoridades de protección de datos y a la supervisión coordinada de los sistemas informáticos a gran escala.

- **Alcance de la consulta**

El SEPD continuará emitiendo los oportunos dictámenes u observaciones sobre propuestas de nueva legislación y garantizará su adecuado seguimiento en los ámbitos pertinentes. Se prestará una atención especial, como se indica a continuación, a la revisión del marco jurídico, a la aplicación del Programa de Estocolmo y a las iniciativas en el ámbito de la tecnología.

- **Revisión del marco jurídico**

El SEPD dará prioridad al desarrollo de un marco jurídico integral para la protección de datos en la UE. Para ello emitirá un dictamen sobre la Comunicación de la Comisión relativa a un enfoque global de la protección de datos personales, y sobre cualquier otra propuesta legislativa ulterior, contribuyendo al debate siempre que sea necesario y apropiado.

- **Ejecución del Programa de Estocolmo**

El SEPD seguirá dedicando gran atención a las diferentes iniciativas relacionadas con la ulterior ejecución del Programa de Estocolmo para el espacio de libertad, seguridad y justicia, como por ejemplo la creación de un sistema de entrada y salida y el Programa de Registro de Pasajeros, la Directiva prevista sobre el uso del registro de nombres de pasajeros para fines policiales y la introducción de un Programa europeo de seguimiento de la financiación del terrorismo.

- **Iniciativas en el ámbito de la tecnología**

El SEPD seguirá analizando a fondo en 2011 las iniciativas tecnológicas que puedan afectar a la intimidad y protección de datos, y en particular seguirá controlando la aplicación de las medidas de la estrategia Europa 2020 relacionadas con las tecnologías de la información e incluidas en la Agenda digital, como los dispositivos RFID, la computación en la nube, la administración electrónica y la aplicación en línea de los derechos de propiedad intelectual.

- **Otras iniciativas**

El SEPD prestará la atención debida a cualquier otra innovación que pueda afectar de manera significativa la protección de datos, por ejemplo en el área del transporte (uso de escáneres corporales en los aeropuertos, paquetes de movilidad electrónica) y en los intercambios de datos a gran escala realizados en el marco del Sistema de Información del Mercado Interior.

- **Cooperación con las autoridades de protección de datos**

El SEPD seguirá contribuyendo de forma activa a las tareas y a los objetivos del Grupo de trabajo del artículo 29, tratando de influir en la programación de sus actividades al objeto de alinearlas con sus propias prioridades, garantizando la coherencia y las sinergias entre el Grupo de trabajo y sus propias posiciones y manteniendo relaciones constructivas con las autoridades nacionales de protección de datos. En su calidad de ponente en expedientes específicos, el SEPD dirigirá y organizará la aprobación de los dictámenes del Grupo de trabajo.

- **Supervisión coordinada**

La legislación de la UE prescribe la supervisión coordinada en el caso de Eurodac, del Sistema de Información Aduanera y, a partir de mediados de 2011, del Sistema de Información de Visados. Un objetivo importante del SEPD consistirá en poner a disposición de las autoridades de protección de datos que intervengan en la supervisión coordinada un servicio de secretaría eficiente. Como supervisor de los sistemas informáticos a gran escala, el SEPD participará activamente en dicha supervisión coordinada, llevando a cabo con regularidad auditorías de seguridad.

8.3. Otros ámbitos

- **Información y comunicación**

Se seguirán desarrollando y mejorando las actividades de información, comunicación y contacto con la prensa, dedicando una atención especial a la mejora de la sensibilización, las publicaciones y la información en Internet. El SEPD culminará los preparativos necesarios para revisar su estrategia de comunicación, en particular mediante la realización de consultas con las principales partes interesadas. Esta tarea de carácter general se complementará con evaluaciones más específicas sobre los efectos de las principales herramientas de información y comunicación.

- **Organización interna**

Los objetivos más destacados para 2011 consistirán en la conclusión de la reorganización interna, la intensificación de los esfuerzos dirigidos a la gestión del rendimiento en el contexto de una revisión estratégica, y el desarrollo e implantación de nuevas herramientas informáticas. Se prestará

asimismo una atención especial al control interno y a los procedimientos correspondientes, a una asignación de recursos más eficiente y a la mejora de la ejecución presupuestaria.

- **Gestión de recursos**

El SEPD seguirá invirtiendo recursos en el desarrollo y aplicación de un sistema de gestión de expedientes. Se asignará asimismo una alta prioridad a la conclusión de los acuerdos de nivel de servicio con la Comisión Europea para el despliegue de las aplicaciones informáticas en el área de recursos humanos (por ejemplo, Syslog Formation, Sysper y Mission Processing).

Anexo A. Marco jurídico

El artículo 286 del Tratado CE, adoptado en 1997 como parte del Tratado de Ámsterdam, estipula que los actos comunitarios relativos a la protección de las personas respecto del tratamiento de datos personales y a la libre circulación de dichos datos son de aplicación a las instituciones y organismos comunitarios, y dispone que se establezca un organismo de vigilancia independiente.

Los actos comunitarios a que se refiere esta disposición son la Directiva 95/46/CE, que establece un marco general para la legislación de los Estados miembros sobre protección de datos, y la Directiva 97/66/CE, una Directiva sectorial que fue sustituida por la Directiva 2002/58/CE, relativa a la protección de la intimidad en el sector de las comunicaciones electrónicas. Puede considerarse que ambas Directivas son el resultado de una evolución jurídica que se inició a comienzos de la década de los setenta en el Consejo de Europa (véase más abajo).

Sobre la base del artículo 286 del Tratado CE, el Supervisor Europeo de Protección de Datos fue establecido por el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en los que respecta al tratamiento de datos personales por las instituciones y organismos comunitarios y a la libre circulación de estos datos, el cual entró en vigor en 2001 ([23]). Este Reglamento define asimismo las normas aplicables a las instituciones y organismos con arreglo a las Directivas antes mencionadas.

([23]) DO L 8, de 12.1.2001, p. 1.

Desde la entrada en vigor del Tratado de Lisboa, el ya mencionado artículo 286 ha quedado sustituido por el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE), que insiste en la importancia de la protección de los datos personales de una manera más general. Tanto el artículo 16 del TFUE como el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, ahora vinculante, disponen que las normas de protección de datos se sometan al control de una autoridad independiente.

Antecedentes

El artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales establece el derecho al respeto de la vida privada y familiar, admitiéndose restricciones únicamente en determinadas condiciones. No obstante, en 1981 se consideró necesario adoptar un convenio separado para la protección de datos de carácter personal, a fin de desarrollar un enfoque positivo y estructural de la protección de los derechos humanos y las libertades fundamentales, que pueden verse afectados por el tratamiento de datos personales en una sociedad moderna. Dicho convenio, también conocido como Convenio 108, ha sido ratificado hasta el momento por más de 40 Estados miembros del Consejo de Europa, entre los que se cuentan todos los Estados miembros de la UE.

La Directiva 95/46/CE se basaba en los principios del Convenio 108, aunque los precisaba y desarrollaba en muchos aspectos. Tenía por objeto garantizar un alto grado de protección de los datos personales y la libre circulación de dichos datos dentro de la UE. Cuando la Comisión presentó la propuesta de esta Directiva a comienzos de los años noventa, indicó que las instituciones y organismos comunitarios debían quedar cubiertos por garantías legales similares que les permitiesen participar en la libre circulación de datos personales, a condición de que respetaran normas de protección equivalentes. Sin embargo, hasta la adopción del artículo 286 del Tratado CE se carecía de fundamento jurídico para este tipo de normativa.

El Tratado de Lisboa, que entró en vigor el 1 de diciembre de 2009, fomenta la protección de los derechos fundamentales de diversas formas. El respeto de la vida privada y familiar y la protección de datos personales reciben trato de derechos fundamentales independientes en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea, que ha adquirido carácter jurídicamente

vinculante, tanto para las instituciones y órganos como para los Estados miembros de la UE cuando aplican el Derecho de la UE. También se trata de la protección de datos como cuestión horizontal en el artículo 16 del Tratado de Funcionamiento de la Unión Europea. Esto indica claramente que la protección de datos se considera un componente básico de la buena gobernanza. La supervisión independiente constituye un elemento esencial de esta protección.

Reglamento (CE) nº 45/2001

Al analizar con más detalle este Reglamento, cabe observar en primer lugar que, de acuerdo con su artículo 3, apartado 1, se aplica al «tratamiento de datos personales por parte de todas las instituciones y organismos comunitarios, en la medida en que dicho tratamiento se lleve a cabo para el ejercicio de actividades que pertenecen al ámbito de aplicación del Derecho comunitario». Sin embargo, desde la entrada en vigor del Tratado de Lisboa y la eliminación de la estructura de pilares – a consecuencia de la cual las referencias a las «instituciones comunitarias» o a la »legislación comunitaria» resultan obsoletas – el Reglamento abarca, en principio, todas las instituciones y organismos de la UE, salvo que otras leyes europeas prevean específicamente lo contrario. Las implicaciones concretas de estos cambios son aún objeto de estudio y pueden requerir de nuevas aclaraciones.

Las definiciones y la sustancia del Reglamento siguen de cerca al planteamiento de la Directiva 95/46/CE. Podría decirse que el Reglamento (CE) n° 45/2001 es la aplicación de esa Directiva a nivel europeo. Esto significa que el Reglamento trata principios generales como el tratamiento justo y legítimo, la proporcionalidad y el uso compatible, las categorías especiales de datos sensibles, la información que debe darse a los interesados, los derechos de éstos, las obligaciones de los responsables del tratamiento (refiriéndose a circunstancias especiales en el plano de la UE, cuando procede) y la supervisión, la aplicación y las vías de recurso. El Reglamento dedica un capítulo especial a la protección de los datos personales y de la intimidad en el contexto de las redes de comunicaciones internas. Dicho capítulo constituye, de hecho, la aplicación a nivel europeo de la Directiva 97/66/CE relativa a la protección de la intimidad en el sector de las telecomunicaciones.

Una característica interesante del Reglamento es que establece la obligación de que las instituciones y organismos comunitarios designen por lo menos una persona como responsable de la protección de datos (RPD). Estos funcionarios tienen la misión de garantizar de forma independiente la aplicación a nivel interno de las disposiciones del Reglamento, incluida la notificación adecuada de las operaciones de tratamiento. Todas las instituciones y la mayoría de los organismos cuentan ya con un responsable de este tipo, en algunos casos desde hace ya muchos años, lo que significa que se ha realizado un trabajo importante para aplicar el Reglamento, incluso en ausencia de una autoridad de control. Además, esos responsables pueden estar en mejores condiciones para prestar asesoramiento o intervenir con prontitud y ayudar a desarrollar buenas prácticas. Dado que los RPD tienen la obligación formal de cooperar con el SEPD, esta es una red de colaboración muy importante y muy apreciada que debe seguir desarrollándose (véase la sección 2.2).

Funciones y competencias del SEPD

Las funciones y competencias del SEPD se describen claramente en los artículos 41, 46 y 47 del Reglamento (véase el Anexo B) en términos tanto generales como específicos. El artículo 41 establece la misión general del SEPD: asegurar que las instituciones y organismos comunitarios respeten los derechos y las libertades fundamentales de las personas físicas, y en especial su intimidad, por lo que se refiere al tratamiento de datos personales. Establece además en líneas generales algunos aspectos específicos de esta misión. Estas responsabilidades generales se desarrollan y se especifican en los artículos 46 y 47 con una lista detallada de funciones y competencias.

Esta presentación de responsabilidades, funciones y competencias sigue esencialmente el mismo modelo que el de los organismos de supervisión nacionales: conocer e investigar las denuncias, llevar a cabo otras indagaciones, informar a los responsables y a los interesados, efectuar controles previos cuando las operaciones de tratamiento presentan riesgos específicos, etc. El Reglamento otorga al SEPD la facultad de obtener el acceso a la información y a los locales pertinentes, cuando sea necesario para las investigaciones. También le permite imponer sanciones y presentar un asunto ante el Tribunal de Justicia. Estas actividades de supervisión se abordan con mayor detenimiento en el capítulo 2 del presente informe.

Algunas funciones presentan características especiales. La tarea de asesorar a la Comisión y a otras

instituciones comunitarias sobre la nueva legislación, que se destaca en el artículo 28, apartado 2, mediante una obligación formal de que la Comisión consulte al SEPD cuando adopte una propuesta legislativa relativa a la protección de datos personales, también se refiere a los proyectos de Directiva y a otras medidas concebidas para ser aplicadas a nivel nacional o incorporadas al Derecho nacional. Esta es una función estratégica que permite al SEPD examinar anticipadamente la incidencia de dichas medidas sobre la intimidad y debatir las posibles alternativas, incluyendo las correspondientes al tercer pilar (cooperación policial y judicial en materia penal). El seguimiento de los cambios que puedan repercutir en la protección de datos personales, y la intervención en asuntos pendientes ante el Tribunal de Justicia son también funciones importantes. Estas actividades de consulta del SEPD se abordan con mayor detenimiento en el capítulo 3.

En la misma línea se encuentra el deber de cooperar con las autoridades nacionales de supervisión y con los organismos de supervisión del tercer pilar. Como miembro del Grupo de trabajo del artículo 29, establecido para asesorar a la Comisión Europea y desarrollar políticas armonizadas, el SEPD tiene ocasión de contribuir a ese nivel. La cooperación con los organismos de supervisión del tercer pilar le permite observar los cambios que se producen en ese contexto y contribuir a un marco más coherente y constante de protección de los datos personales, independientemente del pilar o del contexto específico de que se trate. Esta cooperación se trata más ampliamente en el capítulo 4 del presente informe.

Anexo B. Extracto del Reglamento (CE) nº 45/2001

Artículo 41. El Supervisor Europeo de Protección de Datos

1. Se instituye una autoridad de control independiente denominada Supervisor Europeo de Protección de Datos.

2. Por lo que respecta al tratamiento de los datos personales, el Supervisor Europeo de Protección de Datos garantizará que los derechos y libertades fundamentales de las personas físicas, en particular el derecho de las mismas a la intimidad, sean respetados por las instituciones y los organismos comunitarios.

El Supervisor Europeo de Protección de Datos supervisará y garantizará la aplicación de las disposiciones del presente Reglamento y de cualquier otro acto comunitario relacionado con la protección de los derechos y libertades fundamentales de las personas físicas en lo que respecta al tratamiento de datos personales por parte de una institución u organismo comunitario, y asesorará a las instituciones y a los organismos comunitarios, así como a los interesados, en todas las cuestiones relacionadas con el tratamiento de datos personales. Con este fin ejercerá las funciones establecidas en el artículo 46 y las competencias que le confiere el artículo 47.

Artículo 46. Funciones

El Supervisor Europeo de Protección de Datos deberá:

a) conocer e investigar las reclamaciones, y comunicar al interesado los resultados de sus investigaciones en un plazo razonable;

b) efectuar investigaciones por iniciativa propia o en respuesta a reclamaciones y comunicar a los interesados el resultado de sus investigaciones en un plazo razonable;

c) supervisar y asegurar la aplicación del presente Reglamento y de cualquier otro acto comunitario relacionado con la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de una institución u organismo comunitario, con excepción del Tribunal de Justicia de las Comunidades Europeas cuando actúe en el ejercicio de sus funciones jurisdiccionales;

d) asesorar a todas las instituciones y organismos comunitarios, tanto a iniciativa propia como en respuesta a una consulta, sobre todos los asuntos relacionados con el tratamiento de datos personales, especialmente antes de la elaboración por dichas instituciones y organismos de normas internas sobre la protección de los derechos y libertades fundamentales en relación con el tratamiento de datos personales;

e) hacer un seguimiento de los cambios relevantes, en la medida en que tengan repercusiones sobre la protección de datos personales, en particular de los cambios en las tecnologías de la información y la comunicación;

f) i) colaborar con las autoridades de control nacionales a que se refiere el artículo 28 de la Directiva 95/46/CE de los países a los que se aplica dicha Directiva en la medida necesaria para el ejercicio de sus deberes respectivos, en particular intercambiando toda información útil, instando a dicha autoridad u organismo a ejercer sus poderes o respondiendo a una solicitud de dicha autoridad u organismo;

ii) colaborar asimismo con los organismos de control de la protección de datos establecidos en virtud del Título VI del Tratado de la Unión Europea, en particular con vistas a mejorar la coherencia en la aplicación de las normas y procedimientos de cuyo respeto estén respectivamente encargados;

g) participar en las actividades del Grupo de trabajo sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales creado en virtud del artículo 29 de la Directiva 95/46/CE;

h) determinar, motivar y hacer públicas las excepciones, garantías, autorizaciones y condiciones mencionadas en la letra b) del apartado 2 y en los apartados 4, 5 y 6 del artículo 10, en el apartado 2 del artículo 12, en el artículo 19 y en el apartado 2 del artículo 37;

i) mantener un registro de los tratamientos que se le notifiquen en virtud del apartado 2 del artículo 27 y hayan sido registrados conforme al apartado 5 del artículo 27, así como facilitar los medios de acceso a los registros que lleven los responsables de la protección de datos con arreglo al artículo 26;

j) efectuar una comprobación previa de los tratamientos que se le notifiquen;

k) adoptar su Reglamento interno.

Artículo 47. Competencias

1. El Supervisor Europeo de Protección de Datos podrá:

a) asesorar a las personas interesadas en el ejercicio de sus derechos;

b) acudir al responsable del tratamiento en caso de presunta infracción de las disposiciones que rigen el tratamiento de los datos personales y, en su caso, formular propuestas encaminadas a corregir dicha infracción y mejorar la protección de las personas interesadas;

c) ordenar que se atiendan las solicitudes para ejercer determinados derechos respecto de los datos, cuando se hayan denegado dichas solicitudes incumpliendo los artículos 13 a 19;

d) dirigir una advertencia o amonestación al responsable del tratamiento;

e) ordenar la rectificación, bloqueo, supresión o destrucción de todos los datos que se hayan tratado incumpliendo las disposiciones que rigen el tratamiento de datos personales y la notificación de dichas medidas a aquellos terceros a quienes se hayan comunicado los datos;

f) imponer una prohibición temporal o definitiva del tratamiento;

g) someter un asunto a la institución u organismo comunitario de que se trate y, en su caso, al Parlamento Europeo, al Consejo y a la Comisión;

h) someter un asunto al Tribunal de Justicia de las Comunidades Europeas en las condiciones previstas en el Tratado;

i) intervenir en los asuntos presentados ante el Tribunal de Justicia de las Comunidades Europeas.

2. El Supervisor Europeo de Protección de Datos estará habilitado para:

a) obtener de cualquier responsable del tratamiento o de una institución o un organismo comunitario el acceso a todos los datos personales y a toda la información necesaria para efectuar sus investigaciones;

b) obtener el acceso a todos los locales en los que un responsable del tratamiento o una institución u organismo comunitario realice sus actividades, cuando haya motivo razonable para suponer que en ellos se ejerce una actividad contemplada en el presente Reglamento.

Anexo C. Lista de abreviaturas

ACC	Autoridad Común de Control
ACNUR	Alto Comisionado de las Naciones Unidas para los Refugiados
ACTA	Acuerdo Comercial de Lucha contra la Falsificación
AEMA	Agencia Europea de Medio Ambiente
APD	Autoridades de protección de datos
BCE	Banco Central Europeo
BEI	Banco Europeo de Inversiones
CCI	Centro Común de Investigación
CdR	Comité de las Regiones
CE	Comunidades Europeas
CEDH	Convenio Europeo para la Protección de los Derechos Humanos
CPAS	Comité de preparación de los asuntos sociales
CPD	Coordinador de protección de datos
DAS	Declaración de fiabilidad
DG INFSO	Dirección General de la Sociedad de Información y Medios de Comunicación
DG MARKT	Dirección General de Mercado Interior y Servicios
DIGIT	Dirección General de Informática
EAS	Escuela Europea de Administración
EASA	Agencia Europea de Seguridad Aérea
ECDC	Centro Europeo para la Prevención y el Control de las Enfermedades
EFSA	Autoridad Europea de Seguridad Alimentaria
EIO	Orden Europea de Investigación
ENCS	Expertos nacionales en comisión de servicios
ENISA	Agencia Europea de Seguridad de las Redes y de la Información
EPSO	Oficina Europea de Selección de Personal
ERCEA	Agencia Ejecutiva del Consejo Europeo de Investigación
EWRS	Sistema de Alerta Precoz y Respuesta
FRA	Agencia de los Derechos Fundamentales de la Unión Europea
I+D	Investigación y desarrollo
IMI	Sistema de Información del Mercado Interior
ISS	Estrategia de seguridad interior
JSIMC	Comité de Dirección del Régimen Común del Seguro de Enfermedad
LIBE	Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo.
LISO	Responsable local de seguridad de la información

LSO	Responsable local de seguridad
OAMI	Oficina de Armonización del Mercado Interior
OEP	Orden Europea de Protección
OIM	Organización Internacional para las Migraciones
OLAF	Oficina Europea de Lucha contra el Fraude
OMA	Organización Mundial de Aduanas
ORC	Operaciones de retorno conjuntas
PNR	Registros de nombres de los pasajeros
RFID	Identificación por radiofrecuencia
RPD	Responsable de protección de datos
RR.HH.	Recursos humanos
SAI	Servicio de Auditoría Interna
SIA	Servicio de Información Aduanera
SIS	Sistema de Información de Schengen
SOC	Centro Operativo y de Servicios
s-TESTA	Servicios Transeuropeos Seguros de Telemática entre Administraciones
SWIFT	Sociedad de telecomunicaciones financieras interbancarias mundiales
TdC	Tribunal de Cuentas
TFTP	Programa de seguimiento de la financiación del terrorismo
TFUE	Tratado de Funcionamiento de la Unión Europea
TI	Tecnología de la información
TIC	Tecnologías de la Información y la Comunicación
TJUE	Tribunal de Justicia de la Unión Europea
TURBINE	Identidades biométricas revocables de confianza
UE	Unión Europea
VIS	Sistema de información de visados
WP 29	Grupo de trabajo del artículo 29
WPPJ	Grupo de trabajo sobre policía y justicia

Anexo D. Lista de responsables de la protección de datos

ORGANIZACIÓN	NOMBRE	CORREO ELECTRÓNICO
Parlamento Europeo (PE)	Jonathan STEELE	Data-Protection@europarl.europa.eu
Consejo de la Unión Europea	Pierre VERNHES	Data.Protection@consilium.europa.eu
Comisión Europea	Philippe RENAUDIÈRE	Data-Protection-officer@ec.europa.eu
Tribunal de Justicia de la Unión Europea	Marc SCHAUSS	Dataprotectionofficer@curia.europa.eu
Tribunal de Cuentas Europeo	Johan VAN DAMME	Data-Protection@europarl.europa.eu
Comité Económico y Social Europeo (CESE)	Maria ARSENE	Data.Protection@eesc.europa.eu
Comité de las Regiones (CDR)	Rastislav SPÁC	Data.Protection@cor.europa.eu
Banco Europeo de Inversiones (BEI)	Jean-Philippe MINNAERT	Dataprotectionofficer@eib.org
Defensor del Pueblo Europeo	Loïc JULIEN	DPO-euro-ombudsman@ombudsman.europa.eu
Supervisor Europeo de Protección de Datos (SEPD)	Alfonso SCIROCCO, Sylvie PICARD (RPD adjunto)	alfonso.scirocco@.edps.europa.eu
Banco Central Europeo (BCE)	Frederik MALFRÈRE	DPO@ecb.int
Oficina Europea de Lucha contra el Fraude (OLAF)	Laraine LAUDATI	Laraine.Laudati@ec.europa.eu
Centro de Traducción de los Órganos de la Unión Europea (CDT)	Benoît VITALE	Data-Protection@cdt.europa.eu
Oficina de Armonización del Mercado Interior (OAMI)	Ignacio DE MEDRANO CABALLERO	DataProtectionOfficer@oami.europa.eu
Agencia de los Derechos Fundamentales de la Unión Europea (FRA)	Nikolaos FIKATAS	Nikolaos.Fikatas@fra.europa.eu
Agencia Europea de Medicamentos (EMEA)	Vincenzo Salvatore	Data.Protection@emea.europa.eu
Oficina Comunitaria de Variedades Vegetales (OCVV)	Véronique DOREAU	Doreau@OCVV.europa.eu
Fundación Europea de Formación (ETF)	Liia KAARLOP	Liia.Kaarlop@etf.europa.eu
Agencia Europea de Seguridad de las Redes y de la Información (ENISA)	Emmanuel MAURAGE	Dataprotection@enisa.europa.eu

>>>

ORGANIZACIÓN	NOMBRE	CORREO ELECTRÓNICO
Fundación Europea para la Mejora de las Condiciones de Vida y de Trabajo (Eurofound)	Markus GRIMMEISEN	MGR@eurofound.europa.eu
Observatorio Europeo de las Drogas y las Toxicomanías (OEDT)	Cecile MARTEL	Cecile.Martel@OEDT.europa.eu
Autoridad Europea de Seguridad Alimentaria (EFSA)	Claus RÉUNIS	Dataprotectionofficer@efsa.europa.eu
Agencia Europea de Seguridad Marítima (EMSA)	Malgorzata NESTEROWICZ	Malgorzata.Nesterowicz@emsa.europa.eu
Centro Europeo para el Desarrollo de la Formación Profesional (Cedefop)	Spyros ANTONIOU	Spyros.Antoniou@cedefop.europa.eu
Agencia Ejecutiva en el Ámbito Educativo, Audiovisual y Cultural (EACEA)	Hubert MONET	eacea-data-protection@ec.europa.eu
Agencia Europea para la Seguridad y la Salud en el Trabajo (EU-OSHA)	TAYLOR Terry	Taylor@osha.europa.eu
Agencia Comunitaria de Control de la Pesca (ACCP)	Clara FERNANDEZ/ Rieke ARNDT	cfca-dpo@cfca.europa.eu
Autoridad Europea de Supervisión del GNSS Europeo (GSA)	Triinu VOLMER	Triinu.Volmer@gsa.europa.eu
Agencia Ferroviaria Europea (ERA)	Guido STÄRKLE (RPD en funciones)	Dataprotectionofficer@era.europa.eu
Agencia Ejecutiva de Sanidad y Consumo (EAHC)	Beata HARTWIG	Beata.Hartwig@ec.europa.eu
Centro Europeo para la Prevención y el Control de las Enfermedades (ECDC)	Elisabeth ROBINO	Elisabeth.Robino@ecdc.europa.eu
Agencia Europea de Medio Ambiente (AEMA)	Gordon McINNES	Gordon.McInnes@eea.europa.eu
Fondo Europeo de Inversiones (FEI)	Jobst NEUSS	J.Neuss@eif.org
Agencia Europea para la Gestión de la Cooperación Operativa en las Fronteras Exteriores (Frontex)	Sakari VUORENSOLA	Sakari.Vuorensola@frontex.europa.eu
Agencia Europea de Seguridad Aérea (EASA)	Francesca PAVESI	Francesca.Pavesi@easa.europa.eu
Agencia Ejecutiva de Competitividad e Innovación (AECI)	Elena FIERRO SEDANO	Elena.Fierro-Sedano@ec.europa.eu
Agencia Ejecutiva de la Red Transeuropea de Transporte (TEN-T EA)	Zsófia SZILVÁSSY	Zsofia.Szilvassy@ec.europa.eu
Agencia Europea de Sustancias y Preparados Químicos (ECHA)	Alain LEFÈBVRE	Minna.Heikkila@echa.europa.eu
Agencia Ejecutiva del Consejo Europeo de Investigación (ERCEA)	Donatella PIATTO	Donatella.Piatto@ec.europa.eu

>>>

ORGANIZACIÓN	NOMBRE	CORREO ELECTRÓNICO
Agencia Ejecutiva de Investigación (REA)	Evangelos TSAVALOPOULOS	Evangelos.Tsavalopoulos@ec.europa.eu
Empresa Común *Fusion for Energy* (Empresa Común Europea para el ITER y el Desarrollo de la Energía de Fusión)	Radoslav HANAK	Radoslav.Hanak@f4e.europa.eu
Empresa Común SESAR	Daniella PAVKOVIC	Daniella.Pavkovic@sesarju.eu
Empresa Común Artemis	Anne SALAÜN	Anne.Salaun@artemis-ju.europa.eu
Empresa común *Clean Sky*	Silvia POLIDORI	Silvia.Polidori@cleansky.eu
Empresa común *Innovative Medicines Initiative* (IMI)	Estefania RIBEIRO	Estefania.Ribeiro@imi.europa.eu
Empresa Común Cells & Hydrogen	Nicolas BRAHY	Nicolas.Brahy@fch.europa.eu
Instituto Europeo de Innovación y Tecnología (EIT)	Camilo SOARES	Camilo.Soares@ext.ec.europa.eu

Anexo E. Lista de dictámenes de control previo

Análisis empírico de las correlaciones entre las variables del sistema de trabajo y el proceso de toma de decisiones - OAMI

Dictamen de 22 de noviembre de 2010 sobre el «Análisis empírico de las correlaciones entre las variables del sistema de trabajo y el proceso de toma de decisiones», notificado por la Oficina de Armonización del Mercado Interior (OAMI) el 22 de julio de 2010 (asunto 2010-0468)

Procedimientos relativos a la selección de agentes - BEI

Dictamen de 11 de noviembre de 2010 sobre la notificación de un control previo relativo a los procedimientos utilizados para la selección de agentes (asunto 2009-0254)

Procedimiento de selección y herramienta de solicitud electrónica - EASA

Escrito de 19 de octubre de 2010 sobre la notificación de un control previo relativo al «Procedimiento de selección y herramienta de solicitud electrónica de la EASA» (asunto 2010-0466)

Procedimientos relacionados con las investigaciones de fraudes - BEI

Dictamen de 14 de octubre de 2010 sobre la notificación de un control previo relacionado con las investigaciones de fraude en el Grupo BEI (asunto 2009-0459)

Expertos en comisión de servicios - CdR

Escrito de 5 de octubre de 2010 sobre la notificación de un control previo relacionado con los expertos nacionales en comisión de servicios destinados al Comité de las Regiones (asunto 2010-0515)

Tratamiento de datos personales en el contexto de las deducciones salariales con motivo de una huelga - BCE

Dictamen de 28 de septiembre de 2010 sobre la notificación de un control previo relacionado con el tratamiento de datos personales en el contexto de las deducciones salariales con motivo de una huelga (asunto 2009-0514)

Selección y contratación de personal - EAHC

Escrito de 24 de septiembre sobre la notificación de un control previo relacionado con la selección y contratación de personal (agentes temporales en comisión de servicios procedentes o no de la Comisión Europea, agentes contractuales, agentes temporales y en prácticas) en la Agencia Ejecutiva de Sanidad y Consumo (asunto 2010-0346)

Selección de revisores internos - Comisión (Oficina de Publicaciones)

Dictamen de 6 de septiembre de 2010 sobre la notificación de un control previo del responsable de protección de datos de la Comisión Europea relativo a la «Lista de participantes en los exámenes para revisores internos en régimen contractual» (asunto 2010-400)

Inspecciones de seguridad - Comisión (DG JRC Ispra)

Dictamen de 5 de septiembre de 2010 sobre la notificación de un control previo del responsable de protección de datos de la Comisión Europea relativo a las «Inspecciones de seguridad en el centro JRC de Ispra» (asunto 2009-682)

Sistema Europeo de Vigilancia (TESSy) - ECDC

Dictamen de 3 de septiembre de 2010 sobre la notificación de un control previo relativo al Sistema Europeo de Vigilancia (TESSy) del Centro Europeo para la Prevención y el Control de las Enfermedades (ECDC) (asunto 2009-0474)

Política relativa a la protección de la dignidad de la persona y la prevención del acoso psicológico y sexual - EASA

Dictamen del 29 de julio sobre la notificación de un control previo en relación con la «Política de la EASA relativa a la protección de las personas y la prevención del acoso psicológico y sexual» (asunto 2010-318)

Aplicación del procedimiento informal para el tratamiento de los casos de acoso psicológico y sexual - CESE

Dictamen de 28 de julio de 2010 sobre la notificación de un control previo relativo a la «Aplicación del procedimiento informal para el tratamiento de los casos de acoso psicológico y sexual» (asunto 2010-321)

Selección y contratación de agentes temporales y contractuales, expertos nacionales en comisión de servicios y personal en prácticas - ECHA

Escrito de 27 de julio de 2010 sobre la notificación de un control previo relativo a la selección y contratación de agentes temporales y contractuales, expertos nacionales en comisión de servicios y personal en prácticas (asunto 2010-0109)

Tratamiento de datos personales en el contexto del control de la calidad de los procesos - Consejo

Dictamen de 26 de julio de 2010 sobre la notificación de un control previo relativo al tratamiento de datos personales en el contexto del control de la calidad de los procesos (asunto 2009-0295)

Seguimiento administrativo de las bajas por enfermedad no justificadas - Consejo

Dictamen de 22 de julio de 2010 sobre la notificación de un control previo relativo al expediente «Seguimiento administrativo de las bajas por enfermedad no justificadas» (asunto 2009-0687)

Procedimiento de certificación de funcionarios - OEDT

Escrito de 22 de julio de 2010 sobre la notificación de un control previo relativo a las actividades de tratamiento en relación con el procedimiento de certificación de los funcionarios del OEDT (asunto 2010-0407)

Procedimientos en relación con el «Informe de resultados sobre el liderazgo de 360°» - BEI

Dictamen de 20 de julio de 2010 sobre la notificación de un control previo en relación con los procedimientos del «Informe de resultados sobre el liderazgo de 360°» (asunto 2009-0215)

Procedimiento para la promoción de funcionarios y agentes - CESE

Dictamen de 19 de julio de 2010 sobre la notificación de un control previo relativo al «Procedimiento para la promoción de funcionarios y agentes» (asunto 2008-474)

Selección y contratación de personal no permanente - Banco Europeo de Inversiones - BEI

Escrito de 14 de julio de 2010 sobre la notificación de un control previo relativo a la selección y contratación de personal no permanente (asunto 2009-0678)

Consulta y actualización de la base de datos central - Comité de las Regiones

Dictamen de 4 de junio de 2010 sobre la notificación de un control previo relativo al expediente «Procedimientos aplicables a la consulta y actualización de la base de datos central de exclusión» (asunto 2010-248)

Procedimiento para abordar los casos de incompetencia - Consejo

Dictamen de 4 de julio de 2010 sobre la notificación de un control previo relativo al expediente «Procedimiento para abordar los casos de incompetencia» (expediente 2010-237)

Gestión y evaluación de las traducciones externas realizadas por la DG TRAD - Parlamento

Dictamen de 4 de junio de 2010 sobre la notificación de un control previo relativo a la «Gestión y evaluación de las traducciones externas realizadas por la DG TRAD» (asunto 2009-0827)

Procedimiento de selección de agentes temporales - Comisión

Dictamen de 4 de junio de 2010 sobre la notificación de un control previo relativo al procedimiento de selección de agentes temporales (asunto 2008-704)

Registro de un titular en la base de datos central de exclusión - Comisión

Dictamen de 26 de mayo de 2010 sobre la notificación de un control previo relativo a la operación de tratamiento «Registro de un titular en la base de datos central de exclusión» (asunto 2009-0681)

Procedimiento para el nombramiento de directores generales, directores y jefes de unidad - Parlamento Europeo

Dictamen de 20 de mayo de 2010 sobre la notificación de un control previo relativo al procedimiento para el nombramiento de directores generales, directores y jefes de unidad (asunto 2010-0270)

Contratación de ENCS y personas en prácticas – Centro Europeo para la Prevención y el Control de las Enfermedades (ECDC)

Escrito de 19 de mayo de 2010 sobre la notificación de un control previo relativo a la selección y contratación de ENCS y personas en prácticas (asunto 2009-0453)

Selección de agentes temporales y contractuales - Agencia Europeo de Medio Ambiente (AEMA)

Escrito de 19 de mayo de 2010 sobre la notificación de un control previo relativo a la selección y contratación de agentes temporales y contractuales (asunto 2009-0467)

Asistencia psicosocial y financiera - Centro Común de Investigación (JRC)

Dictamen de 10 de mayo de 2010 sobre la notificación de un control previo relativo a la asistencia psicosocial y financiera en el Centro Común de Investigación (JRC ITU) de Karlsruhe (asunto 2008-713)

Registro de los nombres y otros datos relevantes de los repatriados en las operaciones de retorno conjuntas - FRONTEX

Dictamen de 16 de abril de 2010 sobre la notificación de un control previo relativo al «Registro de los nombres y otros datos relevantes de los repatriados en las operaciones de retorno conjuntas (ORC)» (asunto 2009-0281)

Sistema de Alerta Precoz y Respuesta (EWRS) - Comisión Europea

Dictamen de 26 de abril de 2010 sobre la notificación de un control previo relativo al Sistema de Alerta Precoz y Respuesta (EWRS) (asunto 2009-0137)

Promoción interna de los funcionarios y reclasificación de los agentes temporales - OEDT

Dictamen de 22.04.10 sobre la notificación de un control previo relativo a la «Promoción interna de funcionarios y reclasificación de los agentes temporales» (asunto 2009-0839)

Operaciones de tratamiento en las convocatorias de licitación - ETF

Dictamen de 22 de abril de 2010 sobre la notificación de un control previo relativo a las operaciones de tratamiento en las convocatorias de licitación (asunto 2009-0037)

Actuaciones en los casos de incompetencia profesional - Tribunal de Justicia de la Unión Europea

Dictamen de 21 de abril de 2010 sobre la notificación de un control previo relativo a las «Actuaciones en los casos de incompetencia profesional» (asunto 2009-860)

Investigaciones administrativas y procedimientos disciplinarios - EMA

Dictamen de 21 de abril de 2010 sobre la notificación de un control previo relativo al tratamiento de datos personales en las investigaciones administrativas y procedimientos disciplinarios (asunto 2010-0047)

Procedimientos de contratación y convocatoria de manifestaciones de interés para la selección de expertos - Comisión

Dictamen de 15 de abril de 2010 sobre el modelo de notificación de un control previo relativo a los «Procedimientos de contratación y convocatoria de manifestaciones de interés para la selección de expertos» (asunto 2009-570)

Eficacia del liderazgo - Comisión

Dictamen de 7 de abril de 2010 sobre la notificación de un control previo relativo a la «Eficacia del liderazgo» (asunto 2010-0002)

Procedimientos de selección de personal para las comisiones técnicas - BEI

Dictamen de 26 de marzo de 2010 sobre la notificación de un control previo relativo a los «Procedimientos de selección de personal para las comisiones técnicas» (asunto 2009-679)

Gestión de los permisos del personal - Parlamento

Dictamen de 25 de marzo de 2010 sobre la notificación de un control previo relativo a la gestión de los permisos del personal (asunto 2009-595)

Tramitación manual de los documentos relacionados con la discapacidad de los visitantes - Parlamento Europeo

Dictamen de 16 de marzo de 2010 sobre la notificación de un control previo relativo a la «Tramitación manual de los documentos relacionados con la discapacidad de los visitantes» (asunto 2009-564)

Procedimiento para la movilidad interna - OAMI

Dictamen de 15 de marzo de 2010 sobre la notificación de un control previo recibido del responsable de protección de datos de la Oficina de Armonización del Mercado Interior, relativo al procedimiento para la movilidad interna (asunto 2008-426)

Cuestionario EAS - BELBIN de autopercepción - Comisión Europea

Dictamen de 5 de marzo de 2010 sobre la notificación de un control previo recibida del responsable de protección de datos de la Comisión Europea relativo al «Cuestionario EAS-BALBIN de autopercepción» (asunto 2009-377)

Evaluación del desempeño - OEDT

Dictamen reflejado en un escrito de 8 de marzo de 2010 sobre la notificación de un control previo relativo a la evaluación del desempeño (asunto 2009-838)

Gestión de las ausencias y bajas por enfermedad - CESE

Dictamen de 5 de marzo de 2010 sobre la notificación de un control previo relativo a la gestión de las ausencias y bajas por enfermedad mediante la base de datos «Centurio» (asuntos reagrupados: 2009-0702 y 2009-0703)

Selección de asesores confidenciales - FRA

Dictamen de 10 de febrero de 2010 sobre la notificación de un control previo relativo a los procedimientos para la selección de asesores confidenciales (asunto 2009-857)

Nombramiento de directivos de nivel intermedio - Oficina Comunitaria de Variedades Vegetales (OCVV)

Dictamen de 28 de enero de 2010 sobre la notificación de un control previo relativo al nombramiento de directivos de nivel intermedio (asunto 2009-0666)

Períodos de prueba gestionados por Internet - Banco Europeo de Inversiones

Dictamen de 21 de enero de 2010 sobre la notificación de un control previo relativo al tratamiento de datos personales en el contexto de la gestión de los períodos de prueba (*e-probation*) (asunto 2009-718)

Reclamaciones de los afiliados - Comité de Dirección del Seguro de Enfermedad

Dictamen de 18 de enero de 2010 sobre la notificación de un control previo recibida del Comité de Dirección del Seguro de Enfermedad relativo al expediente «Reclamaciones de los afiliados» (asunto 2009-070)

Acceso a los dispositivos de almacenamiento y correos electrónicos privados - Tribunal de Cuentas

Dictamen de 18 de enero de 2010 sobre la notificación de un control previo relativo al «Procedimiento de acceso a los dispositivos de almacenamiento y correos electrónicos privados del personal» (asunto 2009-620)

Anexo F. Lista de dictámenes sobre propuestas legislativas

Agencia Europea de Seguridad de las Redes y de la Información (ENISA)

Dictamen de 20 de diciembre de 2010 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la Agencia Europea de Seguridad de las Redes y de la Información (ENISA)

La Estrategia de Seguridad Interior de la UE en acción: cinco medidas para una Europa más segura

Dictamen de 17 de diciembre de 2010 sobre la Comunicación de la Comisión «La Estrategia de Seguridad Interior de la UE en acción: cinco medidas para una Europa más segura»

EURODAC

Dictamen de 15 de diciembre de 2010 sobre la creación del sistema Eurodac para la comparación de las impresiones dactilares

Propuesta de Reglamento sobre la comercialización y la utilización de precursores de explosivos

Dictamen de 15 de diciembre de 2010 sobre la propuesta de Reglamento relativo a la comercialización y la utilización de precursores de explosivos

La política antiterrorista de la UE: logros principales y retos futuros

Dictamen de 24 de noviembre de 2010 sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo relativa a la política antiterrorista de la UE: logros principales y retos futuros

Enfoque global sobre las transferencias de los registros de nombres de pasajeros (PNR) a terceros países

Dictamen de 19 de octubre de 2010 sobre el enfoque global relativo a las transferencias de los registros de nombres de pasajeros (PNR) a terceros países

Orden Europea de Protección y Orden Europea de Investigación

Dictamen de 5 de octubre de 2010 sobre la Orden Europea de Protección y la Orden Europea de Investigación en asuntos penales

Gestión de la información en el espacio de libertad, seguridad y justicia

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»

Programas de garantía de depósitos

Dictamen de 9 de septiembre de 2010 sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a los programas de garantía de depósitos (refundición)

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 II)

Dictamen de 22 de junio de 2010 sobre la propuesta de Decisión del Consejo en relación con la conclusión de un 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 Estados Unidos a efectos del Programa de Seguimiento de la Financiación del Terrorismo (TFTP II)

Agencia Europea para la Gestión de la Cooperación Operativa en las Fronteras Exteriores (FRONTEX)

Dictamen de 17 de mayo de 2010 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (CE) nº 2007/2004 por el que 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)

Abusos sexuales a menores y pornografía infantil

Dictamen de 10 de mayo de 2010 sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la lucha contra los abusos y explotación sexual de menores y la pornografía infantil, y por la que se deroga la Decisión marco 2004/68/JHA

Iniciativa ciudadana

Dictamen de 21 de abril de 2020 sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la iniciativa ciudadana

Residuos de aparatos eléctricos y electrónicos (RAEE)

Dictamen de 14 de abril de 2010 sobre la propuesta de Directiva del Parlamento Europeo y del Consejo sobre residuos de aparatos eléctricos y electrónicos (RAEE).

Fortaleciendo la confianza en la sociedad de la información

Dictamen de 18 de marzo de 2010 sobre el fomento de la confianza en la sociedad de la información mediante el fomento de la protección de los datos y la intimidad

Cooperación entre la UE y Japón en materia aduanera

Dictamen de 12 de marzo de 2010 sobre la propuesta de Decisión del Consejo relativa a la posición que la Unión Europea debía adoptar en el seno del Comité Conjunto de Cooperación Aduanera UE-Japón acerca del reconocimiento mutuo de los programas de Operador Económico Autorizado en la Unión Europea y Japón.

Acuerdo Comercial de Lucha contra la Falsificación (ACTA)

Dictamen de 22 de febrero de 2010 sobre las negociaciones en curso de la Unión Europea sobre un Acuerdo Comercial de Lucha contra la Falsificación (ACTA)

Accidentes e incidentes en la aviación civil

Dictamen de 4 de febrero de 2010 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo sobre la investigación y prevención de accidentes e incidentes en la aviación civil

Cooperación en temas fiscales

Dictamen de 6 de febrero de 2010 sobre la propuesta de una Directiva del Consejo relativa a la cooperación administrativa en materia de fiscalidad

Anexo G. Alocuciones del Supervisor y el Supervisor adjunto

El Supervisor y el Supervisor adjunto continuaron dedicando a lo largo del año un tiempo y un esfuerzo importantes a la explicación de su misión y a la mejora de la sensibilización sobre la protección de datos en general, así como a diversos problemas específicos, mediante alocuciones y actuaciones similares ante diversas instituciones y en distintos Estados miembros.

Parlamento Europeo – Comisiones

27 de enero	Supervisor adjunto, Comisión LIBE sobre las políticas antiterroristas (Bruselas)*
4 de marzo	Supervisor, Comisión LIBE sobre los PNR y la intimidad transatlántica (Bruselas)
21 de junio	Supervisor, Comisión LIBE sobre la Carta de los Derechos Fundamentales (Bruselas)*
23 de junio	Supervisor, Comisión LIBE sobre el acuerdo TFTP II (Bruselas)
28 de septiembre	Supervisor adjunto, Comisión LIBE sobre la lucha contra los abusos sexuales (Bruselas)*
9 de noviembre	Supervisor, Comisión PETI sobre el acceso público a los documentos (Bruselas)*
15 de noviembre	Supervisor y Supervisor adjunto, Comisión LIBE sobre el Informe anual 2009 (Bruselas)

Parlamento Europeo – Otros

28 de enero	Supervisor, Día de la protección de datos (Bruselas)
9 de febrero	Supervisor, Jornada por un Internet más seguro (Estrasburgo)*
16 de marzo	Supervisor, preguntas de diputados al Parlamento sobre ACTA (Bruselas)
24 de marzo	Supervisor adjunto, Plataforma para la intimidad: libertad en Internet (Bruselas)
8 de abril	Supervisor, preguntas de diputados al Parlamento sobre los PNR (Bruselas)
1 de diciembre	Supervisor, Plataforma para la intimidad: revisión de la protección de datos (Bruselas)

Consejo

19 de enero	Supervisor adjunto, Conferencia sobre la ECRI (Bruselas)*
25 de enero	Supervisor, Representación de Polonia, Día de la protección de datos (Bruselas)
11 de febrero	Supervisor, Conferencia sobre la Confianza en las TIC (León)*
24 de marzo	Supervisor, Grupo de trabajo sobre protección de datos (Bruselas)

Comisión

28 de enero	Supervisor, Día de la protección de datos, minisimposio (Bruselas)
28 de enero	Supervisor, Día de la protección de datos, alocución durante el almuerzo (Bruselas)
22 de junio	Supervisor, Conferencia sobre Sistemas de transporte inteligente (Bruselas)*
29 de junio	Supervisor y Supervisor adjunto, comparecencia sobre la revisión de la protección de datos (Bruselas)
22 de septiembre	Supervisor, Grupo de trabajo sobre los servicios de las redes sociales (Bruselas)

* Texto disponible en el sitio del SEPD en Internet

5 de octubre	Supervisor, Mesa redonda sobre el futuro de la protección de los datos personales (Bruselas)*
18 de noviembre	Supervisor, Conferencia de la OLAF (París)*
3 de diciembre	Supervisor, Conferencia sobre Sistemas de transporte inteligente (Bruselas)*

Otras instituciones y órganos de la UE

27 de enero	Supervisor adjunto, Día de la protección de datos en la EMEA (Londres-Bruselas)*
7 de mayo	Supervisor, Agencia de los Derechos Fundamentales (Viena)
27-28 de mayo	Supervisor y Supervisor adjunto, Taller sobre organizaciones internacionales (Florencia)
31 de mayo	Supervisor, Protección de datos y orden público (Tréveris)*
7 de junio	Supervisor adjunto, CESE, sobre el acoso en Internet (Bratislava)*
15-16 de junio	Supervisor y Supervisor adjunto, Protección de datos en el procedimiento penal (Madrid)
13 de septiembre	Supervisor, Escuela de verano ENISA-FORTH (Heraklion)
15 de noviembre	Supervisor y Supervisor adjunto, conferencia de prensa sobre el Informe anual 2009 (Bruselas)*

Conferencias internacionales

30 de enero	Supervisor, Equipos informáticos, intimidad y protección de datos (Bruselas)
10 de marzo	Supervisor, Mesa redonda sobre los 30 años de las directrices de privacidad de la OCDE (París)*
20 de abril	Supervisor, Cumbre global sobre intimidad de la IAPP (Washington DC)**
29 de abril	Supervisor y Supervisor adjunto, Autoridades de protección de datos europeas (Praga)*
6 de julio	Supervisor, La legislación sobre intimidad y las empresas (Cambridge)
25 de octubre	Supervisor adjunto, La voz pública de la sociedad civil (Jerusalén)*
26 de octubre	Supervisor, 30 años de las directrices de privacidad de la OCDE (Jerusalén)
27 de octubre	Supervisor, Comisarios de intimidad y protección de datos (Jerusalén)
28 de octubre	Supervisor adjunto, Comisarios de intimidad y protección de datos (Jerusalén)*

Otros actos

22 de enero	Supervisor adjunto, 30 aniversario del CRID (Namur)*
2 de febrero	Supervisor, Congreso de la Policía europea (Berlín)*
26 de febrero	Supervisor, Propiedad intelectual y sociedad de la información (Barcelona)*
5 de marzo	Supervisor, Coloquio sobre PLN (Bruselas)
9 de marzo	Supervisor, Cámara de Comercio Británica en Bélgica (Bruselas)*

* Texto disponible en el sitio del SEPD en Internet
** Vídeo disponible en el sitio del SEPD en Internet

12 de marzo	Supervisor adjunto, Deontología médica y derechos de los pacientes (San Remo)
23 de marzo	Supervisor, Reunión parlamentaria conjunta sobre seguridad (París)*
26 de marzo	Supervisor, Movilidad global y seguridad (Bruselas)*
13 de abril	Supervisor, Día europeo de la sensibilización en materia de ciberseguridad (Bruselas)*
23 de abril	Supervisor, Cámara de Comercio De Estados Unidos en la UE (Bruselas)
28 de abril	Supervisor adjunto, Consejo Judicial (Roma)
11 de mayo	Supervisor adjunto, Conferencia sobre Computación en la nube (Bruselas)*
20 de mayo	Supervisor, Protección intensiva de datos (Londres)
1 de junio	Supervisor, Confianza digital (Bruselas)
2 de junio	Supervisor, Internet de los objetos (Bruselas)
8 de junio	Supervisor adjunto, Mesa redonda sobre seguridad (Bruselas)
15 de junio	Supervisor adjunto, Tratado de Lisboa (Londres)
17 de junio	Supervisor adjunto, Foro Europeo de Responsables de la Intimidad (Bruselas)
22 de junio	Supervisor, Cámara de Comercio de Estados Unidos en la UE (Bruselas)
23 de junio	Supervisor, La UE digital y la IAPP (Bruselas)
29 de junio	Supervisor adjunto, CEPS, Fronteras y justicia penal, (Bruselas)
8 de julio	Supervisor adjunto, Alma Graduate School (Bolonia)
12 de julio	Supervisor adjunto, Consejo Judicial (Roma)
7 de septiembre	Supervisor, La seguridad del futuro (Berlín)
15 de septiembre	Supervisor, Intimidad y seguridad (Bruselas)
16 de septiembre	Supervisor, Consejo de Lisboa sobre el mercado digital (Bruselas)
20 de septiembre	Supervisor, Contraterrorismo y protección de datos (Bruselas)
23 de septiembre	Supervisor, Taller sobre la revisión de la protección de datos (Bruselas)
28 de septiembre	Supervisor, Protección de datos y libertad de información (Budapest)
29 de septiembre	Supervisor, La seguridad de la información y la intimidad (Budapest)
29 de septiembre	Supervisor adjunto, Seguridad de las fronteras de la UE (Bruselas)*
13 de octubre	Supervisor, Intimidad en un mundo digital (Bruselas)
22 de octubre	Supervisor adjunto, La justicia penal en Europa (Luxemburgo)*
5 de noviembre	Supervisor adjunto, Cumplimiento de las normas de intimidad (Roma)
17 de noviembre	Supervisor adjunto, El transporte inteligente (Milán)

23 de noviembre	Supervisor, Intimidad e investigación científica (Bruselas)*
23 de noviembre	Supervisor adjunto, Investigaciones médicas e intimidad (Bruselas)*
24 de noviembre	Supervisor adjunto, Seminario sobre protección de datos – presentación por videoconferencia (Buenos Aires)
29 de noviembre	Supervisor, Amigos de Europa, La protección de datos en la UE (Bruselas)
30 de noviembre	Supervisor, Foro de Europa, La protección de datos en la UE (Bruselas)
30 de noviembre	Supervisor, Foro Europeo de Internet (Bruselas)
2 de diciembre	Supervisor, Hogan & Lovells (Londres)
9 de diciembre	Supervisor, Ética y Gobernanza en materia de biometría (Bruselas)*
10 de diciembre	Supervisor adjunto, Derechos de los pasajeros en la UE (Tréveris)
16 de diciembre	Supervisor, Futura Asamblea de Internet (Gante)*

Anexo H. Composición de la Secretaría del SEPD

El Supervisor y el Supervisor adjunto con la mayor parte de su personal.

Director interino, Jefe de la Secretaría

Christopher DOCKSEY

• Supervisión y Aplicación

Sophie LOUVEAUX *Jefa de Supervisión y Aplicación*	John-Pierre LAMB *Experto nacional en comisión de servicios*
Laurent BESLAY *Coordinador de Seguridad y Tecnología*	Xanthi KAPSOSIDERI *Administrador/jurista*
Jaroslaw LOTARSKI *Coordinador de Reclamaciones*	Luisa PALLA *Asistente de Supervisión y Aplicación*
Maria Verónica PEREZ ASINARI *Coordinadora de Consultas*	Dario ROSSI *Asistente de Supervisión y Aplicación* *Corresponsal contable* *Responsable del almacén de datos externo (EDWM)*
Isabelle CHATELIER *Administradora/jurista*	Tereza STRUNCOVA *Administradora/jurista*
Bart DE SCHUITENEER *Encargado técnico* *Responsable local de seguridad/LISO*	Michaël VANFLETEREN *Administradora/jurista*
Delphine HAROU *Administradora/jurista*	

• Política y Consulta

Hielke HIJMANS *Jefe de Política y Consulta*	Raffaele DI GIOVANNI BEZZI *Asistente de Política y Consulta*
Bénédicte HAVELANGE *Coordinador para los grandes sistemas informáticos y política de fronteras*	Herke KRANENBORG *Administradora/jurista*
Anne-Christine LACOSTE *Coordinadora para la cooperación con los RPD*	Roberto LATTANZI *Experto nacional en comisión de servicios*
Rosa BARCELO *Administradora/jurista*	Alfonso SCIROCCO *Responsable de protección de datos* *Gestión de la calidad*
Zsuzsanna BELENYESSY *Administradora/jurista*	Luis VELASCO *Encargado técnico*
Katarzyna CUADRAT-GRZYBOWSKA *Administradora/jurista*	

• Registro y Apoyo Operativo

Andrea BEACH *Jefa de Registro y Apoyo Operativo*	Kim Thien LÊ *Asistente administrativo*
Christine HUC *Asistente administrativo*	Ewa THOMSON *Asistente administrativo*
Kim DAUPHIN *Asistente administrativo*	

• Información y Comunicación

Nathalie VANDELLE *Jefa de Información y Comunicación*	Agnieszka NYKA *Asistente de Información y Comunicación*
Olivier ROSSIGNOL *Asistente de Información y Comunicación*	

• Recursos Humanos, Presupuesto y Administración

Leonardo CERVERA NAVAS *Jefe de Recursos Humanos, Presupuesto y Administración*	Aida PASCU *Asistente de administración* *LSO adjunto*
Isabelle DELATTRE *Asistente de Finanzas y Contabilidad*	Sylvie PICARD *Responsable adjunto de protección de datos* *COFO - ICO*
Anne LEVÊCQUE *Asistente de Recursos Humanos* *GECO*	Anne-Françoise REYNDERS *Asistente de administración*
Vittorio MASTROJENI *Responsable de recursos humanos*	Marian SANCHEZ LOPEZ *Responsable de Finanzas y Contabilidad*

Supervisor Europeo de Protección de Datos

Informe Anual 2010

Luxemburgo: Oficina de Publicaciones de la Unión Europea

2011 — 124 pp. — 21 x 29,7 cm

ISBN 978-92-95073-23-4
doi:10.2804/219

CÓMO OBTENER LAS PUBLICACIONES DE LA UNIÓN EUROPEA

Publicaciones gratuitas

- A través de EU Bookshop (http://bookshop.europa.eu).
- En las representaciones o delegaciones de la Unión Europea. Para ponerse en contacto con ellas, consulte el sitio http://ec.europa.eu o envíe un fax al número +352 2929-42758.

Publicaciones de pago

- A través de EU Bookshop (http://bookshop.europa.eu).

Suscripciones de pago (por ejemplo, a las series anuales del *Diario Oficial de la Unión Europea* o a las recopilaciones de la jurisprudencia del Tribunal de Justicia de la Unión Europea)

- A través de los distribuidores comerciales de la Oficina de Publicaciones de la Unión Europea (http://publications.europa.eu/others/agents/index_es.htm).

SUPERVISOR EUROPEO
DE PROTECCIÓN DE DATOS

QT-AA-11-001-ES-N

El guardián europeo de la protección de datos personales

www.edps.europa.eu

Oficina de Publicaciones

ISBN 978-92-95073-23-4