ISSN 1830-9429

# Informe Anual

# 2009

Supervisor Europeo
de Protección de Datos

# Informe Anual

## 2009

**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 978-92-95073-09-8
doi:10.2804/13085



*Printed in Luxembourg*

IMPRESO EN PAPEL BLANQUEADO SIN CLORO ELEMENTAL (ECF)

# Índice


Guía para el usuario 7
Declaración de misión 9
Introducción 11

1 HECHOS DESTACADOS DE 2009

1. HECHOS DESTACADOS DE 2009 12

**1.1. Elementos esenciales 12**
**1.2. Panorámica general del año 2009 13**
**1.3. Resultados alcanzados en 2009 17**

2 SUPERVISIÓN

2. SUPERVISIÓN 18

**2.1. Introducción 18**
**2.2. Responsables de la protección de datos 18**
**2.3. Controles previos 19**
2.3.1. Base jurídica 19
2.3.2. Procedimiento 20
2.3.3. Principales temas de los controles previos 24
2.3.4. Consultas sobre la necesidad de control previo 30
2.3.5. Notificaciones no sometidas a control previo y notificaciones retiradas 30
2.3.6. Seguimiento de los dictámenes de control previo 31
2.3.7. Conclusiones y futuro 32
**2.4. Reclamaciones 32**
2.4.1. El mandato del SEPD 32
2.4.2. Procedimiento de tramitación de reclamaciones 34
2.4.3. Garantía de confidencialidad para los reclamantes 35
2.4.4. Reclamaciones atendidas en 2009 36
2.4.5. Trabajo adicional en el ámbito de las reclamaciones 39
**2.5. Control del cumplimiento 40**
2.5.1. El ejercicio «Primavera 2009» 40
2.5.2. Inspecciones 41
**2.6. Medidas administrativas 43**
2.6.1. Transmisión de datos personales a terceros países 43
2.6.2. Tratamiento de datos personales en el marco de un procedimiento de pandemia 44
2.6.3. Ejercicio del derecho de acceso 44
2.6.4. Aplicación de las normas de protección de datos al Servicio de Auditoría Interna (SAI) 44
2.6.5. Modalidades de aplicación del Reglamento (CE) nº 45/2001 44
**2.7. Orientaciones temáticas 45**
2.7.1. Directrices sobre contratación 45
2.7.2. Directrices acerca de los datos relativos a la salud 46
2.7.3. Directrices sobre la videovigilancia 46
**2.8. Eurodac 49**

3 CONSULTA

3. CONSULTA 52

**3.1. Introducción: situación y algunas tendencias 52**
**3.2. Marco normativo y prioridades 53**
3.2.1. Aplicación de las directrices del SEPD en materia consultiva 53
3.2.2. Resultados de 2009 54
**3.3. Espacio de libertad, seguridad y justicia 54**
3.3.1. Evolución general 54
3.3.2. Eurodac y el Reglamento de Dublín 56
3.3.3. Agencia para la Gestión Operativa de Sistemas Informáticos a gran Escala en el Ámbito de la Libertad, la Seguridad y la Justicia 57
3.3.4. Sistema de Información Aduanero (SIA) 58

**3.4. Protección de la intimidad y tecnología** **58**
3.4.1. El SEPD y la Directiva sobre la privacidad en las comunicaciones electrónicas 58
3.4.2. Sistemas de transporte inteligentes 60
3.4.3. Aplicación de la Directiva sobre conservación de datos 61
3.4.4. Identificación por radiofrecuencia (RFID) 61
3.4.5. Participación en el Séptimo Programa Marco de Investigación 62
**3.5. Globalización** **62**
3.5.1. Participación en normas internacionales 62
3.5.2. El registro de nombres de pasajeros y el diálogo transatlántico 63
3.5.3. SWIFT: transferencia de datos financieros a las autoridades de los EE.UU. 63
3.5.4. Medidas restrictivas en relación con presuntos terroristas y ciertos terceros países 64
**3.6. Salud pública** **65**
**3.7. Acceso del público y datos personales** **67**
3.7.1. Introducción 67
3.7.2. Modificación de la legislación de la UE sobre el acceso del público a los documentos 67
3.7.3. El recurso en el asunto Bavarian Lager 67
3.7.4. Otras acciones judiciales sobre el acceso del público y la protección de datos 68
**3.8. Otras cuestiones** **68**
3.8.1. Sistema de Información del Mercado Interior (IMI) 68
3.8.2. Otros dictámenes 68
**3.9. ¿Qué nos depara el futuro?** **69**
3.9.1. Novedades tecnológicas 69
3.9.2. Progresos en materia de política y legislación 70
3.9.3. Prioridades para 2010 70

4 COOPERACIÓN

4. COOPERACIÓN 72

**4.1. Grupo de trabajo del artículo 29** **72**
**4.2. Grupo de trabajo sobre protección de datos del Consejo** **73**
**4.3. Supervisión coordinada de Eurodac** **73**
**4.4. Tercer pilar** **74**
**4.5. Conferencia Europea** **75**
**4.6. Conferencia Internacional** **76**
**4.7. Iniciativa de Londres** **77**
**4.8. Organizaciones internacionales** **77**

5 COMUNICACIÓN

5. COMUNICACIÓN 78

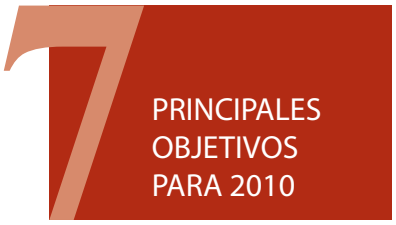
**5.1. Introducción** **78**
**5.2. Características de la comunicación** **79**
**5.3. Relaciones con los medios de comunicación** **79**
**5.4. Solicitudes de información y de asesoramiento** **81**
**5.5. Visitas de estudio** **82**
**5.6. Herramientas de información en línea** **82**
**5.7. Publicaciones** **84**
**5.8. Eventos de sensibilización** **85**

6 ADMINISTRACIÓN, PRESUPUESTO Y PERSONAL

6. ADMINISTRACIÓN, PRESUPUESTO Y PERSONAL 86

**6.1. Introducción** **86**
**6.2. Presupuesto** **86**
**6.3. Recursos humanos** **86**
6.3.1. Contratación 87
6.3.2. Programa de prácticas 87
6.3.3. Programa para expertos nacionales en comisión de servicios 87
6.3.4. Organigrama 87
6.3.5. Formación 88
6.3.6. Actividades sociales 88

**6.4. Funciones de control** **88**
6.4.1. Control interno 88
6.4.2. Auditoría interna 89
6.4.3. Seguridad 89
6.4.4. Responsable de protección de datos 89
**6.5. Infraestructura** **89**
**6.6. Entorno administrativo** **89**
6.6.1. Asistencia administrativa y cooperación interinstitucional 89
6.6.2. Normas internas 90
6.6.3. Gestión de los documentos 90




7. PRINCIPALES OBJETIVOS PARA 2010 92

ANEXO A. MARCO NORMATIVO 94
ANEXO B. EXTRACTO DEL REGLAMENTO (CE) Nº 45/2001 97
ANEXO C. LISTA DE ABREVIATURAS 99
ANEXO D. LISTA DE RESPONSABLES DE LA PROTECCIÓN DE DATOS 101
ANEXO E. LISTA DE DICTÁMENES DE CONTROL PREVIO 104
ANEXO F. LISTA DE DICTÁMENES SOBRE PROPUESTAS LEGISLATIVAS 109
ANEXO G. DISCURSOS DEL SUPERVISOR Y DEL SUPERVISOR ADJUNTO 111
ANEXO H. COMPOSICIÓN DE LA SECRETARÍA DEL SEPD 113

# GUÍA PARA EL USUARIO

Adjunta a la presente guía figura una definición del mandato 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 2009)** presenta los aspectos más sobresalientes del trabajo del SEPD en 2009 y los resultados alcanzados en los diferentes ámbitos en los que se desarrolla su actividad.

**El capítulo 2 (Supervisión)** describe el trabajo efectuado con el fin de garantizar y de comprobar que las instituciones y organismos de la Comunidad cumplen con sus obligaciones en materia de protección de datos. En este capítulo se presenta un análisis de los acontecimientos más destacados de la labor realizada en 2009 en relación con los controles previos, reclamaciones, control del cumplimiento y función de asesoramiento en relación con medidas administrativas. También se presentan las directrices temáticas adoptadas por el SEPD en materia de contratación, datos sanitarios y videovigilancia, así como información actualizada en lo que respecta a la supervisión de Eurodac.

**El capítulo 3 (Consulta)** aborda el ejercicio de la función consultiva por parte del SEPD, centrándose en los dictámenes y los comentarios emitidos respecto de propuestas legislativas y documentos relacionados, así como sus repercusiones en una serie de ámbitos cada vez extendida. El capítulo incluye además un análisis de temas transversales: presenta una serie de nuevas cuestiones de índole tecnológica e incide en las evoluciones más recientes a nivel político y legislativo.

**El capítulo 4 (Cooperación)** describe el trabajo realizado en foros importantes como el Grupo de protección de datos del artículo 29, en las autoridades comunes de control del tercer pilar y en las conferencias europeas e internacionales de protección de datos.

**El capítulo 5 (Comunicación)** expone las actividades y los logros del SEPD en materia de información y comunicación, incluidas la comunicación externa con los medios de comunicación y la información al público.

**El capítulo 6 (Administración, presupuesto y personal)** expone detalladamente las principales novedades organizativas del SEPD, entre ellas los cuestiones presupuestarias y de recursos humanos y los acuerdos administrativos.

**El capítulo 7 (Principales objetivos para 2010)** ofrece una breve perspectiva de las principales líneas de actuación para 2010.

Completan el informe una serie de anexos que brindan una visión general del marco jurídico relevante, las disposiciones del Reglamento (CE) nº 45/2001, una lista de autoridades competentes en materia de protección de datos, listas de los dictámenes de control previo y los dictámenes consultivos, los discursos pronunciados por el Supervisor y el Supervisor Adjunto y la composición de la secretaría del SEPD.

Existe también un resumen del presente informe que ofrece una versión sintetizada de las novedades más importantes en lo que a las actividades del SEPD se refiere, durante el año 2009.

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

Pueden encargarse al servicio de publicaciones de la UE (http://www.bookshop.europa.eu) o al SEPD ejemplares impresos del Informe Anual y del Resumen; son gratuitos. Los datos de contacto están disponibles en nuestro sitio en Internet, pulsando el enlace «Contacto».

# DECLARACIÓN DE MISIÓN

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

Las competencias del SEPD incluyen:

- hacer un seguimiento y velar por el cumplimiento de las disposiciones del Reglamento (CE) nº 45/2001 ([2]) y otros actos comunitarios relativos a la protección de los derechos y las libertades fundamentales en el momento de proceder al 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 seguimiento de las evoluciones en materia de protección de datos personales (consulta);

- cooperar con las autoridades nacionales responsables de la supervisión de datos personales y con los organismos responsables de la supervisión contemplados en el tercer pilar de la Unión Europea, con el fin de mejorar la coherencia en materia de protección de datos personales (cooperación).

En consonancia con lo anterior, el propósito del SEPD es trabajar estratégicamente con el fin de:

- propiciar una cultura de la protección de datos en las instituciones y organismos, contribuyendo adicionalmente a fomentar el principio de recta administración;

- integrar el respeto de los principios de protección de datos en las políticas y en la legislación de la UE siempre que se revele pertinente;

- mejorar la calidad de las políticas de la UE en todos aquellos casos en los que una protección de datos eficaz constituya un requisito esencial para llevarlas a buen puerto.

([2]) 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, 12.1.2001, p. 1.


Peter Hustinx, Supervisor Europeo de Protección de Datos, y Giovanni Buttarelli, Supervisor Adjunto.

# INTRODUCCIÓN

Nos complace presentar a continuación el Informe Anual que recoge las actividades del Supervisor Europeo de Protección de Datos (SEPD) y que será presentado al Parlamento Europeo, al Consejo y a la Comisión Europea, de conformidad con el Reglamento (CE) nº 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 presente informe cubre el ejercicio correspondiente a 2009, quinto año completo de actividad del SEPD en tanto que nueva autoridad de supervisión independiente encargada de velar por el respeto de los derechos y libertades fundamentales de las personas físicas, y en especial de su derecho a la intimidad, respecto del tratamiento de los datos personales por parte de las instituciones y organismos comunitarios. Al mismo tiempo, el presente informe cubre el primero de nuestros cinco años de mandato común en tanto que miembros actuales de esta autoridad (en número de dos).

Ha sido un año sumamente importante para el derecho fundamental a la protección de datos, debido a una serie de acontecimientos sumamente relevantes: la entrada en vigor del Tratado de Lisboa, que garantiza una base jurídica sólida para la instauración de un marco integral de protección de datos en todos los ámbitos de actividad política de la Unión; el inicio de un proceso de consulta pública sobre el futuro marco jurídico de protección de datos en la UE, y la adopción de un nuevo programa político a cinco años para el espacio de libertad, seguridad y justicia («Programa de Estocolmo»), que hace especial hincapié en la protección de datos como elemento crucial que garantiza la legitimidad y la eficacia en este ámbito.

El SEPD ha adquirido un compromiso firme en estos ámbitos y está decidido a ahondar en esta dirección en un futuro próximo. Al mismo tiempo, hemos velado por que en todos los ámbitos de actividad habituales se ejerza la función de autoridad de control independiente, lo que ha permitido avances importantes, tanto en lo que se refiere al control del tratamiento de los datos personales por parte de las instituciones y los organismos comunitarios, como en la consulta sobre nuevas políticas y medidas legislativas, así como en la estrecha cooperación con otras autoridades de control a la hora de garantizar una protección de datos más coherente.

Quisiéramos, por tanto, aprovechar esta oportunidad para expresar nuestro agradecimiento a quienes, en el Parlamento Europeo, el Consejo y la Comisión, apoyan nuestra labor, así como a los muchos miembros de diversas instituciones y organismos que son responsables del procedimiento por el que se ejerce, en la práctica, la protección de datos. Quisiéramos, igualmente, alentar a todos aquellos que afrontan los importantes desafíos que tenemos por delante.

Por último, deseamos expresar también un especial agradecimiento al personal de nuestro departamento. 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 2009

## 1.1. Elementos esenciales

Algunos cambios sobrevenidos en 2009 han sido un acicate para que actualmente el derecho fundamental a la protección de los datos personales sea objeto de mayor atención y para que se actualicen los medios empleados con el fin de velar por una protección más eficaz de los datos personales en la práctica. No es posible sino congratularse de que así sea, en vista de los retos que plantean las nuevas tecnologías, la globalización y los intereses públicos en conflicto.

La entrada en vigor del Tratado de Lisboa, en diciembre de 2009, ha garantizado un fundamento jurídico sólido para la institucionalización de un marco integral de protección de datos en todos los ámbitos de actividad política de la Unión Europea (UE). La Carta de los Derechos Fundamentales de la UE ha adquirido el mismo valor jurídico que los Tratados. Esto es igualmente válido para su artículo 8, relativo a la protección de los datos personales. El artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE) prevé ahora, entre otras disposiciones generales del mismo, el derecho que toda persona puede invocar directamente a la protección de sus datos personales.

El artículo 16 del TFUE ofrece asimismo un fundamento jurídico general para las disposiciones relativas a la protección de los individuos respecto del tratamiento de los datos de carácter personal por parte de las instituciones y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actuaciones comprendidas en el ámbito de aplicación del Derecho de la UE. El cumplimiento de estas disposiciones estará sometido al control de autoridades independientes, como se contempla igualmente en el artículo 8 de la Carta. Esto permitirá, e incluso exigirá, una revisión completa del marco jurídico en vigor en materia de protección de datos, a fin de garantizar que todas las personas incluidas en el ámbito de aplicación de la jurisprudencia de la UE gocen plenamente del derecho fundamental a la protección de datos.

El segundo desarrollo decisivo ha sido la decisión de la Comisión Europea de iniciar una consulta pública sobre el futuro del marco jurídico vigente en la UE en materia de protección de datos, antes incluso de la entrada en vigor del Tratado de Lisboa en tanto que realidad jurídica y política.

Instancias de dicho desarrollo han sido la celebración de una conferencia pública en mayo de 2009 y la realización de una consulta pública entre julio y diciembre del mismo año. Tanto el Supervisor como el Supervisor Adjunto contribuyeron personalmente a la conferencia. También han colaborado muy activamente con sus colegas del Grupo de trabajo del artículo 29 y del Grupo de trabajo sobre policía y justicia para aportar una contribución conjunta a la consulta pública, lo que permitirá a la Comisión elaborar un marco jurídico global que incluya todos los ámbitos de actividad política de la UE y asegurar su eficacia en la práctica, pese a las dificultades que ello conlleva.

La contribución conjunta de ambos grupos de trabajo, adoptada con el apoyo pleno y activo del

Supervisor Europeo de Protección de Datos (SEPD) en diciembre de 2009, ha sido una de las principales aportaciones al proceso de consulta pública. En el futuro inmediato, el SEPD seguirá efectuando un seguimiento en profundidad de este asunto, asesorando si así se revela necesario.

El tercer desarrollo esencial fue la adopción, poco después de la entrada en vigor del Tratado de Lisboa, también en diciembre de 2009, de un nuevo programa político a cinco años para el espacio de libertad, seguridad y justicia («Programa de Estocolmo»), en el que se presta una atención especial a la protección de datos como elemento crucial para la legitimidad y la eficacia en este ámbito. El programa examina la incidencia del Tratado de Lisboa y establece las líneas maestras de la política de la UE durante los próximos cinco años. En cualquier caso, los cambios institucionales introducidos por el Tratado de Lisboa facilitarán su aplicación.

El intercambio de datos de carácter personal entre las autoridades competentes en materia de inmigración, cuerpos y fuerzas de seguridad y seguridad pública de los diferentes Estados miembros es parte integrante de esta política. Garantizar la integración de la protección de datos en estas políticas y sistemas desde el principio constituye un compromiso importante que el SEPD ha apoyado y alentado activamente y que seguirá supervisando cuando y donde se aplique en la práctica.

Estas medidas adquieren aún más entidad cuando coinciden con la entrada en funciones, en febrero de 2010, de una nueva Comisión que también presta una atención especial a la protección de los derechos fundamentales en general y a la protección de los datos de carácter personal en tanto que materia específica y prioritaria. Por lo que respecta a las dificultades mencionadas inicialmente, sólo cabe señalar que en gran medida son resultado de una sociedad cada vez más dependiente del uso a gran escala de las tecnologías de la información en diversos ámbitos de la existencia.

Dado que esta situación está llamada a continuar e incluso a acentuarse en el contexto de la Agenda Digital de la Comisión, conviene destacar la necesidad de una protección más eficaz e integral de los datos personales en el futuro inmediato. El SEPD se complace de las propuestas que formule la Comisión en todos los ámbitos pertinentes; las tendrá en cuenta y las evaluará con suma atención llegado el momento.

## 1.2. Panorámica general del año 2009

Las principales actividades del SEPD durante el año 2009 se fundaron en la misma estrategia general seguida anteriormente, si bien desarrolladas a mayor escala y con un alcance mayor. También ha mejorado la capacidad del SEPD para actuar de manera efectiva y eficaz.

El marco jurídico ([2]) en el que opera el SEPD contempla una serie de funciones y competencias que permiten efectuar una primera distinción entre tres cometidos principales. Esos cometidos siguen constituyendo plataformas estratégicas para las actividades del SEPD y quedan reflejados en su declaración de misión:

- un cometido de «supervisión», que consiste en controlar y en velar por que las instituciones y organismos ([3]) comunitarios respeten las garantías legales vigentes cada vez que efectúan el tratamiento de datos personales;

- un cometido de «consulta», que consiste en asesorar a las instituciones y organismos comunitarios en todas las cuestiones pertinentes, y en particular respecto de las propuestas legislativas que tengan repercusiones en la protección de datos personales;

- un cometido de «cooperación», que consiste en cooperar con las autoridades nacionales de supervisión y con las autoridades de control en el marco del 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 serán desarrolladas en los capítulos 2, 3 y 4 del presente Informe Anual, en el que se exponen las principales actividades del SEPD y los avances alcanzados en 2009. En esta sección se sintetizarán algunos elementos esenciales.

([2]) Véase la panorámica del marco jurídico en el anexo A y el extracto del Reglamento (CE) nº 45/2001 en el anexo B.

([3]) A lo largo de todo el informe se emplean los términos «instituciones» y «organismos», del Reglamento (CE) nº 45/2001, entre los que se incluyen las agencias comunitarias. Para consultar la lista completa, utilicen el siguiente enlace: http://europa.eu/about-eu/institutions-bodies/index_es.htm

La importancia de la información y la comunicación respecto de estas actividades justifica plenamente un capítulo 5 dedicado por entero a la comunicación. Todas estas actividades se basan en una gestión eficaz de los recursos financieros, humanos o de otro tipo, como se expondrá en el capítulo 6.

## 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.. El asesoramiento adicional prestado a la administración de la UE puede revestir la forma de consultas respecto a medidas administrativas o puede consistir en la publicación de directrices temáticas.

Todas las instituciones y organismos de la UE deben contar al menos con un funcionario responsable de la protección de datos. En 2009, el número total de responsables de protección de datos se elevaba a cuarenta y cinco. La interacción periódica con dichos funcionarios y con la red que conforman es una condición previa importante para que la supervisión resulte eficaz.

A lo largo de 2009, el principal elemento en materia de supervisión siguió siendo el control previo de las operaciones de tratamiento de riesgo. El SEPD adoptó 110 dictámenes de control previo sobre datos sanitarios, evaluación del personal, contratación, gestión del tiempo, registro telefónico, herramientas relacionadas con los resultados e investigaciones de seguridad. Estos dictámenes se han publicado en el sitio del SEPD en Internet y su aplicación es objeto de un seguimiento sistemático.

La aplicación del Reglamento por parte de las instituciones y organismos también es objeto de un seguimiento sistemático mediante la realización de un inventario periódico de los indicadores de resultados de todas las instituciones y organismos de la UE. Tras el ejercicio «Primavera 2009», el SEPD publicó un informe en el que se hacía eco del progreso satisfactorio de las instituciones de la UE en el cumplimiento de sus obligaciones en materia de protección de datos, así como del menor nivel de cumplimiento observado en la mayoría de las agencias.

El SEPD también llevó a cabo cuatro inspecciones sobre el terreno en diversas instituciones y organismos. Las inspecciones son objeto de un seguimiento sistemático y se efectuarán con mayor frecuencia en el futuro próximo. En julio de 2009, el SEPD adoptó un manual de procedimiento de inspección y publicó en su página web los elementos esenciales de dicho procedimiento.

En 2009, el número total de reclamaciones recibidas se elevaba a ciento 11, si bien sólo se admitieron a trámite 42. Muchas de las reclamaciones no admitidas a trámite se referían a problemática nacional en la que el SEPD no tiene competencia. La mayoría de las reclamaciones admitidas a trámite se referían a supuestas violaciones de la confidencialidad, exceso de celo en la recogida de datos o utilización ilegal de los mismos por parte del funcionario encargado de su tratamiento. En ocho casos, el SEPD concluyó que se habían infringido las normas que regulan la protección de datos.

También prosiguieron las actividades de consulta sobre las medidas administrativas contempladas por las instituciones y organismos de la UE en relación con el tratamiento de datos personales. Se plantearon diversas cuestiones, como la transferencia de datos a terceros países u organizaciones internacionales, el tratamiento de datos en caso de procedimiento de pandemia, la protección de datos en el Servicio de Auditoría Interna y las modalidades de aplicación del Reglamento (CE) nº 45/2001.

El SEPD adoptó las directrices relativas al tratamiento de los datos personales en procedimientos de contratación y de los datos sanitarios en el lugar de trabajo. En 2009, el SEPD celebró asimismo una consulta pública sobre las directrices en materia de videovigilancia en la que insistió, entre otras cosas, en el principio de «intimidad en la concepción» y en la obligación de rendir cuentas como requisitos esenciales en este contexto.

**Algunas cifras clave del SEPD durante 2009**

→ **Adoptó 110 dictámenes de control previo** en relación con datos sanitarios, evaluación del personal, procesos de contratación, gestión del tiempo de trabajo, investigaciones de seguridad, registro telefónico y herramientas relacionadas con el rendimiento.

➔ **Acusó recibo de 111 reclamaciones, cuarenta y dos de ellas admitidas a trámite.** La mayoría referidas a supuestas violaciones 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 12 asuntos** en los que el SEPD no vio indicio de violación de la normativa que regula la protección de datos.
- **Declaró ocho casos de incumplimiento** de las normas que regulan la protección de datos.

➔ **Acusó recibo de 32 consultas sobre medidas administrativas.** Asesoró en un amplio abanico de cuestiones jurídicas relacionadas con el tratamiento de los datos personales por parte de las instituciones y organismos de la UE.

➔ **Practicó cuatro inspecciones sobre el terreno** en diversas instituciones y organismos de la UE.

➔ **Publicó tres orientaciones** sobre contratación, datos sanitarios y videovigilancia.

➔ **Emitió 16 dictámenes legislativos** en relación con los sistemas de información a gran escala, las listas de terroristas, el futuro marco de protección de datos, la salud pública, la fiscalidad y los transportes.

➔ **Emitió cuatro comentarios formales** sobre acceso público a los documentos, el servicio universal y la intimidad en las comunicaciones electrónicas, y las negociaciones entre la UE y los EE.UU. acerca del nuevo acuerdo SWIFT.

➔ **Organizó tres reuniones del Grupo de coordinación de la supervisión de Eurodac**, que dieron origen a un segundo informe coordenado de inspección sobre la información a los titulares de los datos y la evaluación de la edad de los solicitantes de asilo jóvenes.

## Consulta

Una serie de eventos significativos contribuyeron a acercar la perspectiva de un nuevo marco jurídico en materia de protección de datos. La materialización de esta posibilidad será uno de los temas prioritarios de la agenda del SEPD durante los próximos años.

A finales de 2008 se adoptó un marco jurídico general para la protección de datos en el ámbito de la cooperación policial y judicial en la UE. Pese a no resultar plenamente satisfactorio, supuso un paso importante en la dirección adecuada.

Un segundo cambio importante en este sentido, durante 2009, fue la adopción de la Directiva sobre la intimidad en las comunicaciones electrónicas revisada, e inscrita dentro de un paquete más amplio. Fue, a su vez, una primera etapa hacia la actualización del marco jurídico aplicado a la protección de datos.

La entrada en vigor del Tratado de Lisboa, el 1 de diciembre de 2009, no solo confirió a la Carta de los Derechos Fundamentales un carácter vinculante para las instituciones y organismos de la UE, así como para los Estados miembros cuando actúan dentro del ámbito del Derecho de la Unión, sino que también sirvió para instituir el fundamento general de un marco jurídico integral en el sentido del artículo 16 del TFUE.

En 2009, la Comisión también inició una consulta pública sobre el futuro marco jurídico para la protección de datos. El SEPD ha colaborado estrechamente con sus homólogos a fin de impulsar conjunta y adecuadamente esta consulta y ha aprovechado en diversas oportunidades para resaltar la necesidad de una protección de datos más completa y eficaz en la Unión Europea.

El SEPD ha continuado aplicando su política de consulta general y ha formulado un número sin precedentes de dictámenes legislativos sobre diferentes materias. Esta política prevé igualmente un enfoque proactivo que incluye un inventario periódico de las propuestas legislativas que vayan a someterse a consulta y la disponibilidad de comentarios informales en las fases preparatorias de las propuestas legislativas. La mayor parte de los dictámenes del SEPD fueron debatidos con el Parlamento y el Consejo.

En 2009 el SEPD siguió con especial interés la evolución de aquellas materias relacionadas con el

Programa de Estocolmo y su visión de los cinco próximos años en el ámbito de la justicia y los asuntos de interior. El SEPD asesoró en la evaluación del programa y participó en los trabajos preparatorios del Modelo Europeo de Información.

Otros trabajos realizados en este ámbito guardaban relación con la revisión de los Reglamentos Eurodac y Dublín, con la creación de una Agencia para la Gestión Operativa de Sistemas Informáticos a gran Escala en el Ámbito de la Libertad, la Seguridad y la Justicia y con un enfoque coherente de la supervisión en este ámbito.

En el contexto de la protección de la intimidad en las comunicaciones electrónicas y la tecnología, aparte de la revisión general mencionada anteriormente, el SEPD intervino en cuestiones referidas a la Directiva sobre la conservación de datos, el uso de etiquetas RFID o sistemas de transporte inteligentes y el informe de Riseptis «Trust in the Information Society» (La confianza en la sociedad de la información).

En el contexto de la globalización, el SEPD participó en la elaboración de estándares internacionales, el diálogo transatlántico sobre protección de datos y datos policiales, así como en cuestiones referidas a medidas restrictivas en relación con presuntos terroristas y determinados terceros países.

Otros ámbitos de considerable interés para el SEPD fueron los de la salud pública (incluidas la asistencia sanitaria transfronteriza, la sanidad electrónica y la farmacovigilancia) y el acceso del público a los documentos [revisión del Reglamento (CE) nº 1049/2001 relativo al acceso del público a los documentos y diversos asuntos judiciales relativos a la relación entre el acceso del público y la protección de los datos].

## Cooperación

La principal plataforma de cooperación entre las autoridades europeas responsables de la protección de datos es el Grupo de trabajo del artículo 29. El SEPD participa en las actividades del Grupo de trabajo, que desempeña un papel importante en la aplicación uniforme de la Directiva sobre protección de datos.

El SEPD y el Grupo de trabajo del artículo 29 han aunado sinergias para cooperar sobre una serie de cuestiones, pero sobre todo en relación con la aplicación de la Directiva sobre protección de datos y los retos asociados a las nuevas tecnologías. El SEPD ha prestado un decidido apoyo a las iniciativas adoptadas con el fin de facilitar los flujos de datos internacionales.

La contribución conjunta sobre el futuro del derecho a la intimidad en respuesta a la consulta de la Comisión Europea respecto del marco jurídico de la UE para la protección de datos, así como la consulta de la Comisión sobre el impacto del escáneres corporales en el ámbito de la seguridad aérea merecen especial mención.

Una de las tareas más importantes del SEPD en el marco de la cooperación tiene que ver con Eurodac, cuya supervisión es una responsabilidad compartida con las autoridades nacionales responsables de la protección de datos. El Grupo de coordinación de la supervisión de Eurodac, integrado por representantes de las autoridades nacionales de protección de datos y el SEPD, se reunió en tres ocasiones y sus trabajos se centraron en la ejecución del programa de trabajo adoptado en diciembre de 2007.

Uno de los principales resultados fue la adopción, en junio de 2009, de un segundo informe de inspección consagrado en dos cuestiones: el derecho a la información de los solicitantes de asilo y los métodos para evaluar la edad de los jóvenes solicitantes de asilo.

El SEPD siguió manteniendo una estrecha cooperación con las autoridades responsables de la protección de datos en el antiguo «tercer pilar» (cooperación policial y judicial) y con el Grupo de trabajo sobre policía y justicia. En 2009 esta cooperación incluyó contribuciones al debate sobre el Programa de Estocolmo y la evaluación de impacto de la Decisión marco del Consejo relativa a la protección de datos.

La cooperación en otros foros internacionales siguió concitando interés, especialmente la 31ª Conferencia Internacional de Comisarios de Protección de Datos y Privacidad celebrada Madrid, que culminó en la creación de un conjunto de normas internacionales en materia de protección de datos.

Por otra parte, el SEPD organizó el seminario «Responder a las infracciones de seguridad» en el contexto de la Iniciativa de Londres iniciada en la 28ª Conferencia Internacional de noviembre de 2006 con el fin de concienciar en materia de protección de datos y obtener una protección más eficiente.

## 1.3. Resultados alcanzados en 2009

El Informe Anual correspondiente a 2008 señalaba que para 2009 se habían seleccionado los siguientes objetivos principales, la mayor parte de los cuales se ha cumplido total o parcialmente.

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

El SEPD siguió ofreciendo un firme respaldo a los funcionarios responsables de la protección de datos, en particular en las agencias de reciente creación, y alentó el intercambio de conocimientos y de buenas prácticas con el fin de reforzar su eficacia.

- Función de control previo

El SEPD casi ha concluido el control previo de las operaciones de tratamiento de la mayor parte de las instituciones y organismos y ha hecho especial hincapié en la aplicación de las recomendaciones. Se prestó una especial atención al control previo de las operaciones de tratamiento comunes a la mayoría de las agencias.

- Orientación horizontal

El SEPD publicó orientaciones sobre los datos relativos a procesos de contratación de personal y salud laboral, así como proyectos de orientación sobre la videovigilancia que fueron objeto de una consulta. Estas orientaciones contribuirán a garantizar el cumplimiento de la normativa en las instituciones y organismos y a que los procedimientos de control previo sean más eficientes.

- Tramitación de reclamaciones

El SEPD adoptó un manual sobre tramitación de reclamaciones a la intención de su personal y publicó en su sitio en Internet las líneas maestras de dicho manual a fin de informar a todas las partes implicadas sobre los procedimientos pertinentes, con inclusión de los criterios para determinar la conveniencia o no de iniciar una investigación respecto de las reclamaciones que se le hubieran presentado. Por otra parte, en la actualidad se puede descargar de Internet un formulario de reclamación.

- Política de inspección

El SEPD siguió cuantificando el grado de cumplimiento del Reglamento (CE) nº 45/2001, mediante la aplicación de diferentes tipos de controles, por parte de todas las instituciones y organismos y efectuó diversas inspecciones sobre el terreno. Se publicó una primera serie de procedimientos de inspección con el fin de garantizar un proceso menos sujeto a imprevistos.

- Alcance de la consulta

El SEPD emitió el mayor número de dictámenes y observaciones formales sobre propuestas de nueva legislación hasta la fecha (16 y cuatro, respectivamente), basándose en un inventario sistemático de los temas y prioridades pertinentes y velando por el adecuado seguimiento de los mismos. Todos los dictámenes y comentarios, así como el inventario, se encuentran disponibles en Internet.

- Programa de Estocolmo

El SEPD prestó especial atención a la elaboración de un nuevo programa político a cinco años para el espacio de libertad, seguridad y justicia, adoptado por el Consejo a finales de 2009. Se destacó como condición fundamental la necesidad de salvaguardias efectivas en materia de protección de datos.

- Actividades de información

El SEPD mejoró la calidad y la eficacia de las herramientas de información en línea (sitio en Internet y boletín electrónico) y actualizó en los casos necesarios otras actividades de información (nuevo folleto informativo y actividades de sensibilización).

- Reglamento interno

El Reglamento interno relativo a las diferentes actividades del SEPD será adoptado próximamente. El Reglamento interno confirmará o aclarará las prácticas actuales del SEPD y estará disponible en el sitio en Internet.

- Gestión de recursos

El SEPD consolidó y siguió desarrollando actividades en materia de recursos financieros y humanos y prestó una atención especial a la contratación de personal encargado de protección de datos por medio de un concurso organizado por la EPSO. Se espera contar con los primeros candidatos aprobados en 2010.

# 2

# SUPERVISIÓN

## 2.1. Introducción

La tarea del SEPD, en su calidad de supervisor independiente, consiste en practicar el seguimiento de los datos personales tratados por todas las instituciones y organismos comunitarios (con excepción del Tribunal de Justicia cuando actúa en el ejercicio de sus funciones jurisdiccionales), en la medida en que dicho tratamiento se lleve a cabo para el ejercicio de actividades englobadas total o parcialmente en el ámbito de aplicación del Derecho comunitario ([4]). El Reglamento (CE) nº 45/2001 (en lo sucesivo, «el Reglamento») describe y concede una serie de derechos y facultades que habilitan al SEPD para efectuar este cometido.

Con la introducción del artículo 16 del TFUE, que sustituye al artículo 286 del Tratado CE, el Tratado de Lisboa marca un giro dentro del marco jurídico que regula la protección de datos por parte de la Administración europea. Las implicaciones concretas tanto de este cambio como de la abolición de la estructura de pilares para la supervisión de actividades por parte del SEPD están siendo actualmente examinadas y podrían requerir ulteriores aclaraciones.

Durante 2009, el control previo de las operaciones de tratamiento siguió constituyendo un aspecto importante de la supervisión (véase la sección 2.3), pero el SEPD ha incorporado también otras formas de supervisión, como la tramitación de reclamaciones, la realización de inspecciones, el asesoramiento respecto de medidas administrativas y la elaboración de orientaciones temáticas. La supervisión de Eurodac es una actividad específica del SEPD.

En 2009, como en años anteriores, el SEPD no ha tenido ninguna necesidad de recurrir a sus facultades de formular advertencias o prohibiciones, pues los responsables de la protección de datos han aplicado sus recomendaciones, han manifestado su intención de aplicarlas o han tomado las medidas necesarias. No obstante, la agilidad de la respuesta varía de unos asuntos a otros.

## 2.2. Responsables de la protección de datos

Una característica importante dentro del panorama de las instituciones de la Unión Europea (UE) es la obligación de nombrar a una autoridad 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 designó 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 coordinar todos los aspectos de la protección de datos en el seno de una dirección o unidad determinada.

([4]) Artículo 3, apartado 2, del Reglamento (CE) nº 45/2001.

En 2009 fueron designados siete nuevos RPD en nuevas agencias o empresas conjuntas, lo que eleva el número total de RPD a 45.

Desde hace varios años, los RPD se reúnen a intervalos regulares para intercambiar experiencias y abordar cuestiones transversales. La colaboración informal en el seno de esta red informal ha venido revelándose muy productiva, y así ha seguido siéndolo a lo largo de 2009.

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

El SEPD asistió a las reuniones del RPD celebradas en marzo de 2009 en el Banco Central Europeo y en octubre de 2009 en la Comisión Europea (copatrocinadas por la OLAF). El SEPD aprovechó estas oportunidades para poner al día a los RPD sobre la labor realizada, presentar un panorama general de las últimas novedades en materia de protección de datos dentro de la UE y debatir cuestiones de interés común.

Más en concreto, el SEPD utilizó este foro para explicar y debatir el procedimiento de los controles previos, informar sobre los avances en el ámbito de las notificaciones de control previo, poner al corriente a los RPD respecto al ejercicio «Primavera 2009» y sus consecuencias (véase la sección 2.5), presentar una actualización de las inspecciones del SEPD y exponer su política y su procedimiento de inspección. Asimismo, el SEPD aprovechó la ocasión para reanudar el trabajo sobre la creación de normas profesionales para los RPD y poner en común las iniciativas adoptadas para el Día Europeo de la Protección de Datos (28 de enero).

Las autoridades responsables de la protección de datos durante su 26ª reunión en Bruselas (octubre de 2009).

## 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. Por ejemplo, el SEPD considera que la presencia de determinados datos biométricos ajenos a la simple fotografía entraña riesgos específicos para los derechos y libertades de los interesados y justifica el control previo de las actividades de tratamiento por parte del SEPD. Estas consideraciones se basan principalmente en la naturaleza de los datos biométricos, ya de por sí intrínsecamente delicados.

En el artículo 27, apartado 2, del Reglamento se enumeran una serie de operaciones de tratamiento que pueden entrañar dichos riesgos. Los criterios determinados en los años anteriores ([5]) siguieron aplicándose en la interpretación de esta disposición, tanto al decidir que una notificación de un RPD no estaba sometida a control previo como al asesorar en una consulta sobre la necesidad de control previo (véase también la sección 2.3.4).

([5]) Véase el Informe Anual 2005, sección 2.3.1.

## 2.3.2. Procedimiento

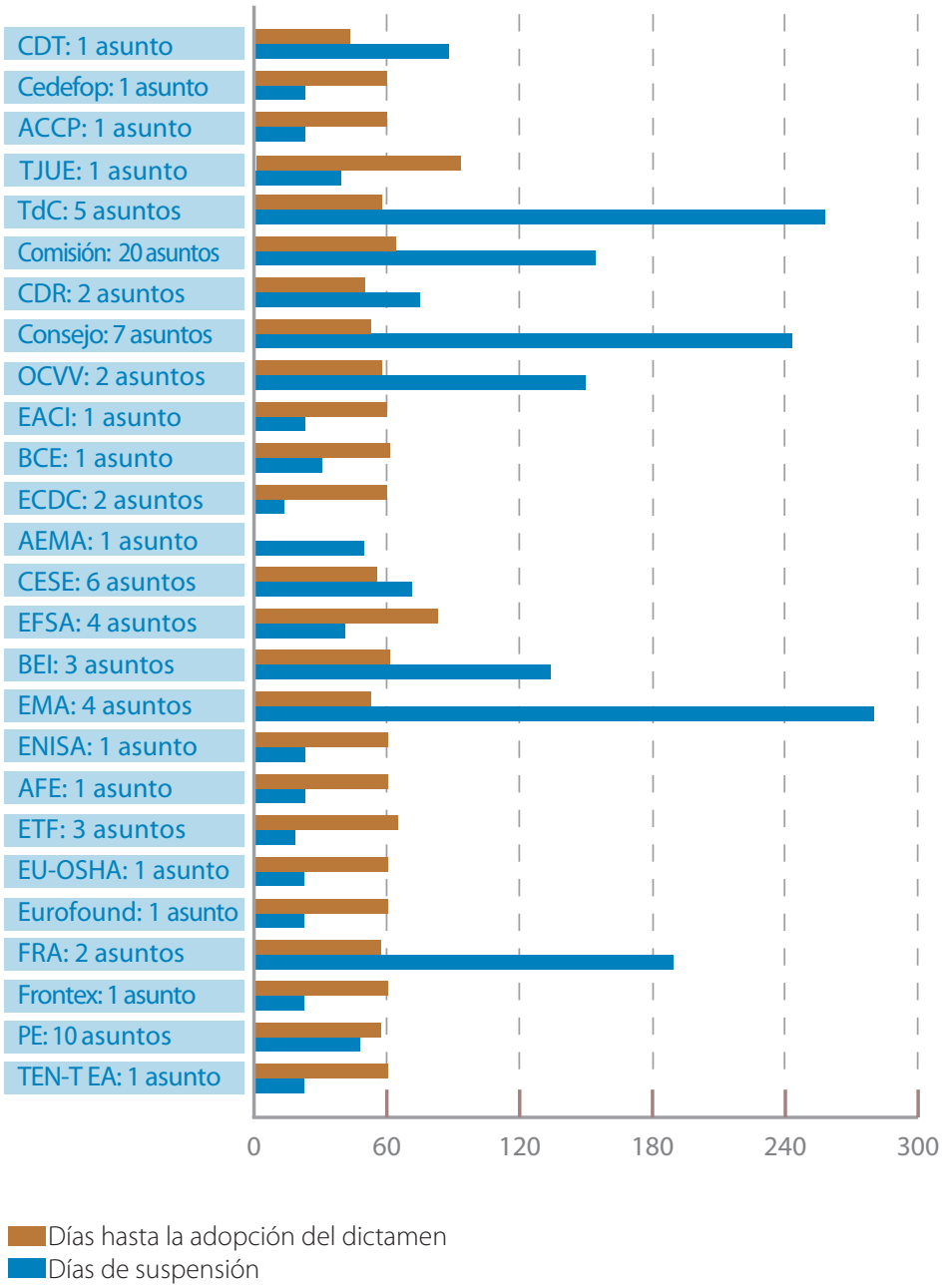
### Notificación

El SEPD debe efectuar controles previos cuando reciba 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 consultar al SEPD (véase la sección 2.3.4).

Los controles previos afectan no solo 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 del SEPD Adjunto) o de que el Reglamento entrara en vigor (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 ha debido efectuarse *ex post*.

### Plazo, suspensión y prórroga

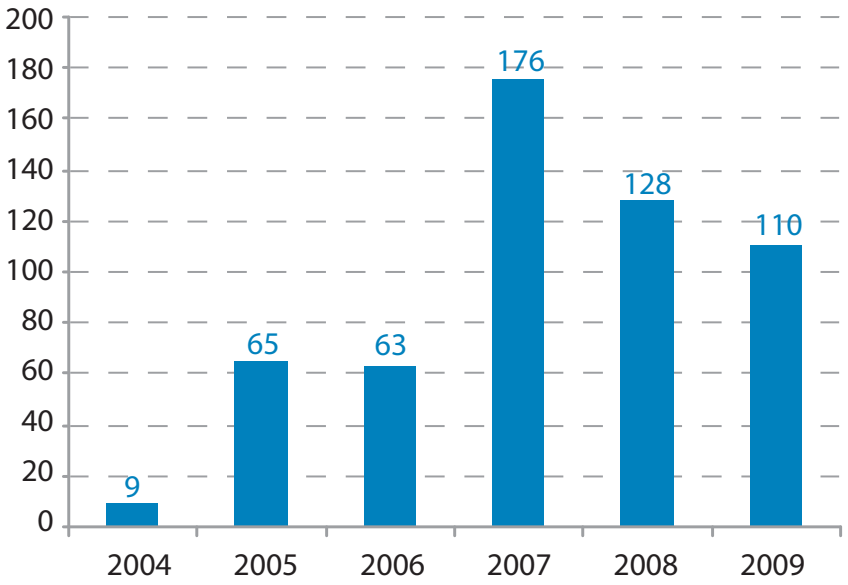
Plazos medios por institución/agencia



El SEPD debe emitir su dictamen en un plazo de dos meses a partir de la recepción de la notificación ([6]). En caso de que el SEPD solicite información complementaria, por lo general el plazo de dos meses queda por lo general aplazado hasta que la reciba. Este periodo de aplazamiento comprende el tiempo concedido al RPD de la institución u organismo para que formule sus observaciones y aporte más información, si procede, al proyecto final. En los casos complejos, el SEPD podrá prorrogar también el periodo inicial otros dos meses. Si transcurrido el plazo de dos meses, en su caso prorrogado, no se hubiera emitido dictamen, deberá entenderse que el dictamen del SEPD es favorable. Hasta ahora no se ha planteado nunca un dictamen tácito de este tipo.

## Registro

Notificaciones al SEPD



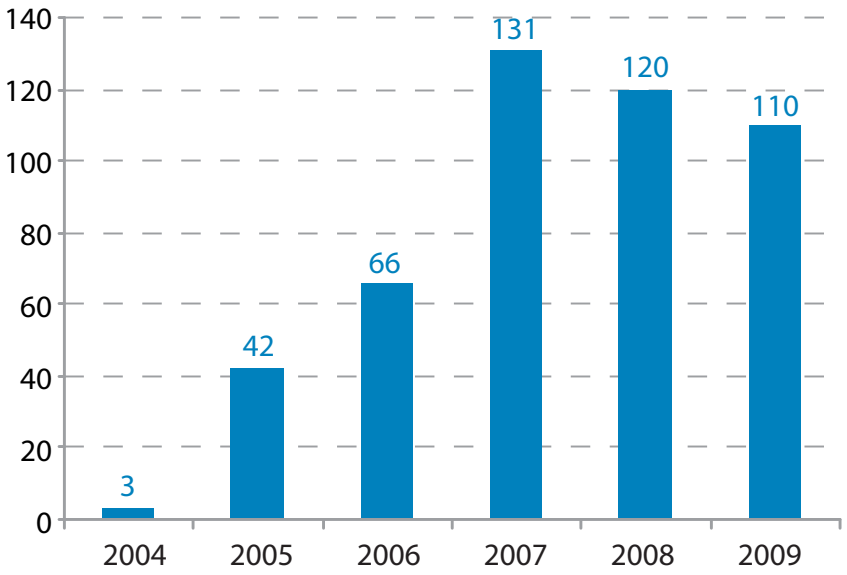

En 2009, el SEPD recibió 110 notificaciones a efectos de control previo. Esta cifra supone una ligera disminución respecto a la de 2008, ya que el SEPD está recuperando el retraso en materia de controles previos *ex post*.

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

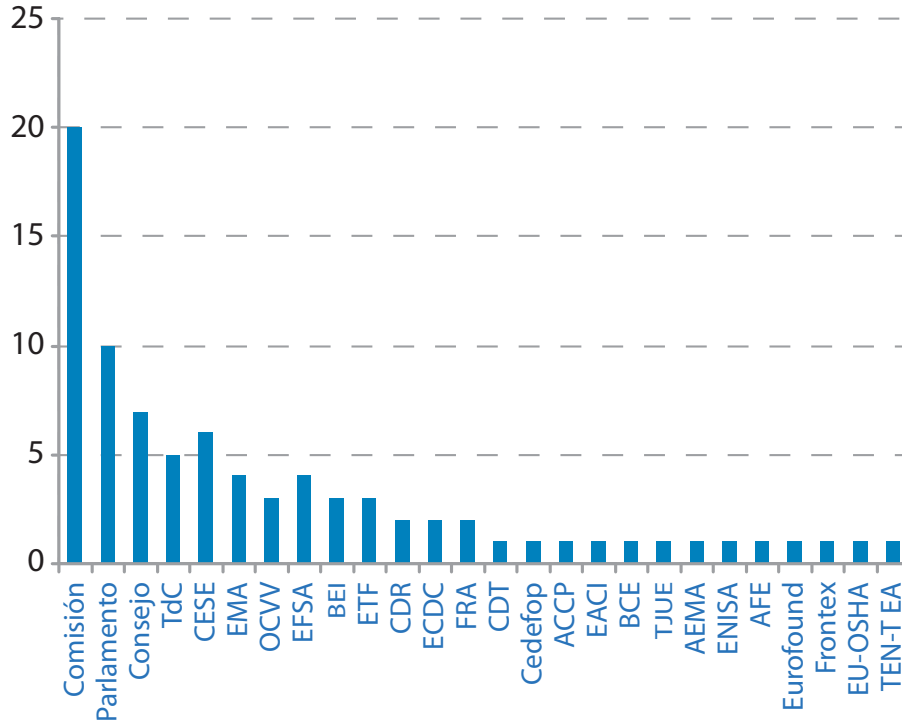
([6]) Respecto de los asuntos *ex post* recibidos antes del 1 de septiembre de 2008, no se ha calculado el mes de agosto ni para las instituciones y organismos ni para el SEPD.

## Dictámenes

Dictámenes de control previo del SEPD por año




Dictámenes de control previo del SEPD por institución en 2009



De acuerdo con el artículo 27, apartado 4, del Reglamento, la posición final del SEPD se expresará en forma de dictamen y deberá ser notificado al responsable de la operación de tratamiento de datos y al RPD de la institución u organismo de que se trate. **En 2009, el SEPD adoptó 110 dictámenes de control previo** (véase más arriba el gráfico «Dictámenes de control previo del SEPD por año»). Esta cifra supone una ligera disminución respecto a los dos años anteriores.

La **mayor parte de estos dictámenes** corresponde a las **instituciones de más envergadura**, con 20 dictámenes sobre operaciones de tratamiento en la Comisión Europea, 10 en el Parlamento Europeo y siete en el Consejo (véase más arriba el gráfico «Dictámenes de control previo del SEPD por institución en 2009»). Muchas agencias también han empezado a notificar actividades básicas y procedimientos administrativos normalizados con arreglo a los procedimientos pertinentes 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 garantizar el cumplimiento de lo dispuesto en el Reglamento. En la conclusión, normalmente el SEPD declara que el tratamiento parece no entrañar infracción de ninguna de las disposiciones del Reglamento, a condición de que se tengan en cuenta las recomendaciones presentadas.

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

Un manual de consulta garantiza que todo el equipo trabaje partiendo de un fundamento común y que los dictámenes del SEPD se adopten tras un completo análisis de toda la información pertinente. El manual presenta una estructura para los dictámenes en función de la experiencia práctica y se actualiza permanentemente. Hay un sistema de seguimiento del flujo de trabajo destinado a velar por que se apliquen todas las recomendaciones de cada asunto concreto y, si procede, por que se cumplan todas las resoluciones (véase la sección 2.3.6).

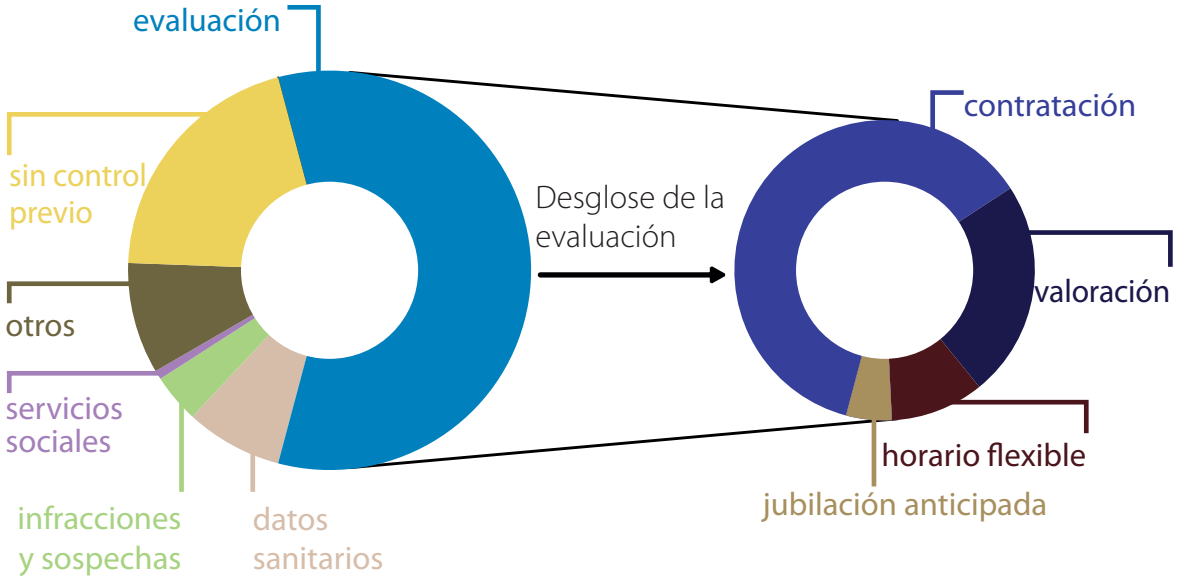
## Procedimiento para los controles previos *ex post* en las agencias

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 numerosos casos los 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 en torno a un tema similar y adoptar bien un dictamen colectivo (para varias agencias), o bien un «mini control previo», en el que aborda 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 sobre el tema correspondiente, sobre la base de dictámenes de control previo en forma de orientaciones temáticas (véase más adelante la sección 2.7, «Orientaciones temáticas»). A continuación, el RPD presenta una notificación conforme al artículo 27, con una nota de transmisión en la que se destacan los aspectos específicos respecto de la posición del SEPD en este ámbito (especificidades del tratamiento dentro del organismo, cuestiones problemáticas, etc.).

El primer tema fue la **contratación** y dio lugar, en mayo de 2009, a un dictamen transversal del SEPD, que abarcaba notificaciones de doce agencias. A finales de septiembre de 2009 se envió a los organismos un segundo conjunto de orientaciones relativa al tratamiento de los datos sanitarios. El SEPD siguió recibiendo notificaciones sobre este ámbito antes de la adopción de un dictamen transversal a principios de 2010.

## 2.3.3. Principales temas de los controles previos

### Dictámenes de 2009 por categorías




### Datos médicos y otros datos sanitarios

*Las instituciones y organismos europeos tratan datos médicos y otros datos sanitarios de las personas en diferentes situaciones relacionadas con la aplicación del Estatuto de los funcionarios (reconocimiento médico previo a la contratación, reconocimiento médico anual, reembolso de gastos médicos, certificados médicos justificativos de baja por enfermedad, etc.). Dado el carácter especialmente delicado de los datos sanitarios, las operaciones de tratamiento de estos datos están sujetas al control previo del SEPD.*

En 2009, el SEPD continuó adoptando dictámenes en el ámbito de los datos sanitarios (véase el gráfico anterior).

En septiembre de 2009, el SEPD publicó unas directrices sobre el tratamiento de tales datos con vistas al análisis de las notificaciones de las operaciones de tratamiento de datos sanitarios por parte de las agencias de la UE (véase, más adelante, la sección 2.7, «Orientaciones temáticas»). Estas directrices sirven también como conjunto de estándares del SEPD para las instituciones.

El SEPD sometió a control previo un asunto relativo al tratamiento de datos sanitarios por el **Sistema de Ayuda a la Seguridad** del Parlamento Europeo (asunto 2009-225). La recogida de datos en el Sistema de Ayuda a la Seguridad tiene por objeto proporcionar respaldo a las misiones fuera de los tres lugares de trabajo del Parlamento Europeo en caso de emergencia médica. El interesado facilita la información voluntariamente y los datos solo se utilizarán en situaciones de emergencia y únicamente se entregarán al personal sanitario local en caso de necesidad.

El SEPD reconoció que el tratamiento de los datos relacionados con la salud podía basarse en el consentimiento de los interesados en virtud del artículo 5, letra d), y del artículo 10, apartado 2, letra a), del Reglamento. Aunque el SEPD destacó que, en el contexto del empleo, el uso del consentimiento como base jurídica está sujeto a ciertas restricciones, en el caso objeto de análisis el interesado es libre de facilitar las categorías de datos mencionadas anteriormente y es informado sobre las consecuencias que podría acarrear el hecho de no facilitar la información.

El tratamiento de datos personales por las **guarderías interinstitucionales** de Bruselas (asunto 2009-088) y en una guardería infantil y centro de estudios de Luxemburgo (asunto 2009-089) planteó algunas cuestiones relativas a la protección de datos médico.

Las instituciones y órganos comunitarios recogen y tratan datos sanitarios.

En el caso del tratamiento realizado por las guarderías de Bruselas, el SEPD se mostró especialmente crítico con el hecho de que el tratamiento de los datos médicos no se limitase a verificar las admisiones en las guarderías y a reaccionar en caso de emergencia, sino que crease de hecho un control médico *de facto* de los niños por parte del Servicio Médico de la Comisión.

El SEPD recomendó que el control de la salud y el crecimiento de los niños por parte de guarderías y similares fuese asumido por el Servicio Médico únicamente con carácter voluntario y con el consentimiento expreso de los padres.

El SEPD criticó también el periodo de 30 años adoptado por la Comisión para conservar los historiales médicos de los niños matriculados en las guarderías de Bruselas. Una crítica en similares términos fue formulada a la guardería y centro de estudios de Luxemburgo, donde los datos médicos se conservan por un plazo de 10 años y a continuación se archivan. El SEPD recomendó que se revisasen tales plazos de conservación de los datos con arreglo a la necesidad específica de datos y expedientes. Además, el SEPD recomendó que se ofreciera a los padres la opción de transmitir a su médico el expediente médico de su hijo una vez que éste abandone la guardería.

Por otra parte, el SEPD consideró esencial imponer en ambos casos una obligación de secreto profesional al personal de las guarderías y centros de estudios que tenga acceso a determinados datos médicos de los niños.

## Evaluación del personal

La evaluación del personal representa una proporción importante de las operaciones de tratamiento presentadas al SEPD para control previo, y que en muchos casos incluyen procedimientos de prueba, valoración y promoción (véase el gráfico de la página 25 DU MANUSCRIP).

En los dictámenes del SEPD acerca de la evaluación del personal se observó un problema concreto relativo a los **plazos de conservación** de los datos personales tras el ejercicio de evaluación.

El SEPD consideró que los **informes de evaluación** solo deberían conservarse cinco años tras el ejercicio de evaluación, salvo que esté pendiente alguna acción judicial. Cualquier decisión resultante de estos ejercicios deberá conservarse en el expediente del miembro del personal de que se trate.

El SEPD concluyó también en estos casos que el **derecho a la rectificación** que el artículo 14 del Reglamento garantiza a los interesados podría dar lugar a que el interesado solicitara la introducción de cualquier resolución de un tribunal u otro organismo en caso de revisión de la valoración o la decisión de promoción.

Un ejemplo especialmente interesante en el ámbito de la evaluación es el dictamen del SEPD relativo a la **evaluación de 360 grados de la inteligencia emocional** realizada por la Escuela Europea de Administración (EAS) en la Comisión Europea (asunto 2009-100).

El objetivo del procedimiento es proporcionar a los participantes en los cursos de formación de la EAS una serie de reacciones, bajo la forma de un informe, que les ayude a mejorar sus competencias en los ámbitos de la autogestión, la gestión de las relaciones con terceros y la comunicación. El ejercicio se realiza mediante una herramienta en línea denominada «Emotional IntelligenceView 360». Las respuestas aportadas por los participantes y sus compañeros generan un informe automático que no revela el modo como los compañeros completaron las respuestas.

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 actividad de tratamiento, ya que determina los objetivos y los medios (el uso de la herramienta en línea). Por lo tanto, el contratista no está autorizado a ejercer ninguna otra actividad de tratamiento aparte de las determinadas por la EAS y especificadas en el contrato.

El SEPD recomendó que la EAS explorase la posibilidad de que el uso de esta herramienta en línea se realizase anónimamente. A este respecto se deberían tener en cuenta variables tales como el desarrollo de las tecnologías de la información, los procedimientos y el coste.

El SEPD abordó asimismo la cuestión de las **notas de trabajo** que el calificador puede tomar durante las reuniones de evaluación (asunto 2007-0421). De acuerdo con el SEPD, los calificadores las toman con carácter oficial, por lo que se les aplica el Reglamento. Aunque tomar notas durante el proceso de evaluación es ilegal, resulta particularmente importante que esas notas personales no terminen en una zona gris desprovista de las garantías suficientes en materia de protección de datos.

El SEPD consideró que todas las notas personales que el calificador y el evaluador tomen durante las entrevistas deben destruirse una vez redactado el informe de evaluación.

## Contratación

A finales de 2008, el SEPD publicó una serie de directrices sobre el tratamiento de los datos personales en el marco de los procedimientos de contratación, con vistas a la notificación de las operaciones de tratamiento relacionadas con dicho tratamiento por parte de los organismos de la UE (véase la sección 2.7, «Orientaciones temáticas»).

La evaluación del personal representa una amplia proporción de las operaciones de tratamiento que se presentan al SEPD para control previo.

El SEPD examinó los procedimientos de contratación del Parlamento Europeo, y concretamente el tratamiento de los datos personales en el marco de las **audiciones de los Comisarios designados** (asunto 2009-332) y en la **selección del director del Instituto Europeo de la Igualdad de Género** (asunto 2008-785). En ambos procedimientos los datos fueron recogidos inicialmente por la Comisión Europea y transmitidos al Parlamento, que procedió a la audición de los candidatos. El SEPD prestó una atención especial a la información facilitada por la Comisión Europea a los candidatos en el momento de recopilar sus datos.

También se formularon recomendaciones acerca de la conservación de datos personales con fines históricos. Pese a no presentar problemas en los procedimientos de selección concretos objeto de examen, los dictámenes de control previo revelaron la ausencia de procesos adecuados de selección y verificación sobre la base de criterios establecidos a escala institucional para conservar únicamente los datos con valor histórico. El SEPD formuló asimismo recomendaciones en el ámbito de las medidas de seguridad.

## Herramientas para la medición de resultados

El **Centro de Datos de la Dirección General de Empresa (EDW)** es un sistema que extrae datos procedentes de múltiples fuentes con el fin de tratarlos y establecer referencias cruzadas entre ellos, con vistas a obtener mediciones, indicadores e informes sobre las actividades de la Dirección General de Empresa de la Comisión Europea (asunto 2008-487). Basándose en la información recogida, la Dirección General de Empresa elaborará informes en los que presentará la métrica de resultados de los jefes de unidad, los directores y el director general. Así pues, el sistema no ha sido diseñado para medir los resultados individuales de los miembros del personal, sino para evaluar los resultados de la Dirección General en conjunto. A este respecto, el SEPD subrayó que el uso de los datos debería limitarse al que se declara explícitamente en la notificación, por ejemplo, desarrollar un cuadro de mando de la gestión y comunicar las discrepancias detectadas entre las diferentes fuentes de datos.

El SEPD hizo hincapié en que esta agregación de bases de datos aumenta el riesgo de **deriva funcional** cuando a la interrelación de dos (o más) bases de datos diseñadas para fines diferentes se le asigne un nuevo fin para el que no hayan sido creadas, resultado que se encuentra en clara contradicción con el principio de limitación de la finalidad. Para recibir autorización, el propósito debe estar claramente delimitado y demostraba su necesidad. Por lo tanto, el EDW deberá limitar el uso a los datos procedentes de las bases de datos declaradas en la notificación y exigir una autorización adicional antes de añadir otras fuentes de datos.

## Gestión del tiempo

Los sistemas de gestión del tiempo siguieron suscitando un interés particular, especialmente cuando las instituciones y organismos de la UE decidían **establecer una interfaz entre los sistemas de gestión del tiempo** y otros sistemas.

El Tribunal de Cuentas Europeo deseaba vincular el Sistema de Gestión de Auditorías (Assyst) al sistema de horario flexible del Tribunal (Efficient) mediante la llamada **herramienta ART** (asunto 2008-239). El propósito de la operación de tratamiento consiste en permitir que los diferentes auditores y sus jefes de unidad concilien el tiempo que tienen registrado en Assyst con Efficient, velar por la coherencia entre ambos y verificar cualquier discrepancia que pudiera surgir.

El SEPD concluyó que, dado que la agregación de bases de datos aumenta el riesgo de deriva funcional, tal propósito debía estar claramente delimitado y su necesidad demostrada. En este caso concreto, al principio la necesidad no se había establecido claramente y era preciso seguir desarrollándola. Este instrumento ha sido adoptado posteriormente por el Tribunal de Cuentas Europeo.

La gestión del tiempo puede plantear cuestiones relacionadas con la protección de datos, especialmente cuando las instituciones de la UE deciden interconectar sistemas de gestión del tiempo con otros sistemas.

También suscitó preocupación el dictamen del SEPD en relación con un sistema previsto de **comprobación del horario flexible mediante comparación con datos sobre el acceso físico** a la Secretaría General del Consejo (SGC) (asunto 2009-477). La SGC utiliza un sistema de flexibilización del horario laboral que registra el tiempo de trabajo y la asistencia, con lo que facilita el cálculo de las horas extraordinarias y los derechos en materia de permisos. Esta aplicación ya se había sometido al control previo del SEPD. La SGC dispone también de un sistema de control de acceso gestionado por la oficina de seguridad y accesible a los servicios de administración en el marco de una investigación formal. La comparación de ambos conjuntos de datos tiene por objetivo identificar a las personas que transgreden las normas del horario flexible y evaluar su comportamiento. El sistema podría asimismo dar lugar a la adopción de medidas disciplinarias.

En su dictamen, el SEPD consideró que la necesidad y la proporcionalidad de la comprobación del horario flexible mediante comparación con datos sobre el acceso físico eran cuestionables. Según el SEPD, no existen pruebas razonables que demuestren que la aplicación de un sistema de control que compare el tiempo medido con los datos sobre acceso físico sea necesaria a los fines de la gestión del personal o de las funciones de la SGC.

Por lo tanto, el SEPD estimó que el tratamiento previsto infringiría varios preceptos del Reglamento (necesidad y proporcionalidad, cambio de finalidad, calidad de los datos) salvo que se realizase a los fines de una investigación administrativa determinada.

## Investigaciones de seguridad

El SEPD analizó los procedimientos instaurados para abordar las amenazas contra los intereses de la Comisión en los ámbitos de la **contrainteligencia** y la **lucha contra el terrorismo** (asunto 2008-440). Se analizaron dos operaciones de tratamiento concretas: las **investigaciones de seguridad** y los **procedimientos de control de seguridad**. Las investigaciones de seguridad se centraron en las filtraciones de información clasificada de la UE por empleados de la Comisión, mientras que el objetivo de los procedimientos de control de seguridad es prevenir la contratación o la celebración de contratos con personas que representan una amenaza para los intereses de la Comisión.

El SEPD acogió favorablemente las diferentes medidas introducidas por la unidad responsable, y especialmente el análisis fundamental que la unidad realiza caso por caso sobre la **necesidad** del procedimiento de control según los procedimientos especificados. El SEPD recomendó que, al recopilar y tratar datos personales, los investigadores tomasen también en consideración los criterios de **proporcionalidad**.

## Grabaciones de llamadas telefónicas

*Las grabaciones de llamadas telefónicas suscitan una preocupación especial, pues el registro de las llamadas constituye una violación del **principio de confidencialidad de las comunicaciones**.*

El SEPD examinó el registro de comunicaciones con fines de seguridad en el Instituto de Energía del Centro Común de Investigación (CCI-IE) (asunto 2008-0014). Este asunto se refiere al registro de las llamadas entrantes y salientes (con detalles relativos a los números de salida y de entrada de la llamada, así como la fecha, la hora y la duración de esta) para uso en caso de incidentes operativos, emergencias, evaluación de ejercicios de formación de emergencia e investigaciones de posibles amenazas. El SEPD reconoció que las grabaciones de

llamadas telefónicas tiene una base jurídica en la legislación nacional relativa a las instalaciones nucleares, pero recomendó que al inicio de las llamadas se informe a las personas externas que las realicen de que su comunicación quedaría grabada por motivos de seguridad.

## EudraVigilance

La Agencia Europea de Medicamentos (EMA) aloja y gestiona la base de datos EudraVigilance, que contiene **informes sobre sospechas de reacciones adversas a medicamentos de uso humano** (informes de seguridad relativos a casos individuales). EudraVigilance facilita la notificación y la evaluación de estos informes. Las autoridades nacionales competentes, los titulares de autorizaciones de comercialización y los patrocinadores de ensayos clínicos facilitan dicha información a la EMA.

El SEPD analizó las operaciones de tratamiento de los datos relacionados con EudraVigilance e hizo hincapié en la responsabilidad compartida de los diferentes responsables del tratamiento de datos que han de velar por el respeto de los derechos de los titulares de los datos (asunto 2008-402). Los responsables del tratamiento de datos a nivel nacional y de la UE deben coordinar y aunar esfuerzos para garantizar el cumplimiento de la legislación nacional y de la UE en materia de protección de datos.

El SEPD recomendó que la EMA considerase la posibilidad de dar un carácter anónimo o pseudoanónimo a la información personal contenida en los informes de seguridad relativos a casos individuales y reducir al mínimo los datos personales contenidos en dichos informes. También recomendó que la EMA preparase, en colaboración con los responsables nacionales del tratamiento de datos, un formulario de notificación centralizado para facilitar a las personas la información legalmente obligatoria. Dicho formulario debía incluir una referencia a EudraVigilance.

## Suspensión de la inmunidad

De conformidad con el Protocolo sobre los privilegios e inmunidades de las Comunidades Europeas, los funcionarios y agentes de las Comunidades gozan de diversos tipos de inmunidades. La **Oficina de Investigación y Disciplina** de la Comisión (IDOC) se encarga de evaluar las solicitudes de suspensión de cualquiera de estas inmunidades presentadas por tribunales u otros organismos nacionales. El SEPD sometió a control previo el procedimiento establecido por la IDOC para la suspensión de dichas inmunidades (asunto 2008-645).

En la mayor parte de los casos, las autoridades nacionales piden a la IDOC que lleve a cabo sus investigaciones en secreto, lo que limita los derechos de los titulares de los datos, ya que no son conscientes de la investigación y no pueden ejercer sus derechos de acceso y rectificación en el curso de tales investigaciones. El SEPD destacó que cualquier limitación de los derechos de los interesados debe ser temporal y que el titular de los datos ha de tener la posibilidad de ejercer el derecho de acceso tan pronto como el secreto deje de estar justificado.

Efectuada la investigación, la IDOC transfiere su resolución y ciertos datos a la autoridad o tribunal nacional solicitante. El SEPD recomendó que la IDOC llevase un registro de los receptores de estos datos en el que constase la justificación legal de la transferencia.

Dado que la suspensión de la inmunidad suele formar parte de un procedimiento más amplio que puede dar o no lugar a otras acciones, el SEPD recomendó que si se procede al archivo definitivo de los procedimientos disciplinarios o los procesos judiciales o si se absuelve al interesado, los periodos de conservación del expediente se reduzcan.

## Proyectos piloto

En tres casos relativos a proyectos piloto, el SEPD aprovechó la oportunidad para recordar a las instituciones y agencias **las normas que regulan el control previo de los proyectos piloto**. Mediante la formulación de recomendaciones previas al pleno desarrollo de un sistema, el SEPD desea reducir al mínimo las modificaciones que el responsable del tratamiento de datos tendrá que realizar posteriormente.

> Los resultados del proyecto piloto se deberán analizar y ser comunicados al SEPD antes de que se inicie el proyecto general y el SEPD deberá ser informado de cualquier modificación que pueda repercutir en el tratamiento de datos personales. El dictamen de control previo debería considerarse la conclusión del análisis final del proyecto piloto.

## 2.3.4. Consultas sobre la necesidad de control previo

A lo largo de 2009, el SEPD recibió 21 consultas del RPD sobre la necesidad de proceder a control previo (basándose en el artículo 27, apartado 3, del Reglamento), 11 de las cuales procedían del RPD del Parlamento Europeo.

*Varios casos fueron declarados aptos para ser **sometidos a un control previo**, por ejemplo:*
- *los datos relacionados con la huelga en el Banco Central Europeo;*
- *las audiciones de los Comisarios designados ante el Parlamento Europeo;*
- *la evaluación ergonómica de los entornos de trabajo del Parlamento Europeo;*
- *los nombramientos de personal directivo en el Parlamento Europeo.*

El tratamiento de datos personales por parte del **Servicio Jurídico y la Unidad de Asuntos Jurídicos del Parlamento Europeo** en el contexto de sus respectivas obligaciones de examen de asuntos, elaboración de respuestas a peticiones y reclamaciones y procedimientos judiciales no se consideró sujeto a control previo por el SEPD (asunto 2009-263).

La mera posibilidad de presencia de **datos sensibles** no conlleva automáticamente un control previo. No obstante, la presencia de datos sensibles en el tratamiento de casos tales como los datos sanitarios o los datos relativos a infracciones significa que es preciso prestar una atención particular a la adopción de medidas de seguridad de conformidad con el artículo 22 del Reglamento.

Aunque algunas de las operaciones de tratamiento podrían guardar relación con una evaluación de los aspectos personales, el tratamiento no tiene por objetivo evaluar al titular de los datos, de manera que en estos casos no es de aplicación el artículo 27, apartado 2, letra b).

Del mismo modo, en relación con el artículo 27, apartado 2, letra d), aunque las operaciones de tratamiento podrían conducir a que a un individuo se le excluyese de un derecho, beneficio o contrato, no es este su propósito específico y único.

También se consultó al SEPD sobre el tratamiento de datos personales en el curso del **procedimiento de selección de los asistentes de los diputados al Parlamento Europeo**. De conformidad con la información recibida, el Parlamento Europeo (PE) no se encarga del procedimiento de selección, por lo que el SEPD estimó que la operación de tratamiento no debería someterse a control previo. El SEPD destacó sin embargo que ello no significa que los asistentes de los diputados al Parlamento Europeo no gocen de ciertos derechos de protección de datos por los que el Parlamento Europeo debe velar.

## 2.3.5. Notificaciones no sometidas a control previo y notificaciones retiradas

En 2009, el SEPD también tramitó 21 asuntos que, tras un cuidadoso análisis, no se consideraron sujetos a control previo. En tales situaciones, el SEPD aún está habilitado para formular recomendaciones.

### Youthlink 2

Un asunto interesante fue el relativo a **Youthlink 2**, el principal registro de datos (estadísticos y financieros) sobre proyectos y actividades presentados en el marco del programa «La juventud en acción» de la Comisión Europea (asunto 2008-484).

El SEPD concluyó que la selección de los beneficiarios de los programas «La juventud en acción» **no conllevaba una evaluación de conductas o capacidades individuales**, sino que era una verificación del proyecto propuesto con arreglo a unos criterios predefinidos y una comprobación de la capacidad financiera y operativa de las personas jurídicas o grupos solicitantes. Además, se trata de una evaluación descentralizada, pues no la realiza el responsable del tratamiento de datos de la Comisión Europea, sino que la llevan a cabo las diferentes agencias nacionales sujetas a sus respectivas legislaciones de protección de datos, o bien la Agencia Ejecutiva en el Ámbito Educativo, Audiovisual y Cultural (EACEA). Por lo tanto, el SEPD consideró que el artículo 27, apartado 2, letra b), del Reglamento no era de aplicación.

### Encuestas de satisfacción del consumidor

El SEPD consideró que las **encuestas de satisfacción del consumidor** del Banco Central Europeo (BCE) **no estaban sujetas a control previo**, pues su objetivo no es evaluar a las personas, sino los servicios, exactamente del mismo modo que el objetivo de una auditoría no es evaluar el

rendimiento de las personas, sino la realización del trabajo por una unidad o un proceso organizativo (asunto 2008-780). El BCE se había esforzado por reducir al mínimo la posibilidad de que pudieran llegar a evaluarse aspectos personales de un individuo. No obstante, el SEPD sugirió que el BCE siguiera tomando medidas para reducir al mínimo la posibilidad de que se incluyese información personal en los resultados de la encuesta, y en particular la que podría originarse en las respuestas a preguntas abiertas.

### Uso del teléfono móvil

Respecto de la notificación acerca del **uso de teléfonos móviles** por el personal de la Agencia Ejecutiva de Competitividad e Innovación (EACI) que se encuentra realizando una misión, el SEPD concluyó que el asunto **no estaba sujeto a control previo** (asunto 2009-162). El objetivo del tratamiento era garantizar que los costes de las llamadas privadas se reembolsasen a la EACI. Por consiguiente, el tratamiento no tenía por objetivo evaluar la capacidad, la eficacia o la conducta de los miembros del personal y no formaba parte del ámbito de aplicación del artículo 27, apartado 2, letra b).

### Gestión de la identidad y del acceso

El SEPD estimó que el **Sistema de Gestión de la Identidad y del Acceso** del Tribunal de Cuentas Europeo no estaba sujeto a control previo (asunto 2009-639). Aunque el sistema utiliza cierta información (nombre, apellido y fecha de nacimiento) para asignar cuentas a los usuarios y brindarles acceso a las mismas, no evalúa a las personas: lo hace para autenticar su identidad y sus derechos de acceso. Una mera comprobación de los derechos basada en normas predefinidas no supone una evaluación *de facto* de la eficiencia, las competencias, la capacidad de trabajo o el comportamiento del usuario, por lo que el asunto no corresponde al artículo 27, apartado 2, letra b).

## 2.3.6. Seguimiento de los dictámenes de control previo

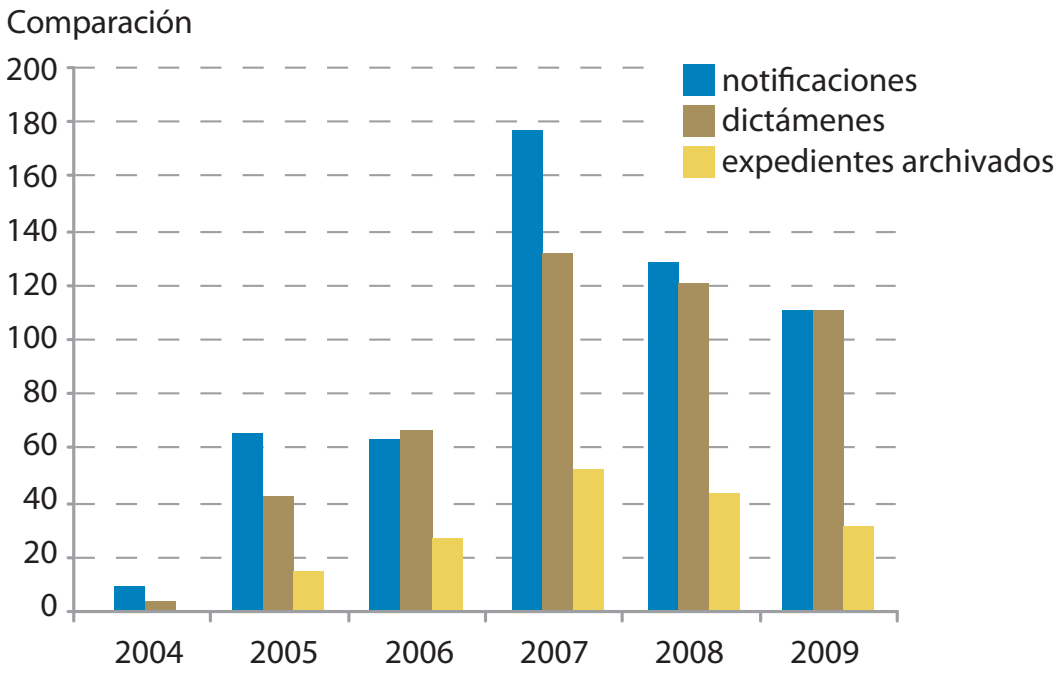
*Los dictámenes de control previo del SEPD incluirán **recomendaciones** que deberán ser tenidas en cuenta para que la operación de tratamiento se ajuste a lo dispuesto en el Reglamento. También se formulan recomendaciones cuando, al analizar un caso para decidir si requiere control previo, se ponen de manifiesto ciertos aspectos críticos que parecen requerir medidas correctoras. Si el responsable del tratamiento desatiende estas recomendaciones, el SEPD puede ejercer las atribuciones que le otorga el Reglamento (CE) nº 45/2001. En particular, el SEPD puede someter el asunto a la institución u organismo comunitario de que se trate.*

La mayor parte de los casos de control previo han dado lugar a recomendaciones relacionadas principalmente con:

- la información a los interesados;
- los plazos de conservación de los datos;
- la limitación de la finalidad, y los derechos de acceso y rectificación.
- los derechos de acceso y rectificación.

Las instituciones y organismos muestran buena disposición para seguir estas recomendaciones, y 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.

Pese a los recordatorios remitidos a las instituciones y organismos para que faciliten dicha reacción, en 2009 el SEPD solo archivó 32 asuntos y dejo diversos casos abiertos. Por tal motivo, el SEPD ha instado a las instituciones y organismos a que lleven a cabo el seguimiento de sus dictámenes con el fin de poder archivar el asunto convenientemente.




### 2.3.7. Conclusiones y futuro

*La mayor parte de las principales instituciones están ultimando la notificación de sus operaciones de tratamiento y la mayoría de las agencias están avanzando en la notificación de actividades comerciales principales que incluyen el tratamiento de datos personales y los procedimientos administrativos normalizados (de conformidad con el nuevo procedimiento establecido para ellas).*

Los 110 dictámenes adoptados han proporcionado al SEPD una visión de las operaciones de tratamiento de las administraciones europeas y le han permitido destacar sus recomendaciones. Asimismo, la experiencia acumulada en la aplicación del Reglamento ha permitido al SEPD adquirir conocimientos y ofrecer orientación genérica en determinados ámbitos (véase la sección 2.7, «Orientaciones temáticas»).

La mayor parte de los asuntos sujetos a control previo dieron lugar a recomendaciones del SEPD y requirieron reacciones de las instituciones y organismos sobre la aplicación de dichas recomendaciones. En 2009 se archivaron pocos asuntos, por lo que el SEPD seguirá trabajando con el fin de obtener mejoras en este ámbito.

## 2.4. Reclamaciones

### 2.4.1. El mandato del SEPD

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

En principio, las personas solo pueden presentar reclamaciones relativas a supuestas violaciones de sus derechos de protección de los datos personales. Únicamente los miembros del personal de la UE pueden presentar reclamaciones acerca de supuestas violaciones de las normas de protección de datos tanto si están directamente afectados por el tratamiento como si no es este el caso. El Estatuto de los funcionarios de la Unión Europea también permite presentar reclamaciones al SEPD [artículo 90, letra b)].

En un interesante caso relativo a los **datos de un menor**, el SEPD consideró que un progenitor en el ejercicio de su autoridad parental legítima puede, en principio, acceder a los datos de su hijo. El asunto se refería al acceso a los documentos


Cualquier persona puede presentar al SEPD una reclamación relacionada con el tratamiento de datos personales por la Administración de la UE.

relativos a la matrícula de un niño en una guardería gestionada por una institución de la UE. El reclamante afirmó que no se le había permitido acceder plenamente a los documentos presentados por el otro progenitor, de quien estaba divorciado. En particular, los nombres de las personas autorizadas a recoger al niño de la guardería no estaban escritos íntegramente.

El SEPD estableció que, en principio, el progenitor que ejerce una autoridad parental compartida legítima tiene derecho a acceder a los datos del niño. En este caso, el SEPD concluyó que tales derechos cubrían también los datos de los terceros autorizados a recoger al niño, pues, por su naturaleza, guardaban relación con los del niño.

El SEPD consideró que al negarse a dar al reclamante acceso a los datos del niño escritos de manera inteligible, la institución en cuestión quebrantaba el artículo 13 del Reglamento.

De conformidad con el Reglamento, el SEPD solo puede investigar reclamaciones presentadas por **personas físicas**. Las reclamaciones presentadas por empresas u otras personas jurídicas no son admisibles. Además, los reclamantes deben identificarse, por lo que las peticiones anónimas no se consideran una «reclamación». Sin embargo, se puede tener en cuenta información anónima en el marco de otro procedimiento (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, modificar el contenido de documentos que el reclamante cuestione o conceder compensaciones financieras en concepto de daños.*

En particular, el hecho de que el Reglamento mencione la «rectificación de los datos personales» no significa que el SEPD sea competente para revisar el contenido de las decisiones por incluir algunos datos personales. En estos casos se aconseja al reclamante que se dirija al Defensor del Pueblo Europeo o al tribunal competente.

*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 autoridad de recurso para las autoridades nacionales de protección de datos.*

## 2.4.2. Procedimiento de tramitación de reclamaciones

El SEPD tramita reclamaciones con arreglo a la base jurídica existente, los principios generales del Derecho de la UE y las buenas prácticas administrativas comunes a las instituciones y organismos de la UE. Con el fin de facilitar la tramitación de reclamaciones. En diciembre del 2009 el SEPD adoptó un **manual interno** diseñado para orientar al personal en la tramitación de reclamaciones. En particular, el SEPD llevó a cabo una revisión minuciosa de las condiciones para admitir a trámite las reclamaciones. A lo largo de 2009, el SEPD aplicó también una **herramienta estadística** diseñada para llevar un control de las actividades relacionadas con reclamaciones, y en particular para controlar la evolución de determinados casos.

En todas las fases de la tramitación de una reclamación, el SEPD respalda 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 del supuesto incumplimiento 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 violación;
- la importancia global potencial del caso, también en relación con el resto de los intereses públicos o privados implicados;
- la probabilidad de que se determine que la infracción se ha cometido;
- la fecha exacta en que sucedieron los hechos, cualquier conducta que haya dejado de tener efecto, la desaparición de esos efectos o una garantía adecuada de tal desaparición.

Toda reclamación recibida por el SEPD se somete a un atento análisis. El examen preliminar de la reclamación está diseñado específicamente para verificar si ésta cumple las condiciones para seguir investigando, incluida la condición de que existan motivos suficientes para una investigación.

Una reclamación para la que el SEPD **carezca de competencia jurídica** se declarará como no admisible a trámite, hecho del cual se informará debidamente al reclamante. En estos casos, el SEPD informa al reclamante acerca de otros organismos que puedan ser competentes (por ejemplo, tribunales, Defensor del Pueblo Europeo, autoridad nacional de protección de datos, etc.).

Una reclamación sobre hechos **manifiestamente insignificantes** o cuya investigación requeriría **esfuerzos desproporcionados** no se sigue 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. Esto incluye un análisis de las restantes opciones disponibles para ocuparse de la cuestión, ya sea por el reclamante, ya por el SEPD. Por ejemplo, el SEPD puede abrir una investigación por iniciativa propia de un problema general en lugar de una investigación sobre un asunto individual presentado por el reclamante. En estos casos se informa al reclamante sobre esos otros medios de acción.

*Se comunicó anónimamente al SEPD que los datos personales de los candidatos que superan las **pruebas de preselección** de las oposiciones a funcionarios de la UE son tratados por un **contratista externo ubicado en un Estado que no es miembro de la UE**. El SEPD abrió una investigación del asunto por iniciativa propia y averiguó que, aunque la Oficina Europea de Selección de Personal (EPSO) había celebrado un contrato con una empresa externa registrada en el Reino Unido, las operaciones de tratamiento de los datos se realizaban en Estados Unidos. El SEPD pidió a la EPSO que verificara el cumplimiento de todas las condiciones recogidas en el artículo 9 del Reglamento y modificase el contrato de modo que incluyera garantías adicionales para los interesados.*

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, el reclamante ha de presentar al SEPD razones suficientes para no hacerlo.

Si la cuestión ya está siendo examinada por los organismos administrativos (es decir, si el organismo ya está llevando a cabo una investigación interna), en principio la reclamación podrá admitirse 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 relativas a la 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, dicho documento estipula que una reclamación presentada previamente no debería ser reabierta por la otra institución salvo que se aporten nuevas pruebas significativas.

En cuanto a los **plazos de conservación de los datos**, si los hechos abordados por el SEPD se presentan en un plazo superior a dos años, en principio la reclamación es inadmisible. El periodo de dos años empieza a contar desde la fecha en que el reclamante hubiera tenido conocimiento de los hechos.

Si la reclamación es admisible, el SEPD iniciará una **investigación** en la medida que considere adecuada. Dicha investigación puede incluir una petición de información a la institución afectada, un análisis de 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 final 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 postura acerca de cualquier infracción de las normas de protección de datos por la institución de que se trate. Los **poderes del SEPD** son amplios y van desde el simple asesoramiento a los titulares de los datos a 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 parte interesada puede solicitar al SEPD una revisión de la decisión en el mes siguiente a la emisión de esta. Las partes afectadas pueden también apelar directamente al Tribunal de Justicia. En 2009, los reclamantes impugnaron en dos ocasiones las decisiones del SEPD ante el Tribunal de Primera Instancia (asuntos T-164/09 y T-193/09).

### 2.4.3. Garantía de confidencialidad para los reclamantes

*El SEPD reconoce que algunos reclamantes ponen su carrera profesional en peligro al denunciar violaciones de las normas de protección de datos y que, por consiguiente, se debería garantizar **confidencialidad** a los reclamantes e informantes que la soliciten. Por una parte, el SEPD se compromete a trabajar con **transparencia** y a publicar al menos lo esencial de sus decisiones. Los procedimientos internos del SEPD 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 las terceras partes implicadas acerca del contenido de la reclamación y de la identidad del reclamante. Además, el SEPD copia al responsable de la protección de datos (RPD) de la institución de que se trate en toda la correspondencia que mantiene con la institución.

Si el reclamante solicita el **anonimato** respecto de la institución, el RPD o los terceros implicados, se le invita a explicar las razones de tal petición. A continuación, el SEPD analiza los argumentos del reclamante y examina las consecuencias en la viabilidad de su posterior investigación. Si el SEPD decide no aceptar el anonimato del reclamante, le explica su evaluación y le pregunta si desea que examine la reclamación sin garantizarle el anonimato o si prefiere retirar la reclamación. Si el reclamante decide

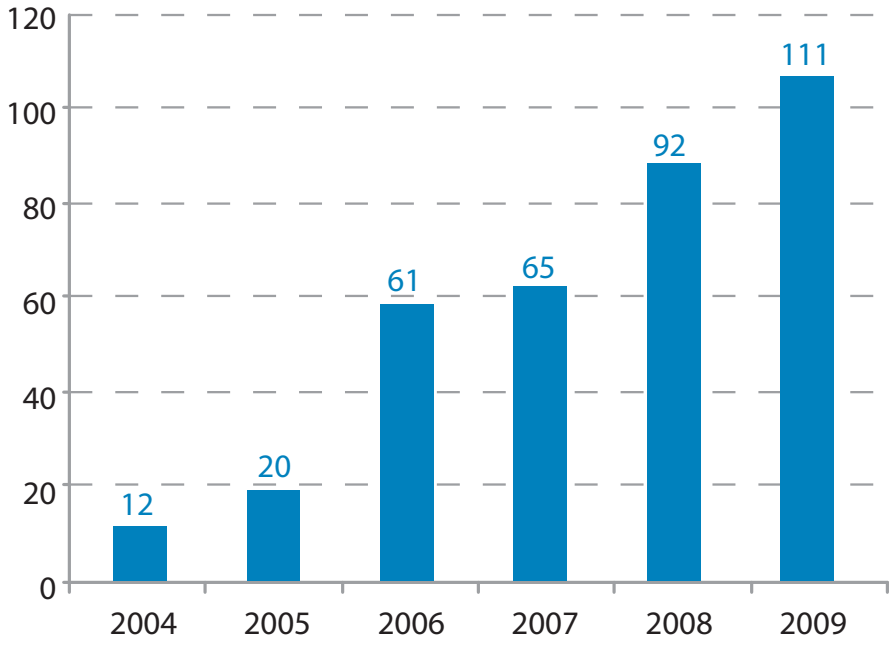
retirar la reclamación, la institución de que se trate no será informada de la existencia de esta. En tal caso, el SEPD podría emprender otras acciones en relación con la cuestión sin revelar a la institución afectada la existencia de la reclamación, es decir, podría realizar una investigación por iniciativa propia o solicitar una notificación de operación de tratamiento de datos.

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

## 2.4.4. Reclamaciones atendidas en 2009

### *2.4.4.1. Número de reclamaciones*

Número de reclamaciones recibidas (evolución 2004-2009)




*Las reclamaciones recibidas por el SEPD están aumentando en número y complejidad.* ***En 2009, el SEPD recibió 111 reclamaciones*** *(lo que supone un incremento del 32 % respecto a 2008). De estas,* ***69 reclamaciones fueron admitidas a trámite****, la mayoría relacionadas con el tratamiento a escala nacional, por contraposición con la tramitación por alguna institución u organismo de la UE.*
*Las 42 reclamaciones restantes requirieron investigaciones a mayor profundidad (lo que supone un incremento del 83 % respecto a 2008). Además, 14 reclamaciones presentadas en años anteriores y admitidas trámite (13 en 2008 y una en 2007) seguían en fase de investigación o de revisión.*

### *2.4.4.2. Tipos de reclamante*

De las 111 reclamaciones recibidas, 26 (el 23 %) fueron presentadas por miembros del personal de las instituciones u organismos de la UE, incluidos antiguos miembros del personal y candidatos a un puesto. Una reclamación era anónima, mientras que en los 84 casos restantes el reclamante no parecía mantener una relación laboral con la administración de la UE.

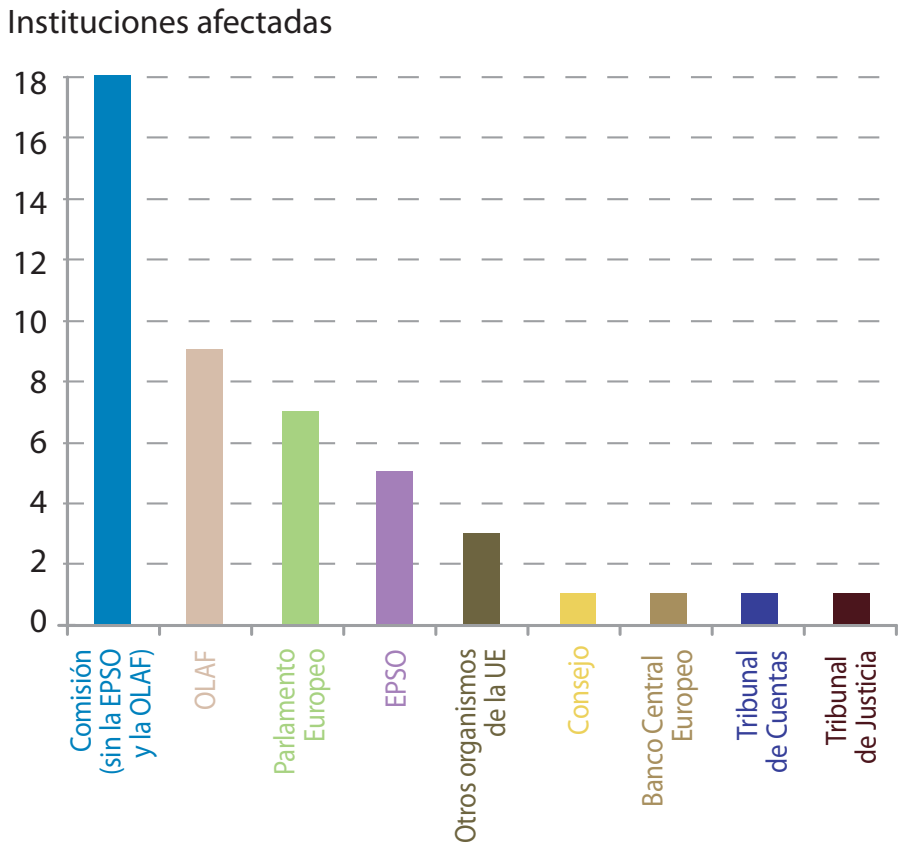
### *2.4.4.3. Instituciones objeto de reclamación*

La mayor parte de las reclamaciones admisibles presentadas en 2009 (más del 70 %) iban dirigidas contra la **Comisión Europea, incluidas la Oficina Europea de Lucha contra el Fraude (OLAF) y la Oficina Europea de Selección de Personal (EPSO)**. No tiene nada de particular, ya que la Comisión trata un mayor número de datos personales que otras instituciones y organismos de la UE.

El elevado número de reclamaciones relacionadas con la OLAF y con la EPSO puede explicarse por la naturaleza de las actividades que llevan a cabo estos organismos.

### *2.4.4.4. Lengua de las reclamaciones*

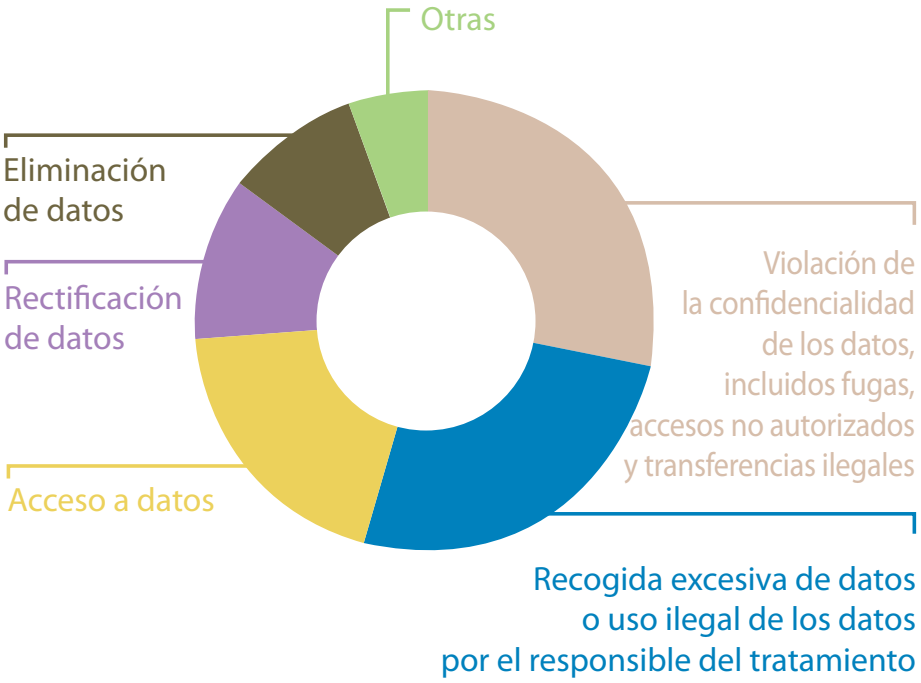
La mayor parte de las reclamaciones se presentaron en inglés (el 64 %); el alemán (19 %) y el francés (9 %) se utilizaron menos. Las reclamaciones en otras lenguas fueron relativamente escasas (el 8 %).



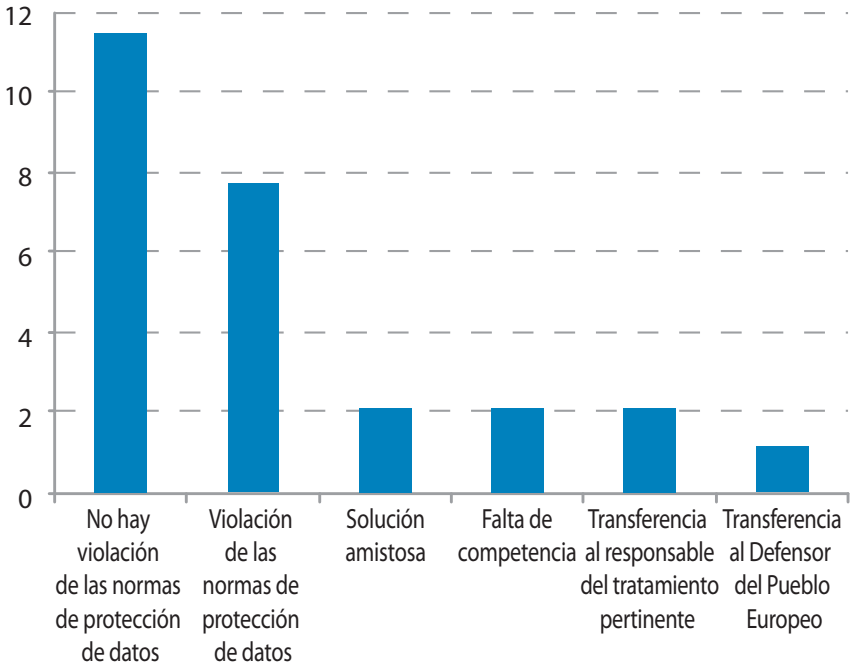

### *2.4.4.5. Tipos de violaciones denunciadas*

Los principales tipos de violación de las normas relativas a la protección de los datos denunciadas por los reclamantes en 2009 fueron: violación de la confidencialidad de los datos, incluidas las filtraciones, los accesos no autorizados y las transferencias ilegales (31 %) y la exceso de celo en la recogida de datos o la utilización ilegal de los mismos por parte del responsable del tratamiento (28 %). Con menor frecuencia se denunciaron otras violaciones, a saber: acceso a los datos (20 %), rectificación de los datos (12 %), supresión de los datos (10 %), videovigilancia (2 %), transferencia de datos fuera de la UE (2 %) y pérdida de datos (2 %).

Tipos de violaciones denunciadas




Resultados de las investigaciones del SEPD



### *2.4.4.6. Resultados de las investigaciones del SEPD*

En 12 de los asuntos resueltos durante 2009, el SEPD no detectó violación de las normas de protección de datos.

*En un asunto dirigido contra la Comisión Europea, un antiguo miembro del personal se quejó de que se le había negado copia de un informe sobre una investigación administrativa efectuada por la Comisión. La Comisión se negó a facilitarle acceso al texto completo del informe y se justificó aduciendo la necesidad de proteger los derechos y libertades de terceros, y en particular los de los testigos que habían declarado en el caso. Sin embargo, facilitó al reclamante acceso a las apreciaciones fácticas que le afectaban y a las conclusiones finales del informe. Dado que la revelación del texto completo podía tener consecuencias adversas en algunas de las personas afectadas, el SEPD consideró que las acciones de la Comisión cumplían los requisitos del artículo 13 del Reglamento, a la vez que protegían los derechos y libertades de terceros.*

En cambio, en ocho de los casos no se respetaban las normas de protección de datos y se presentaron recomendaciones al responsable del tratamiento.

*En un caso, un miembro del personal denunció las irregularidades de un organismo en relación con una investigación sobre las cualificaciones profesionales de los miembros de su personal. El reclamante alegó que el empresario había transferido ilegalmente documentos considerados confidenciales en los que se acreditaban las cualificaciones a diversos receptores de las instituciones de la UE y ajenos a ellas.*

*Sobre la base de la información facilitada por el responsable del tratamiento de datos, el SEPD concluyó que las transferencias dentro de la UE eran necesarias para que los receptores pudieran ejercer legítimamente sus funciones. En relación con las transferencias a terceros, si bien el SEPD se mostró satisfecho de que se hubieran realizado conforme al artículo 8, consideró que la transferencia a una consultoría mediática (contratada para ocuparse de la posible cobertura de la investigación en la prensa) fue excesiva en vista de las tareas efectuadas por el receptor. Por consiguiente, el SEPD concluyó que esa transferencia incumplía el principio de calidad de los datos, pues el organismo de la UE afectado violaba el artículo 4, apartado 1, letra c).*

En dos asuntos, el SEPD contribuyó a una solución informal entre el reclamante y la institución afectada y no se suscribió ninguna decisión.

## 2.4.5. Trabajo adicional en el ámbito de las reclamaciones

La adopción del **manual interno para la tramitación de reclamaciones** en diciembre de 2009 facilitó la revisión de las páginas pertinentes del sitio del SEPD en Internet. La nueva página describe los principales elementos del procedimiento e incluye un formulario descargable para la presentación de reclamaciones, junto con información sobre cómo admitir a trámite. Esta información, publicada en la página web del SEPD a comienzos de 2010, orientará a los posibles interesados sobre cómo presentar una reclamación. También se espera que limite el número de reclamaciones que por razones obvias no puedan admitirse a trámite y que facilite al SEPD información más completa y pertinente que agilice la tramitación de las reclamaciones. Está previsto que pronto se disponga de una versión interactiva del formulario de reclamación que los usuarios podrán rellenar en pantalla y a continuación enviar automáticamente al SEPD.

# 2.5. Control del cumplimiento

*El SEPD tiene atribuida la función de garantizar y supervisar la aplicación del Reglamento (CE) nº 45/2001 (artículo 41, apartado 2, del Reglamento). La supervisión se ha efectuado principalmente mediante un ejercicio de notificación denominado «Primavera 2009», continuación a su vez de otra iniciativa similar («Primavera 2007») y revistió la forma de cartas dirigidas a los directores de las instituciones y organismos de la UE instándoles a actualizar los progresos realizados hasta la fecha en determinados ámbitos. Además de este ejercicio de control general, se llevaron a cabo inspecciones en determinadas instituciones y organismos con el fin de verificar el cumplimiento de determinadas materias.*

## 2.5.1. El ejercicio «Primavera 2009»

Como resultado del ejercicio, el SEPD emitió un segundo informe general en el que se cuantificaban los progresos alcanzados en la aplicación de las normas y principios de protección de datos por parte de las instituciones y organismos de la UE. El informe muestra que, en general, las instituciones de la UE han avanzado adecuadamente en el cumplimiento de los requisitos relativos a la protección de datos, mientras que en las agencias el nivel de cumplimiento de las agencias ha sido relativamente menor.

## Principales resultados de las agencias

**Principales resultados en las instituciones**

- **Inventario de las operaciones de tratamiento**: el SEPD está satisfecho de que todas las instituciones, salvo una, hayan elaborado un inventario de las operaciones de tratamiento de datos personales, lo que permite enfocar la aplicación desde una perspectiva más sistemática.
- **Notificación de operaciones de tratamiento por parte de los responsables del tratamiento de datos al RPD**: el SEPD constata un incremento del número de instituciones que han completado el proceso. A finales de 2008, al menos seis instituciones podían afirmar que todas las operaciones de tratamiento habían sido notificadas al RPD, cuando a principios de 2008, a modo de comparación, solo lo habían hecho dos instituciones.
- **Notificación de operaciones de tratamiento al SEPD para control previo**: hasta el momento solo dos instituciones han notificado al SEPD todas las operaciones de tratamiento relativas al control previo. Sin embargo, la mayor parte de las instituciones indicaron que a finales de 2009 se notificarán al SEPD todas las operaciones de tratamiento identificadas.

El SEPD constató que se habían alcanzado **resultados positivos** en la identificación de las operaciones de tratamiento y en la adopción de las modalidades de aplicación relativas a las tareas y obligaciones del RPD. No obstante, el nivel general de notificaciones de operaciones de tratamiento al RPD y notificaciones adicionales al SEPD para control previo fue por lo general muy escaso. Solo una agencia declaró que todas las operaciones identificadas habían sido notificadas al SEPD.

Pese a no haberse producido peticiones de acceso a datos en virtud del Reglamento, o en su caso muy pocas, al SEPD le satisfizo observar que las agencias están considerando la posibilidad de instaurar herramientas de control para efectuar el seguimiento de estas peticiones.

### Pasos adicionales

El SEPD fomentará y supervisará atentamente posteriores avances, especialmente en aquellas instituciones y agencias en las que es preciso mejorar el cumplimiento en el ámbito de las notificaciones de control previo al SEPD y al RPD. Se seguirá investigando en relación con el cumplimiento a fin de evaluar los nuevos avances.

## 2.5.2. Inspecciones

Las inspecciones son una herramienta fundamental que permite al SEPD supervisar y garantizar la aplicación del Reglamento, en cuyos artículos 41, apartado 2, 46, letra c), y 47, apartado 2, se basan.

Las amplias facultades de acceso a toda la información y datos personales necesarios para sus investigaciones y para acceder 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 herramientas suficientes para llevar a cabo su función. El SEPD puede iniciar las inspecciones a raíz de una reclamación o por iniciativa propia.

El artículo 30 del Reglamento insta a las instituciones y organismos de la UE a cooperen 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. A las inspecciones le siguen las reacciones adecuadas a la institución u organismo inspeccionados.

En 2009, el SEPD prosiguió las inspecciones anunciadas en el marco del ejercicio «Primavera 2007», especialmente en el Parlamento Europeo y en la EPSO, y llevó a cabo una inspección en el Tribunal de Cuentas Europeo. En julio de 2009, sobre la base de la experiencia acumulada durante las inspecciones, el SEPD adoptó un manual sobre procedimiento de inspección interno y publicó los elementos fundamentales de dicho procedimiento en su página web.

### Política y procedimiento de inspección del SEPD

El **manual de inspecciones del personal interno del SEPD** tiene por objetivo asesorar al personal del SEPD. El manual se basa esencialmente en el marco jurídico existente, los principios generales del Derecho de la UE y las buenas prácticas administrativas comunes a todas las instituciones y organismos de la UE.

El manual contiene información sobre el procedimiento administrativo, las tareas de los inspectores y la política de seguridad, así como formularios normalizados para la elaboración de los documentos de inspección. En él se explican los objetivos de estos documentos y se proporcionan consejos útiles para la preparación de una inspección.

El manual de inspección es un documento vivo, sujeto a revisiones regulares a medida que evolucionan las prácticas y experiencias del SEPD. A su debido tiempo se redactará un documento político sobre el papel de las inspecciones y sobre los criterios aplicados para acometer su realización.

### Inspección en el Parlamento Europeo

En febrero de 2009, el SEPD llevó a cabo una inspección en el Parlamento Europeo. La inspección tenía por objeto investigar los hechos relacionados con las operaciones de tratamiento de datos personales tanto de los servicios médicos de Bruselas como de los de Luxemburgo y del servicio de ausencias médicas, en relación con tres dictámenes de control previo emitidos por el SEPD. Un segundo objetivo era verificar la aplicación de las recomendaciones formuladas en tales dictámenes. La obligación de los responsables del tratamiento de datos de la Dirección General Políticas Externas de notificar al RPD las operaciones de tratamiento de datos personales en virtud del artículo 25 del Reglamento también formó parte de la inspección.

Como resultado de la inspección, el SEPD manifestó su inquietud en relación con una serie de deficiencias constatadas en el ámbito de la **seguridad de la información en los servicios médicos** (es decir, organizativa, física y técnica) y planteó la necesidad de introducir considerables mejoras. En particular, el SEPD instó a encontrar una solución adecuada para transferir los informes médicos del servicio de ausencias por enfermedad al servicio médico.

El SEPD remitió una lista de recomendaciones al Secretario General del Parlamento y le urgió a tomar las medidas adecuadas. Con posterioridad, varias de dichas medidas se han llevado a la práctica, pero el seguimiento de esta inspección continúa.

## Inspección en 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). La inspección tenía por objetivo investigar los hechos relativos a las operaciones de tratamiento de datos personales correspondientes a diversos controles previos en el ámbito de la selección de funcionarios, personal temporal y agentes contractuales, así como cualquier operación de tratamiento de datos personales relacionada.

La inspección reveló que la EPSO había realizado considerables **progresos en materia de transparencia** de sus procedimientos y de la información facilitada a los candidatos. No obstante, el SEPD reiteró en sus conclusiones la obligación de la EPSO de facilitar a los candidatos que las soliciten las hojas de evaluación elaboradas por el tribunal en el marco de los exámenes orales. Durante la inspección no se abordó la cuestión del acceso a las preguntas en las pruebas de respuesta múltiple, pues está pendiente ante el Tribunal.

Por lo que se refiere a la **política de conservación**, el SEPD reclamó un procedimiento documentado parar archivar los expedientes en los archivos históricos de la Comisión.

Otro objetivo de la inspección fue verificar el cumplimiento de la legislación en **determinadas bases de datos y herramientas informáticas de la EPSO** utilizadas en los procedimientos de selección. Por regla general, el SEPD solicitó que se documentaran las pautas de seguridad de carácter técnico y organizativo y que su integración en los procedimientos de competencia fuera más sistemática.

Las conclusiones de la inspección fueron remitidas al director de la EPSO, que ha adoptado un plan de acción para las recomendaciones formuladas por el SEPD. Dado que este plan de acción forma parte de un plan de mejora continua y que los procedimientos se encuentran en fase de revisión, el SEPD se ha reservado sus conclusiones finales hasta principios de 2010.

## Inspección en el Tribunal de Cuentas Europeo

En marzo de 2009, el SEPD procedió a inspeccionar en el Tribunal de Cuentas al **personal de control** (informe de la herramienta de control y auditoría).

EL SEPD acogió con satisfacción el uso por parte del Tribunal de Cuentas Europeo de **técnicas de filtrado** orientadas a disuadir del uso inadecuado de Internet mediante técnicas basadas en la prevención y no en la represión. Cabe destacar que el SEPD rechazó las características y funciones de los filtros de software utilizados para controlar los intentos fallidos de acceso a Internet y subrayó la importancia de las **evaluaciones de impacto en la privacidad** como herramienta utilizable en el proceso de selección del software con fines de control. El SEPD consideró asimismo como mejor práctica ampliar los principios de **intimidad mediante el diseño** a todo el proceso de diseño de los sistemas y los procesos de control de Internet y de red. El SEPD instó al Tribunal de Cuentas Europeo a mejorar las políticas destinadas a mantener un **elevado nivel de cumplimiento de la política de seguridad** con el fin de construir un procedimiento de control de Internet sólido, seguro, justo y respetuoso de las normas de protección de la intimidad y de los datos.

En cuanto al aspecto de la inspección relacionado con la consulta sobre un procedimiento de **acceso al disco y al correo electrónico privados de los miembros del personal**, el SEPD analizó las finalidades pertinentes y las prácticas actuales del Tribunal de Cuentas Europeo y concluyó que existía un riesgo de violar la confidencialidad de las comunicaciones. En consecuencia, el SEPD insistió en que se le presentara una notificación formal de control previo acerca de esta operación de tratamiento, ya que generaba un riesgo específico en virtud del artículo 27, apartado 1, del Reglamento.

## La inspección de s-TESTA

La red s-TESTA (Servicios Transeuropeos Seguros de Telemática entre Administraciones) ofrece una infraestructura general que atiende a las necesidades empresariales y de intercambio de información entre las administraciones nacionales y europeas. En la actualidad, más de treinta aplicaciones se basan en esta red segura que facilita la Comisión Europea.

En tanto que autoridad supervisora de los sistemas y aplicaciones de la Comisión Europea que tratan datos personales, en septiembre de 2009 el SEPD decidió llevar a cabo una inspección de la red s-TESTA, y más concretamente de su Centro de Servicios y Operativo, con sede en Bratislava. La Comisión Europea confió la gestión del Centro a un contratista, Orange Business Service/Hewlett

Packard (OBS/HP). El principal objetivo de la inspección era reunir información sobre las medidas de seguridad y de protección de datos aplicadas y compararla con los requisitos definidos en el contrato y en la normativa correspondiente. En este marco, el SEPD sometió a inspección la infraestructura, el personal, la organización y las tecnologías del Centro.

El SEPD consideró satisfactorias en líneas generales las medidas de seguridad introducidas por la Comisión Europea y aplicadas por OBS/HP en los sistemas de tecnologías de la información, las aplicaciones y los procesos organizativos del Centro. La puesta en marcha de diferentes actualizaciones de la seguridad y la ejecución de un plan de mejora continua reforzarán aún más el mecanismo de protección de datos.

## 2.6. Medidas administrativas

*El Reglamento (CE) nº 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 al respecto, bien a* ***petición*** *de la institución u organismo, bien por* ***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 o 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 cuestiones abstractas 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, entre las que cabe mencionar, por ejemplo:

- la transmisión de datos personales a terceros países;
- el tratamiento de datos personales en el marco de un procedimiento ligado a una pandemia;
- el ejercicio del derecho de acceso;
- la aplicación de las normas de protección de datos al Servicio de Auditoría Interna, y
- la aplicación de las normas del Reglamento (CE) nº 45/2001.

### 2.6.1. Transmisión de datos personales a terceros países

La **Oficina Europea de Lucha contra el Fraude** (OLAF) planteó la pregunta de si cabe considerar que tres grupos de países presentan un **nivel adecuado de protección de datos** a la luz de su relación con el Convenio 108 del Consejo de Europa y su Protocolo adicional.

La OLAF preguntó también si, en caso de considerarse que uno o más de dichos grupos no presentase un nivel adecuado de protección en el sentido del Reglamento de protección de datos (artículo 9, apartado 1), los compromisos que hubieran adquirido en el contexto del Convenio o de los acuerdos sobre asistencia administrativa mutua y en asuntos aduaneros se considerarían «garantías suficientes» (artículo 9, apartado 7) (asunto 2009-0333).

Tras analizar la consulta, el SEPD concluyó que **no había pruebas suficientes** de la aplicación satisfactoria del Convenio 108 y su Protocolo adicional en los países en cuestión. Por lo tanto, en principio no podía considerarse que en los tres grupos de países hubiese un nivel de protección adecuado.

El SEPD agregó que, no obstante, la OLAF podía considerar la posibilidad de evaluar si se podría efectuarse una transmisión (o un conjunto de transmisiones) determinada, limitada a determinados objetivos y receptores del país de destino que ofrecieran un nivel adecuado de protección. Dicha valoración implicaría una revisión de la legislación nacional por la que se aplican el Convenio y su Protocolo y su aplicación efectiva.

El SEPD mencionó asimismo que, como tercera vía de acción, la OLAF y los receptores podían introducir las garantías suficientes.

## 2.6.2. Tratamiento de datos personales en el marco de un procedimiento de pandemia

El SEPD recibió una consulta sobre el tratamiento de datos personales por el **Banco Central Europeo** (BCE) en caso de **pandemia** (asunto 2009-0456). Aparte del tratamiento de datos personales por los servicios médicos del BCE, la pandemia exigiría informar al personal directivo sobre los indicios de infección de una persona determinada, de manera que se pudiera alertar a los miembros pertinentes del equipo.

El SEPD consideró que, a falta de obligación jurídica nacional, el artículo 5, letra a), del Reglamento podía servir como base jurídica para el tratamiento de datos en el marco del procedimiento de pandemia. No obstante, por tratarse de un caso excepcional, convendría que el BCE adoptase una decisión formal en la que podría basarse cualquier comunicación elevada al personal directivo.

Por otra parte, el SEPD subrayó que, por centrarse en datos relacionados con la salud, el tratamiento estaba prohibido, a menos que pudieran encontrarse excepciones que cumpliesen el artículo 10. El tratamiento de los datos relacionados con la salud podría estar basado en una obligación impuesta por ley a los empresarios de cumplir con las obligaciones en materia de salud y de seguridad en el trabajo. El SEPD consideró también que, en este asunto, había «motivos de interés público importantes» que podían justificar este tratamiento de los datos de carácter sanitario, pero que podían establecerse garantías suficientes para proteger los intereses de los titulares de los datos.

## 2.6.3. Ejercicio del derecho de acceso

La **OLAF** consultó al SEPD sobre un caso hipotético relacionado principalmente con el ejercicio del **derecho de acceso** (asunto 2009-0550).

El SEPD consideró que, en principio, la solicitud de una lista de casos en los que apareciesen los datos personales de los titulares quedaría contemplada por el artículo 13, letra a), del Reglamento, dado es un modo de obtener «confirmación de la existencia o no de tratamiento de datos que le conciernan». El procedimiento para la concesión de la confirmación depende, hasta cierto punto, de la naturaleza y de las características de los datos y de la actividad de tratamiento en cuestión. También depende de si un modo determinado de conceder la confirmación permitiría wvo no al titular de los datos ejercer los diversos derechos a la protección de sus datos ([7]).

Para evaluar los métodos y parámetros de acceso debería adoptarse un planteamiento caso por caso. La información facilitada al titular de los datos debe ser comprensible («en forma inteligible») a la vez que debe explicitar qué actividad de tratamiento se está llevando a cabo y a qué datos afecta. El nivel de detalle debería permitir al titular de los datos evaluar la exactitud de la información y la legalidad del tratamiento, así como reflejar la carga que la tarea supone para el responsable del tratamiento.

## 2.6.4. Aplicación de las normas de protección de datos al Servicio de Auditoría Interna (SAI)

Con vistas a una próxima auditoría de la gestión de los recursos humanos en la Agencia Europea de Medicamentos (EMA), el director administrativo de esta entidad solicitó del SEPD que confirmase en el transcurso de la auditoría si el Reglamento es aplicable al equipo del SAI (asunto 2009-0097).

El SEPD consideró que el SAI es un órgano europeo que efectúa el tratamiento de datos personales en el marco del ejercicio de actividades incluidas dentro del ámbito de aplicación del Derecho de la UE, tal como resulte de aplicación en dicha fase, y, por lo tanto, si el SAI tuviese acceso a datos personales durante sus actividades de auditoría, serían aplicables las normas previstas en el Reglamento.

## 2.6.5. Modalidades de aplicación del Reglamento (CE) nº 45/2001

Diferentes RPD formularon consultas al SEPD respecto a los borradores relativos a la aplicación de las normas del Reglamento (CE) nº 45/2001 por parte de sus agencias. El SEPD observó que,

([7]) Véase el apartado 57, sentencia del TJE en el asunto C-553/07, *Rotterdam/Rijkeboer*.

además de abordar las tareas, obligaciones y poderes de los RPD (artículo 24, apartado 8, y anexo del Reglamento), todos los borradores cubrían el papel de los responsables del tratamiento y los derechos de los titulares de los datos. Varias recomendaciones de particular importancia formuladas por el SEPD fueron las referidas a las siguientes cuestiones:

- el RPD debería velar por la aplicación interna de las disposiciones del Reglamento de **manera independiente**, sin recibir instrucciones de nadie (asuntos 2009-0656 y 2009-0684);
- el RPD puede obtener **asistencia externa** siempre y cuando ello no comprometa su independencia (asunto 2009-0656);
- en caso necesario, la agencia deberá organizar **formación en protección de datos** (asunto 2009-0656);
- al personal que apoya al RPD se le debería imponer la misma obligación de **secreto profesional** que al RPD (asunto 2009-0684);
- el **Comité de Personal** también deberá estar capacitado para consultar al RPD, y en general este podrá ser consultado sin recurrir a los canales oficiales (asuntos 2009-0684, 2009-0204 y 2009-0163).

## 2.7. Orientaciones temáticas

*La experiencia reunida en la aplicación del Reglamento (CE) nº 45/2001 ha permitido al personal del SEPD traducir sus conocimientos en orientación genérica para las instituciones y organismos. En 2009 el SEPD desarrolló orientaciones sobre determinados temas en forma de documentos monográficos.*

### 2.7.1. Directrices sobre contratación

Las directrices del SEPD sobre el tratamiento de datos personales en relación con la contratación (adoptadas a finales de 2008) examinan el ciclo de procedimientos administrativos (selección, contratación y disposiciones contractuales) establecido para reclutar personal permanente, contractual y temporal, así como expertos nacionales y personal en prácticas.

Entre otras cosas, las directrices analizan la **recogida** por las instituciones de datos relativos a **condenas penales anteriores** con el fin de cumplir lo estipulado en el Estatuto de los funcionarios: solo se puede reclutar como miembro del personal a una persona si goza plenamente de los derechos de ciudadanía y puede ofrecer las garantías de moralidad requeridas para el ejercicio de sus funciones. El SEPD consideró que la recogida de datos


En el momento de contratar personal, las instituciones de la UE velarán por limitarse a recoger únicamente los datos pertinentes.

relacionados con condenas penales es legal. No obstante, subrayó que la manera de recogerlos (por medio de diferentes documentos, como registros de antecedentes penales o certificados de buena conducta) podía dar lugar a la recogida abusiva de información. De hecho, estos documentos pueden contener información que excede el propósito legítimo de verificar que la persona goza de la totalidad de sus derechos.

Por lo tanto, las directrices recomiendan que el análisis del contenido de tales documentos se lleve a cabo caso por caso, de modo que solo los datos pertinentes se sometan a tratamiento a la luz de los requisitos del Estatuto de los funcionarios.

En cuanto al **periodo de conservación** de los datos relacionados con condenas penales, las directrices insisten en la devolución del registro de antecedentes penales al interesado inmediatamente después de la selección y la posible contratación. Estos documentos tienen valor en el presente y pueden quedar obsoletos al día siguiente de su emisión. Con fines testimoniales y de auditoría, podría crearse un formulario normalizado que acreditase que la persona en cuestión es adecuada para el desempeño de sus funciones y goza de todos sus derechos de ciudadanía.

Las directrices analizan también las **transferencias externas** de datos, ya sea a empresas que organicen pruebas en nombre del comité de selección, ya a expertos externos reclutados como miembros del comité de selección. Debería establecerse la necesidad de dichas transferencias en virtud del artículo 8, letra a). Por otra parte, el mandato exacto de los contratistas externos deberá estipularse en un contrato o un acto jurídico, y sus obligaciones de confidencialidad y seguridad deberán garantizarse en virtud del artículo 23 del Reglamento.

## 2.7.2. Directrices acerca de los datos relativos a la salud

En septiembre de 2009, el SEPD emitió una serie de directrices sobre el tratamiento por parte de las instituciones y organismos de la UE de los datos relativos a la salud en el lugar de trabajo.

En estas directrices se examina la **base jurídica** para el tratamiento de los datos relativos a la salud por parte de las instituciones y organismos de la UE tal como se establece principalmente en el Estatuto de los funcionarios, y se determina para qué fines y bajo qué condiciones se pueden someter a tratamiento los datos relativos a la salud. Por ejemplo, el Estatuto de los funcionarios prevé el tratamiento de los datos sobre la salud en relación con un examen médico previo a la contratación, con el fin de determinar si el futuro miembro del personal se encuentra o no físicamente apto para ejercer sus funciones. En cambio, el Estatuto de los funcionarios no prevé que ese mismo examen médico previo a la contratación pueda servir también para fines preventivos. Dicho esto, el SEPD reconoce que los datos recogidos durante el examen médico podrían servir además para alertar a un futuro miembro del personal sobre alguna cuestión específica relativa a su salud y emplearse, consiguientemente, con fines preventivos. Sin embargo, ello no implica que se hayan de pedir datos adicionales con fines de prevención.

Las directrices aplican también el **principio de calidad de los datos**. Este principio presupone una evaluación de todos los cuestionarios médicos presentados a los miembros del personal con el fin de cerciorarse de que solo se recogen y se tratan los datos necesarios y pertinentes. Si se ofrece al titular de los datos la posibilidad de someterse a una prueba de VIH durante la visita médica, se debe especificar claramente que esta prueba no es obligatoria y que solo se puede realizar con el consentimiento explícito e informado del interesado. El principio de calidad de los datos induce también al SEPD a concluir que en caso de que un miembro del personal decida que el examen médico lo realice un profesional de su elección, los resultados de la visita solo se deberán comunicar a los servicios médicos de las instituciones con el consentimiento libre e informado del interesado.

## 2.7.3. Directrices sobre la videovigilancia

El 7 de julio de 2009, el SEPD publicó una versión de consulta de las Directrices sobre videovigilancia. Se invitó a todos los interesados a que presentasen su opinión al respecto por escrito, y el 30 de septiembre de 2009 se organizó un seminario en Bruselas en el que participaron casi cien responsables de la protección de datos, responsables de seguridad, especialistas en tecnologías de la videovigilancia y en tecnologías de la información y representantes de más de 40 instituciones y organismos de la UE.

El taller y el proceso de consulta consiguieron el doble objetivo de obtener información que ayudase a mejorar el proyecto de directrices y de

Giovanni Buttarelli, Supervisor Adjunto, en el Seminario del SEPD sobre videovigilancia en las instituciones y órganos de la UE (Bruselas, 30 de septiembre de 2009).

aumentar la cooperación para velar por el cumplimiento de los principios de protección de datos. La respuesta global al proyecto de directrices fue positiva. En un clima de creciente preocupación suscitada por el incremento continuo de los métodos de vigilancia, los participantes acogieron con satisfacción el hecho de que el proyecto de directrices aportara asesoramiento práctico a la hora de optar por el uso de equipos de videovigilancia y sobre el tratamiento más adecuado para las cuestiones relacionadas con la protección de datos.

## Objetivos de las Directrices sobre videovigilancia y principios fundamentales

La intención del SEPD era publicar estas Directrices a principios de 2010 con el doble objetivo de: i) contribuir a reducir y evitar el uso incontrolado de videovigilancia en los casos en los que no está injustificada, y ii) prestar asistencia a las instituciones en el uso responsable de la videovigilancia y en la creación de salvaguardias cuando dicho uso esté justificado.

*Temas clave abordados en las Directrices*
- *Cómo seleccionar, situar y configurar un sistema.*
- *Cuánto tiempo se deben conservar las grabaciones.*
- *Quién debe tener acceso a las imágenes.*
- *Qué medidas de seguridad se deben tomar para proteger los datos.*
- *Cómo informar al público.*
- *Cómo cumplir las condiciones de acceso.*

Las Directrices tienen por objeto alentar la toma de decisiones localizada basada en necesidades de seguridad localizadas, teniendo a la vez en cuenta las preocupaciones concretas de otros interesados, incluido el personal. También subrayan la obligación para las instituciones de rendir cuentas y recomiendan adoptar una política de videovigilancia, así como llevar a cabo auditorías periódicas para garantizar y demostrar el cumplimiento. Por último, animan a las instituciones a integrar la privacidad y la protección de los datos en la tecnología utilizada, así como en sus prácticas organizativas, siguiendo el principio de intimidad mediante el diseño.

## Necesidad y proporcionalidad

Las Directrices se basan en los principios de necesidad y proporcionalidad, que, a su vez, deberían dar lugar a una minimización de los datos, contribuyendo a frenar a frenar la proliferación incontrolada de cámaras de seguridad. Las decisiones relativas a si instalar o no cámaras y sobre cómo utilizarlas no deberán basarse únicamente en las necesidades de seguridad, sino que también deberán tener en cuenta los derechos fundamentales del individuo.

*Preguntas previas a la instalación de un sistema*
- *¿Qué beneficios presenta la videovigilancia?*
- *¿Está claramente especificado el propósito del sistema? ¿Es explícito y legítimo?*
- *¿Tiene la videovigilancia un motivo lícito?*
- *¿Se ha demostrado claramente la necesidad de la videovigilancia?*
- *¿Es el mejor modo de conseguir el fin que se pretende?*
- *¿Existen alternativas menos intrusivas?*
- *¿Quedan los efectos perjudiciales compensados por los beneficios?*

Dicho esto, la protección de datos no debería obstaculizar el desempeño de las tareas de los servicios de seguridad. Las necesidades de seguridad y la protección de datos se suelen presentar como intereses opuestos difíciles de conciliar. 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 vigilancia pueden satisfacer las necesidades de seguridad sin dejar de respetar la privacidad. La tecnología de la vigilancia se debería utilizar de manera específica, de modo que se minimice la recogida de datos no pertinentes. Ello no solo reduce las intrusiones en la privacidad, sino que también ayuda a garantizar un uso más específico y, en última instancia, más eficiente de la vigilancia para abordar un problema de seguridad. En conclusión, el SEPD considera necesario que se adopte un enfoque selectivo a la hora de utilizar los sistemas de vigilancia, de manera que el público no se vea sometido a limitaciones excesivas a resultas de las acciones de una minoría.

## Intimidad en la concepción y obligación de rendir cuentas

No se puede velar por el respeto a la intimidad y la protección de los datos limitándose a marcar casillas para indicar que se cumplen los requisitos establecidos. Siempre que sea posible se ha de adoptar un enfoque preventivo: la intimidad debe incorporarse en la concepción a los sistemas de tecnologías de la información y la comunicación (TIC) desde el principio. La protección de la intimidad en la concepción no abarca solo las soluciones de diseño y las técnicas de los sistemas de TIC, sino que también requiere prácticas organizativas responsables y respetuosas de la intimidad e infraestructuras físicas respetuosas de la intimidad. En el ámbito de la videovigilancia, los principios de la intimidad en la concepción pueden resultar especialmente útiles y pertinentes.

Los sistemas de videovigilancia con fines de seguridad y otros objetivos de vigilancia deberían atenerse siempre al principio de protección de la intimidad en la concepción, y los requisitos relativos a la protección de datos deberían formar parte integrante del desarrollo de cualquiera de estos sistemas. Los sistemas de tratamiento de datos se deben diseñar y seleccionar con el objetivo de minimizar la recogida y el uso de datos personales. Por otra parte, los diseñadores del sistema deben identificar las técnicas disponibles y obtener el mejor uso de las mismas. Por razones evidentes, conviene que las inquietudes suscitadas por la protección de datos sean abordadas desde una fase inicial: una vez instaurado un sistema, resulta más difícil adoptar soluciones respetuosas con la protección de datos, por ejemplo, para velar por la existencia de los niveles de seguridad necesarios, permitir diferentes niveles de acceso y garantizar una pista de auditoría fiable o los derechos de acceso de los titulares de los datos.

La obligación de rendir cuentas significa que la organización responsable (el responsable del tratamiento) debe ser capaz de demostrar el cumplimiento de sus obligaciones en materia de protección de datos. De este modo se fomenta la práctica de evaluaciones y auditorías del impacto de la protección de datos y de la intimidad, y el equilibrio en el cumplimiento de la intimidad pasa a depender, en lugar de las comprobaciones de las autoridades reguladoras, de las medidas proactivas adoptadas por los propios responsables del tratamiento. La necesidad de demostrar el cumplimiento a los interesados y a las autoridades reguladoras significa igualmente que la obligación de rendir cuentas conlleva una mayor transparencia, por ejemplo, al hacer pública la política de videovigilancia de una organización.

La vigilancia por videocámara debe utilizarse de manera responsable y con salvaguardias eficaces.

### Los sistemas normalizados frente al examen más exhaustivo

El objeto de las Directrices es proporcionar salvaguardias detalladas en materia de protección de datos para la mayoría de los sistemas estándar de videovigilancia utilizados con fines de seguridad comunes. Así pues, en la mayor parte de los casos no es necesario efectuar una evaluación más formal y profunda sobre el impacto de la protección de datos obtenidos a partir de la videovigilancia en una institución, introducir nuevas salvaguardias o presentar planes de vigilancia para el control previo por el SEPD: basta con seguir las Directrices y aplicarlas.

Sin embargo, cuando la vigilancia propuesta aumenta considerablemente la amenaza para los derechos fundamentales y los intereses legítimos de quienes están sometidos a vigilancia (en comparación con los sistemas estándar de videovigilancia y las salvaguardias descritas en las Directrices), conviene evaluar sus repercusiones sobre la protección de la intimidad y los datos antes de instalar y aplicar el sistema. El objetivo de la evaluación de impacto es determinar las repercusiones adicionales del sistema propuesto sobre la intimidad de los individuos y otros derechos fundamentales e identificar vías que permitan mitigar o evitar posibles efectos adversos. Estos sistemas están sujetos a control previo y el SEPD los someterá a un examen detenido.

*Examen detenido*
- *Control de los empleados y control de las diferentes oficinas.*
- *Vigilancia encubierta y uso de la videovigilancia en investigaciones.*
- *Control de manifestantes.*
- *Videovigilancia de alta tecnología o inteligente (por ejemplo, reconocimiento de rostros, vigilancia dinámica preventiva).*
- *Sistemas interconectados.*
- *Grabación de sonido y cámaras* talking CCTV.

## 2.8. Eurodac

Eurodac fue creado en virtud el Reglamento (CE) nº 2725/2000 (conocido como «Reglamento Eurodac») que, al igual que el Reglamento Dublín II, está en fase de revisión. Eurodac es una gran base de datos de impresiones dactilares de los solicitantes de asilo y los inmigrantes ilegales en la UE cuyo objeto es contribuir a la aplicación efectiva del Reglamento Dublín II relativo a la determinación del Estado responsable del examen de las solicitudes de asilo de las personas que buscan la protección internacional con arreglo a la Convención de Ginebra en la Unión Europea.

El SEPD se encarga de **supervisar el tratamiento de los datos personales en la base de datos central del sistema gestionado por la Comisión**

y de transmitir dichos datos a los Estados miembros. En el desempeño de esta función, el SEPD coopera estrechamente con las autoridades de protección de datos de los Estados miembros encargadas de supervisar el tratamiento de datos a escala nacional, así como la transmisión de esos datos a la unidad central. Los representantes de las autoridades de protección de datos y el SEPD se reúnen regularmente para discutir los problemas comunes relacionados con el funcionamiento del sistema.

Este **modelo de supervisión coordinada** constituye un ejemplo excelente de enfoque coordinado de la supervisión de la protección de datos (véase la sección 4.3).

Las actividades del SEPD en relación con Eurodac incluyen también tareas de consulta y asesoramiento en el contexto de la revisión de los Reglamentos Eurodac y Dublín que las instituciones de la UE están debatiendo actualmente. En febrero de 2009, el SEPD emitió dos dictámenes sobre este asunto (véase la sección 3.3.2).

# 3

# CONSULTA

## 3.1. Introducción: situación y algunas tendencias

El considerable número de actividades y eventos celebrados en 2009 contribuyó a que pudiera entreverse con más claridad la **perspectiva de un nuevo marco jurídico para la protección de datos**. Materializar dicha posibilidad será una de las prioridades del SEPD durante los próximos años.

A finales de 2008 se adoptó por primera vez en la UE un marco jurídico general para la protección de datos en el ámbito de la cooperación policial y judicial (Decisión marco 2008/977/JAI del Consejo). En 2009 se produjo un segundo gran avance en materia legislativa.

*La primera actualización del marco jurídico para la protección de datos, la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas, fue modificada por la Directiva 2009/136/CE el 25 de noviembre de 2009.*

Con todo, no se trata si no de los primeros pasos.

*La entrada en vigor del Tratado de Lisboa marca el comienzo de una nueva era en el ámbito de la protección de datos. El artículo 16 del TFUE no solo prevé el derecho individual del titular de los datos, sino que también obliga al Parlamento Europeo y al Consejo a establecer normas respecto de la protección de datos en todos los ámbitos del Derecho de la UE.*

En otras palabras, el Tratado contempla un marco jurídico integral respecto de la protección de datos aplicable tanto al sector privado como al sector público de los Estados miembros e igualmente a las instituciones y organismos de la UE.

**El Programa de Estocolmo:** Una Europa abierta y segura que sirva y proteja al ciudadano, como aprobó el Consejo Europeo en diciembre de 2009, significa que la Unión debe garantizar una estrategia integral respecto de la protección de datos dentro de la UE y en sus relaciones con otros países. En el dictamen del SEPD en relación con el Programa de Estocolmo se subrayó la necesidad de un nuevo marco legislativo que, entre otras cosas, sustituya a la Decisión marco 2008/977/JAI del Consejo.

*No obstante, el paso más importante en este sentido consiste en la consulta pública sobre el marco jurídico para el derecho fundamental a la protección de los datos personales, organizada por la Dirección General de Justicia, Libertad y Seguridad.*

Esta consulta pública debe ser entendida como un primer paso en el logro de un instrumento jurídico actualizado y exhaustivo en el ámbito de la protección de datos que refleja plenamente los cambios introducidos por el Tratado de Lisboa y que velará asimismo por la protección efectiva de los datos personales en la sociedad de la información.

La contribución conjunta del Grupo de trabajo del artículo 29 y el Grupo de trabajo sobre policía

y justicia sobre el futuro del derecho a la intimidad fue adoptada en diciembre de 2009 y contó con el pleno apoyo y aportaciones significativas del SEPD. Este documento es merecedor de seria consideración en tanto que asesoramiento atinado de la comunidad europea implicada en la protección de datos para el desarrollo del marco jurídico integral y actualizado al que se hizo referencia anteriormente.

**En el contexto global** es importante señalar que en la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada en Madrid en noviembre de 2009, se adoptó una resolución sobre las normas internacionales en materia de protección de datos. Respecto de la protección de datos transatlántica, se ha seguido avanzando hacia un acuerdo entre la UE y los EE.UU. en relación con el intercambio de datos personales para fines relacionados con la actuación policial.

*2009 puede caracterizarse también como el año en que el SEPD se implicó en dos ámbitos adicionales de la política de la UE en los que el tratamiento de los datos personales reviste la mayor importancia: las listas de terroristas y la fiscalidad.*

La política relacionada con las denominadas «listas de terroristas» se inscribe en la política exterior y de seguridad común de la UE, mientras que la fiscalidad es un ámbito relacionado por naturaleza con el tratamiento intensivo de datos personales y la cooperación administrativa, en particular en la lucha contra el fraude. La atención en otros dos ámbitos, la salud pública y el transporte, se intensificó. Por último, huelga decir que el SEPD siguió muy implicado en diferentes actividades de la Dirección General de Sociedad de la Información y Medio de Comunicación y de la Dirección General de Justicia, Libertad y Seguridad.

## 3.2. Marco normativo y prioridades

### 3.2.1. Aplicación de las directrices del SEPD en materia consultiva

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

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

Ocasionalmente el SEPD formula por escrito comentarios de alcance más limitado, con el fin de comunicar un mensaje político rápido y esencial o centrarse en uno o más aspectos técnicos.

El SEPD está presente en todas las fases del proceso político y legislativo y su capacidad de influencia descansa en un amplio abanico de instrumentos. Pese a que ello puede requerir un contacto estrecho con las instituciones de la UE, salvaguardar su independencia y respetar la posición de todas las demás instituciones implicadas es de capital importancia.

El contacto con la Comisión tiene lugar en las diferentes fases de la preparación de propuestas, y la intensidad varía en función del tema y también en función del enfoque adoptado por los servicios de la Comisión. Por ejemplo, en los proyectos a largo plazo, como los relativos a la justicia electrónica (e-Justice) o los debates sobre el marco de notificación de las infracciones de la seguridad, el SEPD ha contribuido en diferentes fases y de diferente manera.

De la misma forma, se han mantenido contactos en la fase de seguimiento, especialmente durante los debates y las negociaciones intensivas en el Parlamento o el Consejo que abocaron a modificaciones fundamentales de alguna propuesta de la Comisión. Como ejemplos de la participación intensiva del SEPD en 2009 en las diferentes fases cabe citar la revisión de la Directiva sobre la privacidad en las comunicaciones electrónicas y la modificación de la normativa relativa al acceso del público.

Como ya se ha comentado, en 2009 se concretó aún más la posibilidad de un nuevo marco normativo para la protección de datos y la cuestión se abordó a distintos niveles y en distintos foros en

([8]) Disponible en el sitio del SEPD en Internet, en el apartado Consulta.

red. El SEPD transmitió su mensaje por diferentes canales. Constituyeron hitos importantes el dictamen respecto al Programa de Estocolmo y el informe del Grupo de trabajo del artículo 29, pero otros dictámenes, como el relativo al acceso de los servicios de seguridad a Eurodac, así como discursos, contribuciones a conferencias y debates en el Parlamento Europeo, también merecen ser tenidos en consideración. Uno de los mensajes principales, a saber, que es necesario un marco integral, en el que tengan cabida la cooperación policial y judicial, también fue presentado por la Comisaria Reding como uno de sus objetivos principales.

### 3.2.2. Resultados de 2009

En 2009, se mantuvo el incremento continuo en el número de dictámenes consultivos. El SEPD emitió dieciséis dictámenes sobre un amplio abanico de temas.

Con estos dictámenes y el resto de los instrumentos utilizados para la intervención, el SEPD aplicó las prioridades para 2009, tal como se establece en el inventario publicado en diciembre de 2008. Los 16 dictámenes cubrieron diferentes ámbitos políticos de la UE.

El inventario correspondiente a 2009 definía tres ámbitos de atención principales, a saber: salud pública, libertad, seguridad y justicia, y sociedad de la información. La salud pública constituye un ámbito relativamente nuevo para el SEPD: en los dictámenes se desarrollaron posiciones generales sobre donación de órganos y farmacovigilancia. En el ámbito de la libertad, la seguridad y la justicia se prestó mucha atención a las evoluciones relativas a la gestión de las fronteras y a los sistemas de información a gran escala. El desarrollo de la sociedad de la información ocupó un puesto prioritario en la agenda y seguirá ocupándolo.

Retrospectivamente, aunque el SEPD se centró en las principales líneas de actuación del inventario correspondiente a 2009, los logros específicos del año no coincidieron exactamente con las intenciones del inventario. Ello es reflejo de la dinámica en este ámbito. No todas las cuestiones seleccionadas al principio del año resultaron ser las más pertinentes durante el ejercicio. Sin embargo, el SEPD no alteró fundamentalmente su orientación. Algunos planes anunciados a comienzos de 2009 darán resultados en 2010. A título de ejemplo, podemos citar un dictamen emitido a principios de 2010 sobre el acuerdo comercial de lucha contra la falsificación (ACTA).

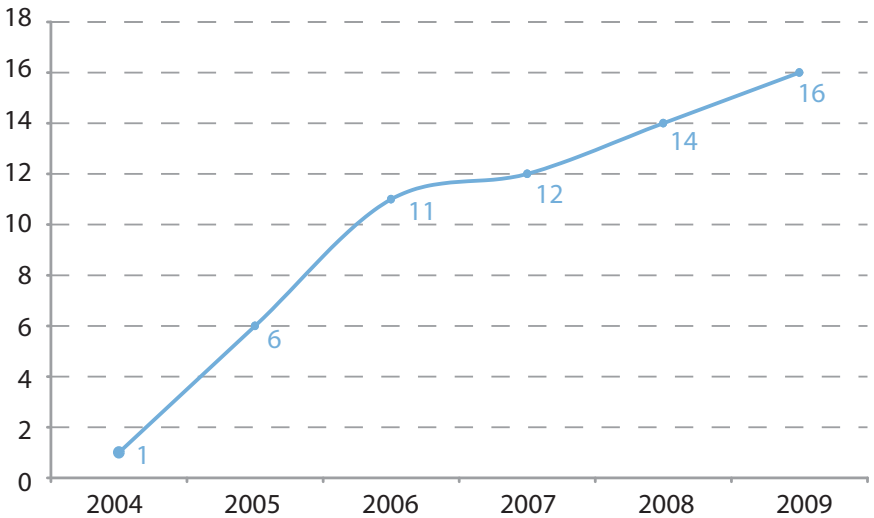
## 3.3. Espacio de libertad, seguridad y justicia

### 3.3.1. Evolución general

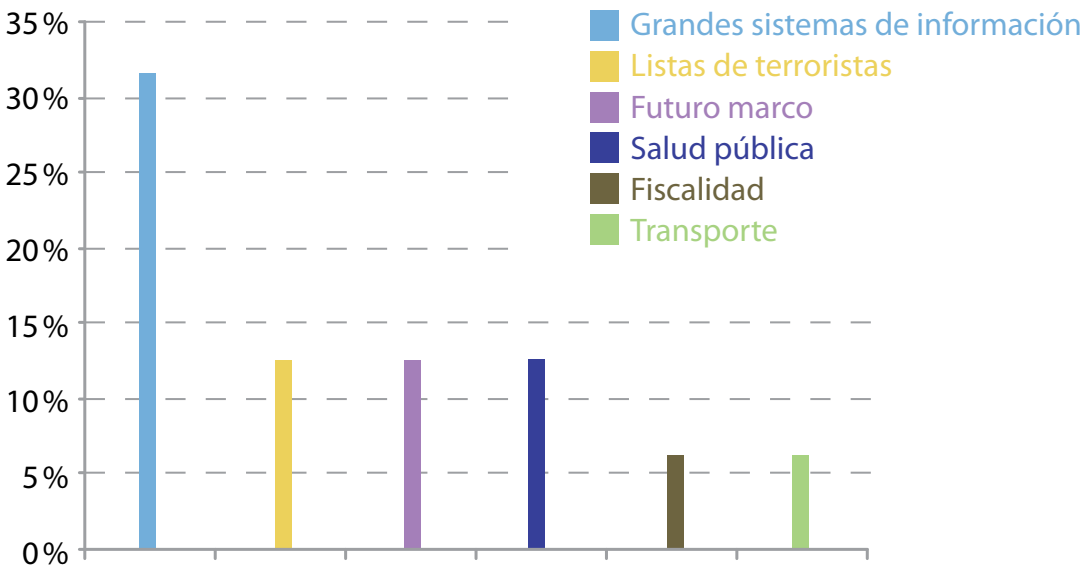
En 2009, el SEPD siguió con especial interés la evolución del **Programa de Estocolmo**, que planteó la visión de la UE en los próximos cinco años en el ámbito de la justicia y los asuntos de interior. El Programa de Estocolmo se debe considerar un paso más en la construcción de un espacio de libertad, seguridad y justicia en la Unión Europea.

En este ámbito, la cooperación entre los servicios de seguridad y, de un modo más general, entre los Estados miembros, así como entre estos y la UE,

Evolución de los dictámenes legislativos 2004-2009



Principales politicas cubiertas por dictámenes legislativos en 2009




depende en gran medida de la recogida y el intercambio de datos personales. Por consiguiente, resulta crucial proteger los datos personales de los ciudadanos en la cooperación policial y judicial, como el SEPD ha destacado en más de 30 dictámenes y comentarios sobre este asunto. El SEPD ha insistido siempre en que garantizar la protección de los datos personales no es solo una manera de proteger a los ciudadanos, sino también un modo de impulsar una actuación policial eficaz y la confianza mutua entre los servicios de seguridad de los diferentes Estados miembros.

El SEPD emitió un dictamen sobre la Comunicación de la Comisión de 10 de junio de 2009 y posteriormente participó de manera activa, mediante contribuciones y discursos ante las instituciones interesadas pertinentes, al debate que culminó con la adopción del programa en la reunión de diciembre del Consejo Europeo.

El SEPD apoyó la atención que el programa presta a la protección de los derechos fundamentales, y en particular a la protección de los datos personales. Por otra parte, el SEPD acoge con satisfacción


De acuerdo con el Programa de Estocolmo, la Unión Europea debe garantizar una estrategia integral de protección de datos dentro de la UE y en sus relaciones con otros países.

el llamamiento para la adopción de un régimen completo de protección de datos, que ahora cuenta con una base jurídica sólida en el Tratado de Lisboa.

*Un marco completo ayudaría también a abordar y regular más adecuadamente las tendencias recientes más significativas:*

- *el crecimiento **exponencial de la información digital** como resultado de la evolución de las tecnologías de la información y la comunicación;*
- *la **internacionalización** de los intercambios de datos personales;*
- *el **uso de datos comerciales** (por ejemplo, datos recogidos por empresas privadas, como operadores de telecomunicaciones, bancos, compañías aéreas, etc.) para la actuación de las fuerzas policiales.*

El SEPD hizo hincapié en que las instituciones deberían reflexionar en las consecuencias en los servicios de seguridad y los ciudadanos europeos antes de adoptar nuevos instrumentos de intercambio. Además, el SEPD destacó la importancia de desarrollar y promover normas internacionales sobre protección de datos, así como de velar por que la transmisión de datos personales a terceros países y organizaciones solo se realice cuando esté garantizada su adecuada protección.

El Programa de Estocolmo destaca el proyecto de un **Modelo Europeo de Información**, que constituye un esfuerzo reconocido por racionalizar y desarrollar una visión a largo plazo de la gestión y el intercambio de datos personales en los ámbitos de la justicia, la seguridad, el asilo y la inmigración.

El SEPD insistió en que esta visión a largo plazo podría resultar útil para construir intercambios de información más eficaces a la vez que se asegura un nivel elevado de protección de los datos personales. La introducción de la privacidad desde el primer momento en la arquitectura de los sistemas de información («intimidad mediante el diseño» o «intimidad por defecto») constituye un paso crucial en la aplicación de esta visión a largo plazo, pues ayudará a mejorar la calidad de la información y a evitar el exceso de información.

El SEPD debatió también sobre la **interoperabilidad** de los diferentes sistemas y bases de datos, que no se debería basar en la tecnología sino en opciones políticas claras y prudentes, además de respetar y garantizar las condiciones jurídicas necesarias para la recogida, el intercambio y el uso de los datos personales.

Los ciudadanos deben estar en condiciones de prever qué datos personales se recogen y con qué fines se usan. Esto es incluso más importante cuando se trata de categorías especiales de datos como las huellas dactilares y el ADN ([9]).

Las nuevas tecnologías se utilizarán también como herramienta para una **mejor cooperación judicial** en el llamado proyecto **e-Justicia** y otras iniciativas, para construir un espacio judicial europeo real. La interconexión de los registros nacionales, por ejemplo los de insolvencia, el uso de conferencias por videocámara en los procedimientos judiciales y el uso de portales de Internet para mejorar el acceso de los ciudadanos a la justicia son elementos de estas iniciativas que el SEPD acoge con satisfacción, siempre y cuando en su aplicación se tengan en cuenta los principios de la protección de datos. Algunas de estas herramientas se pueden utilizar también para facilitar una protección más eficaz y una aplicación más elemental de los derechos de protección de datos en toda Europa.

### 3.3.2. Eurodac y el Reglamento de Dublín

Debe prestarse especial **atención** a las cuestiones relacionadas con la privacidad y la protección de datos en el sistema de Dublín y Eurodac, el sistema de almacenamiento e intercambio a gran escala de huellas dactilares de solicitantes de asilo y otros grupos de inmigrantes (potenciales), que permite determinar cuál es el Estado miembro responsable de la tramitación de una solicitud de asilo. Las personas afectadas por este sistema se encuentran entre las **más vulnerables de la población** y se enfrentan con grandes dificultades para defender sus derechos.

La protección de los datos es también un **factor clave del éxito** para el funcionamiento de Eurodac, y por lo tanto, para el correcto funcionamiento del sistema de Dublín. Elementos como la seguridad de los datos, su calidad técnica y la legalidad de la consulta contribuyen, todos ellos, al correcto funcionamiento del sistema Eurodac.

El SEPD adoptó dos dictámenes interrelacionados relativos a la propuesta de revisión del denominado «Reglamento Eurodac» y a la propuesta de

([9]) Como se sigue también de las condiciones formuladas por el Tribunal Europeo de Derechos Humanos en el asunto S. y Marper, 4 de diciembre de 2008 (demandas nº 30562/04 y nº 30566/04).

refundir el Reglamento de Dublín, que determina cuál es el Estado miembro responsable de una solicitud de asilo.

Estas propuestas tienen por objetivo garantizar un mayor grado de armonización, más eficacia y mejores normas de protección para el sistema europeo común de asilo. Por otro lado, resultan de especial importancia para el SEPD, dado el papel que actualmente desempeña como autoridad supervisora de Eurodac.

En sus dictámenes, el SEPD apoyó los objetivos de la revisión y acogió con agrado la considerable atención deparada en ambas propuestas al respeto de los derechos fundamentales de los nacionales de terceros países y los apátridas. El SEPD formuló diversas observaciones relativas, *inter alia,* al respeto de los derechos del titular de los datos, la supervisión del sistema y los mecanismos de puesta en común de información.

La Comisión propuso que se permitiera asimismo el acceso al sistema Eurodac (cuya finalidad es facilitar la aplicación del Reglamento de Dublín mediante la comparación de las huellas dactilares de los solicitantes de asilo y los inmigrantes ilegales) a las fuerzas de seguridad responsables de la prevención, la detección y la investigación de los delitos de terrorismo y de otros delitos graves, en las condiciones establecidas en las propuestas.

El SEPD analizó las propuestas a la luz de su proporcionalidad y legitimidad, partiendo de la premisa de que es preciso guardar el equilibrio adecuado entre la necesidad de seguridad pública y el derecho fundamental a la intimidad y la protección de los datos, en cumplimiento de lo dispuesto en el artículo 8 del Convenio Europeo de Derechos Humanos (CEDH).

El análisis llevó a la conclusión de que la necesidad y la proporcionalidad de las propuestas, elementos cruciales ambos a la hora de legitimar la violación de la intimidad, no se había demostrado.

El SEPD recomendó evaluar la legitimidad de las propuestas en un contexto más amplio, en particular:

- la tendencia a conceder acceso a las fuerzas de seguridad a los datos personales de personas que no son sospechosas de ningún delito recogidos con otros fines;
- la necesidad de evaluar por separado cada propuesta de este tipo, y
- la necesidad de una visión coherente, integral y orientada al futuro, preferiblemente relacionada con el próximo programa marco quinquenal de justicia e interior («Programa de Estocolmo»).

### 3.3.3. Agencia para la Gestión Operativa de Sistemas Informáticos a gran Escala en el Ámbito de la Libertad, la Seguridad y la Justicia

La Comisión ha propuesto un paquete legislativo por el que se crea una Agencia para la Gestión Operativa de Sistemas Informáticos a gran Escala en el Ámbito de la Libertad, la Seguridad y la Justicia.

La Agencia sería la responsable de la gestión operativa del Sistema de Información de Schengen (SIS II), el Sistema de Información de Visados (VIS), Eurodac y quizás otros sistemas informáticos a gran escala.

Dado que todas estas bases de datos contienen **grandes cantidades de datos personales** (por ejemplo, detalles de pasaportes, visados y huellas dactilares), algunos de los cuales son de carácter confidencial, el SEPD orientó su análisis de la propuesta a garantizar que el instrumento legislativo aborde suficientemente el **impacto en la intimidad de las personas**.

El SEPD es consciente de las ventajas de la creación de una Agencia para la Gestión Operativa de Sistemas Informáticos a gran Escala en el Ámbito de la Libertad, la Seguridad y la Justicia, pero tal agencia solo se debería crear si su ámbito de actividad y responsabilidad se encuentra claramente definido.

La creación de una Agencia para la Gestión Operativa de Sistemas Informáticos a gran Escala en el Ámbito de la Libertad, la Seguridad y la Justicia debe basarse en una legislación que no presente ambigüedades en cuanto a sus competencias y su ámbito de actividad. Esta claridad evitaría futuros malentendidos acerca del funcionamiento de la agencia, y evitaría el riesgo de desviación de uso. La redacción actual de las propuestas no cumple estos requisitos.

### 3.3.4. Sistema de Información Aduanero (SIA)

Tanto un **enfoque coherente y global de los sistemas de tecnologías de la información a gran escala de la UE** como una **supervisión eficaz de la protección de datos** son elementos esenciales para el buen funcionamiento de estos sistemas. El nuevo marco jurídico que brinda el Tratado de Lisboa y la abolición de la estructura de pilares del Derecho de la UE deberían conferir una mayor **coherencia** entre los sistemas cuyo fundamento jurídico lo constituían anteriormente los pilares primero y tercero. También es necesaria una mayor colaboración entre los organismos de protección de datos que intervienen en la supervisión de los sistemas.

En este contexto, el SEPD emitió un dictamen sobre la iniciativa de la República Francesa relativa a la Decisión del Consejo sobre la utilización de la tecnología de la información a efectos aduaneros. En dicho dictamen, el SEPD insistió en la necesidad de garantizar la mayor coherencia posible entre ambas partes del SIA, es decir, la parte regida por el antiguo primer pilar y la regida por el antiguo tercer pilar. El SEPD pidió que en la propuesta se prestase más atención a las **salvaguardias específicas para la protección de datos**, especialmente en relación con la limitación de la finalidad para el uso de los datos introducidos en el SIA.

El SEPD pidió también que se introdujera en la propuesta un **modelo coordinado de supervisión** que en caso necesario garantizase la coherencia con el resto de los instrumentos jurídicos que dirigen la creación o el uso de los sistemas informáticos a gran escala, dado que este modelo se ha anticipado también para el Sistema de Información de Schengen (SIS II), el Sistema de Información de Visados (VIS).

El modelo de supervisión fue un tema importante en los debates del Consejo y del Parlamento Europeo. El SEPD invirtió mucho tiempo y energía en defender un modelo coordinado. Lamentablemente, el Consejo adoptó un texto que no refleja plenamente este modelo. Por otra parte, el texto da un mayor impulso a una cooperación estrecha entre el SEPD y las autoridades nacionales de protección de datos.

## 3.4. Protección de la intimidad y tecnología

### 3.4.1. El SEPD y la Directiva sobre la privacidad en las comunicaciones electrónicas

En 2009, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, conocida también como **Directiva sobre la privacidad en las comunicaciones electrónicas**, entró en las fases finales del proceso de revisión. La adopción final tuvo lugar el 25 de noviembre de 2009 ([10]). Sus nuevas disposiciones reforzaron la protección de la intimidad y de los datos personales de todos los ciudadanos europeos activos en el entorno electrónico. Entre las mejoras particularmente relevantes cabe señalar:

- La notificación obligatoria de los delitos respecto de los datos personales. Todo proveedor de servicios de comunicaciones electrónicas, como los proveedores de servicios de Internet, deben informar a los particulares sobre cualquier violación de los datos personales que pueda afectarles negativamente. Cabe citar como ejemplo aquellos casos en los que una pérdida de datos personales puede dar lugar a la usurpación de identidad, fraude, humillación o vulneración de la propia imagen.

- Nuevas normas sobre *cookies* y programas espía. En virtud de esta nueva disposición, debe ofrecerse a los usuarios mejor información y modos más sencillos de aceptar o rechazar los *cookies* que se instalan en sus terminales.

- Potenciación del derecho de actuar contra el correo basura *(spam)*, lo que se logrará brindando a toda persona negativamente afectada, incluidos los proveedores de servicios de Internet (PSI), la posibilidad de incoar

([10]) Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores, DO L 337, 18.12.2009.


Las comunicaciones electrónicas siempre dejan huellas de las personas.

procedimientos legales contra quienes lo envían.

- Disposiciones que refuerzan las competencias de actuación de las autoridades responsables de protección de datos.

A lo largo del proceso legislativo y hasta su adopción final, el SEPD ha colaborado en todo momento con los responsables políticos para asesorarlos y ayudarlos a definir las soluciones políticas adecuadas. El SEPD se sintió especialmente satisfecho con el marco final en materia de notificación obligatoria de los delitos contra la seguridad.

En su segundo dictamen legislativo, el SEPD asesoró, entre otras cosas, sobre las características principales del marco jurídico sobre notificación de las violaciones de la seguridad ([11]).

El SEPD acogió con satisfacción la amplitud de miras en la definición de violación de la seguridad, entendiendo por tal cualquier violación que provoque la destrucción, la pérdida, la difusión, etc., de datos personales transmitidos, almacenados o tratados de otro modo en relación con el servicio. Como causa de la notificación sugirió que fuera obligatoria la notificación a los particulares cuando la violación pueda incidir negativamente en los datos personales o la intimidad del titular. El SEPD razonó por qué esta norma era preferible a otras propuestas y se mostró satisfecho de que se hubieran tenido en cuenta sus preferencias. También acogió favorablemente la decisión de responsabilizar a las entidades afectadas de la evaluación de si la violación cumple o no con la condición desencadenante.

Desgraciadamente, el legislador no siguió la recomendación del SEPD en el sentido de que esta disposición fuese aplicable a todos los responsables del tratamiento de datos, sino que la limitó a los servicios de comunicaciones electrónicas, como empresas de telecomunicación, proveedores de servicios en Internet, proveedores de correo electrónico, etc.

Esta limitación del ámbito de aplicación provocó un acalorado debate entre el Parlamento Europeo, partidario de ampliar considerablemente dicho ámbito, y el Consejo y la Comisión, que se inclinaban por un ámbito más reducido. Aunque el resultado final no es satisfactorio, el debate movió a la Comisión a manifestar su intención de imponer este régimen a todos los responsables del tratamiento de datos en un futuro próximo.

La Directiva sobre la privacidad en las comunicaciones electrónicas revisada capacita a la Comisión, en consulta con las partes interesadas y el SEPD, a adoptar medidas técnicas de aplicación, es decir, medidas detalladas sobre la notificación de las violaciones de la seguridad, mediante el procedimiento de comitología. De este modo se garantizará una implementación y una aplicación coherentes en toda la UE del marco jurídico relativo a las violaciones de la

([11]) Segundodictamen del Supervisor Europeo de Protección de Datos, de 9 de enero de 2009, sobre la revisión de la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), DO C 128, 6.6.2009, p. 28.

seguridad, de manera que los ciudadanos gocen de un nivel de protección uniformemente elevado y los proveedores de servicios no se vean abrumados por unos requisitos de notificación divergentes.

El SEPD organizó dos actos con el fin de compartir experiencias y mejores prácticas. Iniciativas de este tipo deberían ser útiles en el futuro procedimiento de comitología. El primero de dichos actos tuvo lugar en abril de 2009 y fue organizado en el marco de la Iniciativa de Londres para las autoridades de protección de datos exclusivamente; el segundo, que contó con un público integrado por un amplio abanico de interesados, se celebró en octubre de 2009 y fue organizado conjuntamente con la Agencia Europea de Seguridad de las Redes y de la Información (ENISA).

La Directiva sobre la privacidad en las comunicaciones electrónicas se adoptó junto con otras Directivas; para todas ellas se suele utilizar la denominación colectiva de **paquete de telecomunicaciones**.

Las disposiciones sobre los sistemas de respuesta graduada o el denominado «enfoque de los tres avisos», incluidas en la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios, plantearon cuestiones en relación con la protección de datos y la privacidad. El SEPD las abordó en sus Comentarios de 16 de febrero de 2009, en los que se reafirmaba en su opinión contra la vigilancia sistemática y proactiva de los usuarios de Internet que respetan las leyes para luchar contra supuestas violaciones de los derechos de autor.

### 3.4.2. Sistemas de transporte inteligentes

El SEPD ha prestado especial atención a las innovaciones en el ámbito del transporte. En Europa están actualmente en fase de despliegue los denominados «sistemas de transporte inteligentes» (STI), cuyo objetivo es reducir la saturación del tráfico y contribuir a un transporte más seguro y respetuoso con el medio ambiente. Los sistemas se basan por lo general en tecnologías de posicionamiento, como la localización por satélite y la RFID (identificación por radiofrecuencia). El despliegue de los STI en Europa tiene repercusiones importantes sobre la intimidad, principalmente porque permite rastrear un vehículo y recopilar una considerable cantidad de datos relativos a las pautas de conducción de los usuarios viales europeos.

Los «sistemas de transporte inteligentes» aplican las tecnologías de la información y la comunicación (como satélites, ordenadores, teléfonos, etc.) a las infraestructuras de transportes y los vehículos. El sistema de llamadas de emergencia «e-Call» y el sistema de peajes electrónicos «e-Toll» son ejemplos de sistemas de transporte inteligentes.

Como comentario a un plan de acción de la Comisión para acelerar y coordinar el despliegue de los STI en Europa, el SEPD insistió en la necesidad de abordar detenidamente las cuestiones relacionadas con la intimidad y la protección de datos a fin de garantizar la viabilidad de los STI en toda Europa.

Por otra parte, advirtió a la Comisión sobre los riesgos de incoherencia y fragmentación que pueden derivarse de dicho despliegue si no se armonizan aún más ciertas cuestiones a escala de la UE:

- Es necesario especificar si los servicios STI se prestarán voluntaria u obligatoriamente y, de ser así, cuáles.
- Es crucial especificar las funciones de las diferentes partes que intervienen en los STI, con el fin de identificar quiénes se responsabilizarán de garantizar el funcionamiento adecuado de los sistemas desde la perspectiva de la protección de datos (es decir, ¿quién es el responsable del tratamiento de datos?).
- Los responsables del tratamiento de datos que presten servicios de STI deberán aplicar garantías suficientes para que el uso de las tecnologías de posicionamiento no suponga una intrusión en la intimidad. El uso de dispositivos de posicionamiento debería limitarse a lo estrictamente necesario para los fines previstos. Se debería velar por que los datos de localización no se revelen a receptores no autorizados.
- La intimidad y la protección de datos deberán tenerse en cuenta desde una fase inicial del diseño de la arquitectura del STI, el funcionamiento y la gestión de los sistemas (intimidad en la concepción).
- Los responsables del tratamiento de datos deben garantizar que se informa debidamente a los usuarios sobre la finalidad del tratamiento de los datos y del modo en que este se desarrolla.

La moderna tecnología permite un seguimiento permanente de los movimientos de los conductores.

### 3.4.3. Aplicación de la Directiva sobre conservación de datos

La Directiva 2006/24/CE sobre conservación de datos es un instrumento para la lucha contra el terrorismo y otros delitos graves que obliga a los proveedores de servicios y redes de telecomunicaciones a conservar los datos relativos al tráfico de las comunicaciones electrónicas. Se adoptó hace pocos años en un contexto de intensa presión política y plantea numerosas incertidumbres que complican su aplicación.

En este marco, se instituyó un grupo de expertos que agrupaba los intereses de los servicios de seguridad, la industria y los titulares de los datos y cuya principal misión consistía en prestar asesoramiento: por ejemplo, en lo relativo a qué proveedores les es aplicable la Directiva, dado el complejo entorno de los servicios de correo web, a qué proveedores de tránsito, a qué redes de terceros, etc. El SEPD participó activamente en este grupo e insistió en que la orientación se adaptase siempre a los principios de la legislación sobre protección de datos.

En este contexto se planteó una cuestión interesante y con no fácil respuesta: qué legislación es aplicable en aquellos casos en los que en la comunicación participa más de un Estado miembro, como sucede, por ejemplo, en las comunicaciones internacionales por móvil o en las comunicaciones transfronterizas por Internet. Y la complejidad de la cuestión aumenta cuando el proveedor almacena los datos conservados en un Estado miembro diferente de aquel en el que se generaron. El grupo tiene previsto publicar sus conclusiones en 2010.

### 3.4.4. Identificación por radiofrecuencia (RFID)

En mayo de 2009, la Comisión Europea adoptó una recomendación sobre la aplicación de los principios relativos a la protección de datos y la intimidad en las aplicaciones apoyadas en la identificación por radiofrecuencia ([12]). Mientras preparaba la recomendación, la Comisión consultó con frecuencia al SEPD, la mayor parte de cuyos comentarios se incorporaron en el documento.

Posteriormente, la Comisión Europea creó un grupo de trabajo informal sobre la aplicación de la recomendación relativa a la RFID y un representante del Grupo de trabajo del artículo 29 (G 29) asistió a las dos reuniones del grupo en 2009. Los temas abordados por el grupo incluían la necesidad de una evaluación del impacto en la privacidad y la protección de datos. De conformidad con el punto 4 de la

([12]) Recomendación de la Comisión C(2009) 3200 final, de 12 de mayo de 2009, disponible en: http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

recomendación, se presentará al G 29 un marco para la evaluación del impacto y se le pedirá que lo respalde.

### 3.4.5. Participación en el Séptimo Programa Marco de Investigación

#### Riseptis

El SEPD se reunió con el Grupo consultivo Riseptis (investigación e innovación para la seguridad, la intimidad y la fiabilidad en la sociedad de la información) ([13]) en calidad de observador. Este grupo asesor de alto nivel creado por la Comisión Europea y compuesto por destacados científicos, industriales y políticos tiene por objeto proporcionar asesoramiento guiado por una visión de futuro en relación con los retos que a nivel político y de investigación se plantean en el ámbito de la seguridad y la confianza en la sociedad de la información. El SEPD desempeñó un papel activo en las reuniones de Riseptis celebradas en 2009 y brindó asesoramiento político específico, especialmente en relación con el Derecho aplicable a las tecnologías futuras y emergentes, el principio de responsabilidad y el concepto de intimidad en la concepción.

El informe de Riseptis, bajo el título «Confianza en la sociedad de la información» y publicado en octubre de 2009, formula recomendaciones para abordar diferentes cuestiones a medida que la UE evoluciona hacia la era digital.

Estas recomendaciones incluyen:

- investigación interdisciplinaria, desarrollo y despliegue tecnológicos;
- iniciativas para agrupar a los interesados de los ámbitos tecnológico, político, jurídico y socioeconómico con el fin de que colaboren en la creación de una sociedad de la información basada en la fiabilidad;
- un marco común en la UE para la gestión de la identidad y la autenticación;
- un mayor desarrollo del marco jurídico de la UE para la protección de datos y la privacidad;
- actividades a gran escala en las que participen los sectores público y privado que se beneficien de los puntos fuertes de Europa en materia de comunicación, investigación, jurisprudencia y valores compartidos a nivel social;
- cooperación a escala global para promover estándares abiertos y marcos federados.

#### Proyectos de investigación y desarrollo tecnológico (IDT) de la UE

Tras la publicación de su documento de orientaciones de mayo de 2008, el SEPD prestó apoyo específico y proporcionó información para una serie de proyectos de investigación y desarrollo tecnológico (IDT) de la UE en distintos ámbitos, como los sistemas de transporte inteligentes, biométrica, sistemas de control remoto y la sanidad electrónica.

## 3.5. Globalización

### 3.5.1. Participación en normas internacionales

Muchos interlocutores, entendiendo entre otros la sociedad civil y la industria, defienden un marco armonizado de protección de datos trasfronterizo, capaz de garantizar la seguridad jurídica y de facilitar los flujos de datos en un contexto internacional. En la Conferencia Internacional de Protección de Datos celebrada en Madrid en noviembre de 2009 se dieron pasos concretos hacia el desarrollo de estándares internacionales de protección de datos. La Conferencia adoptó una resolución favorable al proyecto de normas internacionales sobre protección de datos personales y privacidad. Estas normas constituyen el primer paso hacia el logro de un instrumento internacional vinculante. Son el resultado de un intenso trabajo preparatorio dirigido por la autoridad española de protección de datos en el que el SEPD también participó activamente.

([13]) Véase el sitio de Internet: http://www.think-trust.eu/riseptis.html

Los estándares recogen los principios básicos de la protección de datos y, aunque en gran parte se inspiran en gran medida en la Directiva europea sobre protección de datos, tienen también en cuenta otros enfoques del tema ([14]).

El cumplimiento de los principios de equidad, necesidad, proporcionalidad y transparencia viene complementado con la obligación de rendir cuentas de los responsables del tratamiento de datos, así como con la necesidad de integrar la intimidad en la concepción. El proyecto de normas confiere igualmente a los titulares de los datos derechos de acceso y rectificación y de recurso judicial y administrativo.

## 3.5.2. El registro de nombres de pasajeros y el diálogo transatlántico

Las cuestiones relacionadas con la protección de datos constituyen una de las prioridades de la agenda de conversaciones entre la UE y los EE.UU.

Otro aspecto de la globalización es el diálogo transatlántico entre la Unión Europea y los Estados Unidos con el fin de facilitar el intercambio de datos personales. La mayoría de las transferencias de datos se realizan con fines de lucha contra el terrorismo y la delincuencia grave, como pone de relieve el acuerdo sobre la transferencia de datos de los pasajeros al Departamento de Seguridad Interior de los Estados Unidos (Decisión del Consejo de 23 de julio de 2007). Tanto el Grupo de trabajo del artículo 29 como el SEPD han mostrado su preocupación por las condiciones en que se produce la recopilación, tratamiento y salvaguardia de los datos de los pasajeros ([15]). En 2009, un subgrupo del G 29 en el que participa el SEPD supervisó la aplicación de este acuerdo respecto al registro de nombres de pasajeros (PNR) y planteó diversas cuestiones, entre las que cabe destacar el amplio acceso concedido a la Administración de los EE.UU. a los datos tratados por sistemas de reserva informatizados y la falta de revisión del sistema por parte de las autoridades europeas.

En un contexto más amplio, la UE y los EE.UU. están negociando la conclusión de un acuerdo sobre el intercambio de información en el ámbito más general de la actuación policial. Las negociaciones han dado lugar a diversos informes del llamado «Grupo de contacto de alto nivel», sobre los que el SEPD ha emitido un dictamen ([16]). En 2009 los debates giraron en torno a cuestiones concretas en las que las partes no habían alcanzado un acuerdo pleno, y en particular al derecho de las personas al recurso administrativo *y* judicial. Las partes pretenden seguir avanzando hacia el acuerdo a lo largo de 2010. El SEPD participó en la consulta sobre el acuerdo, organizada por la Comisión.

## 3.5.3. SWIFT: transferencia de datos financieros a las autoridades de los EE.UU.

El SEPD siguió de cerca la evolución de la transferencia de datos sobre transacciones financieras europeas al Tesoro de Estados Unidos con fines de lucha contra el terrorismo y la financiación del terrorismo. Este es un claro ejemplo de datos personales recogidos por sociedades comerciales que se utilizan para fines de actuación policial global.

Cuando la SWIFT (sociedad de telecomunicaciones financieras interbancarias mundiales), que es el principal soporte de datos financieros, modificó su arquitectura a fin de mantener los datos financieros europeos en territorio europeo, la Comisión Europea empezó a negociar un acuerdo internacional con las autoridades de Estados Unidos con objeto de evitar que se interrumpiese su acceso a estos datos. Se consultó al SEPD, quien emitió algunos comentarios que se enviaron a las instituciones pertinentes y se presentaron a la Comisión de

([14]) Como el enfoque de los países de la Organización de Cooperación y Desarrollo Económicos (OCDE) y del Foro de Cooperación Económica Asia-Pacífico (APEC), que es ligeramente diferente del de la UE.

([15]) Véase el Informe Anual 2008 del SEPD.

([16]) Dictamen de 11 de noviembre de 2008 acerca del Informe final del grupo de contacto de alto nivel entre la UE y Estados Unidos sobre el intercambio de información y la protección de la vida privada y los datos personales, DO C 128, 6.6.2009, p. 1.

El acceso de las autoridades públicas a las transacciones de datos bancarios deberá estar sometida a condiciones estrictas.

Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo en septiembre de 2009.

*En opinión del SEPD, un acuerdo internacional debería garantizar que:*

- *las solicitudes de transferencias de datos son legales y proporcionadas, especialmente teniendo en cuenta que la propuesta supone intrusión en la intimidad;*
- *existen mecanismos de recurso que los ciudadanos europeos pueden utilizar eficazmente;*
- *el intercambio con otras autoridades nacionales y otros países es limitado;*
- *las autoridades de control de la protección de datos independientes pueden ejercer sus facultades de supervisión, incluida la revisión de la aplicación del acuerdo*

En noviembre de 2009 se firmó un acuerdo provisional, pero, en virtud de las nuevas normas del Tratado de Lisboa, el Parlamento Europeo retiró su consentimiento. En 2010 el SEPD seguirá asesorando a las instituciones de la UE para garantizar que se continúen aplicando las normas europeas de protección de los datos personales, en especial en relación con cualquier nuevo acuerdo que sustituya al acuerdo provisional.

## 3.5.4. Medidas restrictivas en relación con presuntos terroristas y ciertos terceros países

En dos dictámenes de 2009, el SEPD trató por primera vez las llamadas «listas negras de terroristas». Estos instrumentos jurídicos prevén la lucha contra el terrorismo o los abusos de los derechos humanos imponiendo medidas restrictivas, como el bloqueo de activos y las prohibiciones de viaje a las personas físicas y jurídicas sospechosas de asociación con organizaciones terroristas o ciertos gobiernos. La Comisión Europea publica y difunde listas negras de personas sujetas a estas medidas restrictivas.

En algunos casos, el Tribunal de Justicia europeo reiteró que todas las medidas de la UE, incluidas las que emanan de decisiones de las Naciones Unidas, deberían respetar los derechos fundamentales de la UE, y en particular el derecho de defensa y el derecho a ser oído. Cabe señalar que el Tribunal suprimió de la lista a algunas personas por desconocer las razones de su inclusión en ella o bien porque habían permanecido en ella varios años sin ser condenadas ni investigadas.

El SEPD acogió con satisfacción las propuestas más recientes de la Comisión dirigidas a mejorar el respeto de los derechos fundamentales y a reconocer


El SEPD se implicó por primera vez activamente en este delicado ámbito.

explícitamente la aplicabilidad del Reglamento (CE) nº 45/2001 a este delicado ámbito político. Recomendó que:

- se garantice la calidad de los datos teniendo en cuenta los resultados pertinentes de las investigaciones policiales y de seguridad en las que se basan las listas y sometiendo estas a revisiones regulares;
- se facilite a las personas incluidas en las listas información adecuada y se les dé derecho a acceder a los datos personales que les conciernen;
- las restricciones y limitaciones necesarias de estos derechos se recojan claramente en la legislación, se prevean y sean proporcionadas;
- se garanticen los recursos judiciales, la responsabilidad civil y una indemnización adecuada en caso de tratamiento ilegal de datos personales.

*El SEPD seguirá atento a la evolución de estas cuestiones como asesor de las instituciones de la UE y como supervisor del tratamiento de estas listas negras, lo cual fue notificado para control previo por la Comisión Europea a finales de 2009.*

## 3.6. Salud pública

La UE ha establecido un ambicioso programa para mejorar la salud de los ciudadanos en la sociedad de la información y ve grandes posibilidades de mejorar la atención sanitaria transfronteriza con el uso de la tecnología de la información. Sin embargo, es evidente que la mejora de la atención sanitaria transfronteriza con el uso de la tecnología de la información tiene importantes consecuencias en la protección de los datos personales.

Desde 2008, la Comisión ha adoptado o propuesto iniciativas concretas en este ámbito. La Comisión ha publicado una Comunicación sobre telemedicina y una recomendación sobre la interoperabilidad transfronteriza de los sistemas de historiales médicos electrónicos. Además, ha mejorado el sistema de alerta y respuesta rápidas en relación con las enfermedades transmisibles y ha propuesto legislación sobre los derechos de los pacientes en materia de atención sanitaria transfronteriza, trasplante de órganos y farmacovigilancia (detección y análisis de los efectos adversos de los medicamentos).

El SEPD se mostró preocupado por que, a la hora de la verdad, la mayor parte de estos textos no aporten nada a la protección de datos. La cuestión de la protección de datos se menciona y se hace referencia a la legislación sobre protección de datos

aplicable, pero no se proponen normas concretas que realmente garanticen el cumplimiento de los requisitos sobre protección de datos y velen por que los Estados miembros apliquen esas normas de manera sistemática. Al parecer, no existe una visión coherente de la protección de datos en el sector de la asistencia sanitaria.

En parte, ello se puede explicar por el desconocimiento de la protección de datos en el sector de la salud pública, como se refleja a escala de la UE en el desconocimiento en los departamentos responsables de la existencia del SEPD y la obligación de consultarlo. El ejemplo más destacado en este sentido fue la propuesta sobre farmacovigilancia, que apenas mencionaba la protección de datos y no se envió al SEPD para consulta.

*El SEPD insistió repetidamente en que los datos sobre la salud se consideran una categoría delicada de la información personal y en que en principio el tratamiento de estos datos está prohibido. Hay excepciones, por ejemplo cuando una persona se somete a una diagnosis médica, pero se han de aplicar de manera restrictiva.*

En el dictamen sobre la farmacovigilancia, el SEPD destacó el principio de necesidad y cuestionó la necesidad del tratamiento de datos personales en la base de datos europea centralizada EudraVigilance.

En el dictamen sobre el trasplante de órganos, el SEPD aclaró el concepto de «anonimización». Explicó que si se garantiza la trazabilidad de los órganos, lo que significa que siempre se puede identificar al donante, la información nunca se puede considerar anónima. Dado que las propuestas garantizaban la trazabilidad y el anonimato al mismo tiempo, se tenían que ajustar haciendo hincapié en la confidencialidad de la información en lugar de en su anonimato.

El SEPD ha insistido repetidamente en que las normas de protección de datos no se han establecido para obstruir una cooperación eficaz en el ámbito de la salud pública. Al contrario, las salvaguardias de la protección de datos resultan cruciales para mantener la confianza en la profesión médica y en los servicios sanitarios en general.

El Tribunal Europeo de Derechos Humanos ha declarado que «la protección de los datos personales, en concreto de los datos médicos, es de esencial importancia en el disfrute de un individuo del derecho al respeto de su vida privada y familiar, tal y como garantiza el artículo 8 del Convenio». Y: «Respetar la confidencialidad de los datos médicos es [...] crucial, no sólo respetar el sentido de la privacidad de un paciente, sino también, preservar su confidencialidad en la profesión médica y en los servicios de salud en general» ([17]).

([17]) Véase Tribunal Europeo de Derechos Humanos, 17 de julio de 2008, *I./Finlandia* (demanda nº 20511/08), apartado 38.

¿Deben tratarse los datos personales en la base de datos EuroVigilance?

El SEPD acogió con satisfacción las invitaciones de la Comisión de Medio Ambiente, Salud Pública y Seguridad Alimentaria del Parlamento Europeo que le permitieron explicar dos de sus dictámenes (sobre la asistencia sanitaria transfronteriza y el trasplante de órganos). También le satisfizo que sus sugerencias dieran lugar a diversas modificaciones que fueron adoptadas por el Parlamento Europeo, si bien de momento no se ha adoptado ninguno de los instrumentos propuestos.

La consulta de las propuestas relativas a la farmacovigilancia se combinó con un análisis sobre la base de una notificación de control previo del sistema por la Agencia Europea de Medicamentos (EMA). Lo mismo sucedió con el posterior desarrollo del sistema de alerta y respuesta rápidas por la Comisión y el Centro Europeo para la Prevención y el Control de las Enfermedades (ECDC) en relación con las enfermedades transmisibles. El SEPD aportó comentarios informales sobre la Decisión de la Comisión correspondiente e inició un análisis del sistema tras recibir una notificación para un control previo.

*Las actividades desarrolladas en el ámbito de la salud pública llevaron al SEPD a adoptar un enfoque integrado de sus funciones de consulta y supervisión.*

## 3.7. Acceso del público y datos personales

### 3.7.1. Introducción

La compleja relación entre las normas de la UE sobre el acceso del público a los documentos y la protección de los datos ha preocupado al SEPD durante varios años. En 2009, el SEPD participó en el debate sobre la modificación de la legislación de la UE sobre el acceso del público a los documentos e intervino en acciones judiciales sobre el tema, incluido el asunto *Bavarian Lager*. Por otra parte, el primer recurso interpuesto ante el Tribunal de Primera Instancia contra una decisión del SEPD en relación con una reclamación trataba de este tema.

### 3.7.2. Modificación de la legislación de la UE sobre el acceso del público a los documentos

Tras observar los debates en curso en el Parlamento Europeo relativos a la modificación de la legislación de la UE relativa al acceso del público a los documentos, el SEPD resumió las opiniones expresadas en su dictamen de 30 de junio de 2008 en comentarios breves. El SEPD destacó las consecuencias negativas de algunas de las modificaciones presentadas en el Parlamento en la relación entre ambos derechos. El SEPD observó con satisfacción que los resultados de las votaciones en la sesión plenaria reflejaban casi completamente su enfoque.

En un comunicado de prensa emitido tras la votación, el SEPD declaró que las modificaciones aportaban claridad y evitaban una aplicación demasiado celosa de las normas de protección de datos en este ámbito, y añadió que confirmaban que la protección de datos no obstaculiza la revelación pública de información personal en los casos en que la persona afectada no tiene una razón legítima para mantener los datos en secreto.

El SEPD ofreció una explicación oral de sus opiniones ante el Grupo de trabajo sobre información del Consejo. Pese a los esfuerzos de la Presidencia sueca por impulsar la modificación por medio del Consejo en el segundo semestre de 2009, el debate sobre la modificación se estancó a causa de un conflicto de procedimiento todavía no resuelto entre la Comisión y el Parlamento.

### 3.7.3. El recurso en el asunto Bavarian Lager

El asunto *Bavarian Lager* trataba de la negativa de la Comisión a revelar cinco nombres contenidos en un documento de la Comisión. El recurso de la Comisión contra la sentencia del Tribunal de Primera Instancia de 8 de noviembre de 2007 culminó en una vista el 16 de junio de 2009. Durante esa vista, el SEPD defendió que se confirmara la sentencia del Tribunal de Primera Instancia. Aunque, en su dictamen de 15 de octubre de 2009, la Abogada General Sharpston también desestimó el recurso de la Comisión, no compartía el razonamiento del Tribunal de Primera Instancia respaldado por el SEPD. Dado que las conclusiones de la Abogada General se basaban en un razonamiento que las

partes no discutían en absoluto, el SEPD y la Comisión pidieron al Tribunal de Primera Instancia que reabriera la fase oral.

### 3.7.4. Otras acciones judiciales sobre el acceso del público y la protección de datos

El asunto *Dennekamp*, de que conocía el Tribunal de Primera Instancia, trataba de la negativa del Parlamento a revelar documentos que mostraban qué diputados al Parlamento Europeo eran miembros del plan de pensiones complementario. Desde el punto de vista jurídico, este asunto se puede considerar una especificación del asunto *Bavarian Lager*. Por esta razón, el SEPD intervino en el asunto.

El primer caso contra una decisión del SEPD fue promovido por la Sra. Kitou el 3 de abril de 2009. La Sra. Kitou disentía de una decisión del SEPD en la que este concluía que las normas de protección de datos no supondrían obstáculo alguno para que la Comisión revelase públicamente si ella estaba trabajando en dicha institución en determinados momentos.

Ambos asuntos siguen pendientes en el momento de imprimir el presente Informe Anual.

Otros dos asuntos que también siguen pendientes son los promovidos por el Sr. Pachtitis contra la Comisión y la EPSO, los dos ante el Tribunal de Primera Instancia y el Tribunal de la Función Pública. El tema de estos asuntos difiere de los descritos más arriba, pues el solicitante deseaba acceder a sus *propios* datos personales, a lo cual se negó la Comisión basándose en la legislación de la UE sobre el acceso del público a los documentos. En los escritos procesales y durante la vista ante el Tribunal de la Función Pública, que tuvo lugar el 1 de diciembre de 2009, el SEPD afirmó que la petición de acceso se debería haber considerado a la luz de las normas de protección de datos y que la Comisión debería haber aplicado esas normas de manera proactiva.

En el debate sobre la modificación de las normas de la UE sobre el acceso del público a los documentos, el SEPD afirmó que esta obligación se debería incluir en el preámbulo del documento modificado. Tal sugerencia recibió el apoyo del Parlamento Europeo.

El SEPD trabaja en la compleja relación entre estos dos derechos fundamentales.

## 3.8. Otras cuestiones

### 3.8.1. Sistema de Información del Mercado Interior (IMI)

En 2009, el SEPD siguió participando activamente en el desarrollo del IMI, que posiblemente constituye el ejemplo más destacado de cooperación administrativa mediante la puesta en común de información, además de ser un instrumento para una mayor integración europea. El sistema IMI empezó a funcionar (al acabar 2009 se habían registrado para usarlo más de 4 500 autoridades competentes) y se tomaron muchas medidas para integrar salvaguardias de protección de datos en el sistema.

El SEPD se mostró satisfecho ante estos esfuerzos, si bien no dejó de destacar la importancia de un marco más completo para el funcionamiento del IMI, con el fin de aportar certidumbre jurídica y un nivel más elevado de protección de datos, a poder ser en forma de Reglamento del Parlamento y el Consejo.

### 3.8.2. Otros dictámenes

El SEPD emitió también otros dictámenes sobre cuestiones cuyo tema central no era la protección de datos, aunque siempre tenían alguna relación con el tratamiento de datos personales. Trataban de una propuesta de Directiva del Consejo que obligaría a los Estados miembros a mantener un mínimo de reservas de petróleo crudo y/o productos petrolíferos, una propuesta de Reglamento del Consejo por el que se establecería un régimen comunitario de control para garantizar el cumplimiento de las normas de la política pesquera común, y una recomendación de Reglamento del Consejo sobre la obtención de información estadística por el Banco Central Europeo.

La sociedad de la información se entrelaza absolutamente con el universo físico de las personas.

## 3.9. ¿Qué nos depara el futuro?

### 3.9.1. Novedades tecnológicas

Como se menciona en el Informe Anual 2007 del SEPD, la sociedad de la información ya no puede considerarse un entorno paralelo y virtual, sino cada vez más un espacio complejo e interactivo entrelazado con el mundo físico de las personas. La convergencia entre estos dos universos se ve facilitada por el número cada vez mayor de puentes creados por el uso innovador de las tecnologías existentes y el desarrollo de tecnologías nuevas y emergentes. Esta tendencia es natural y positiva y acabará por dar paso a una integración plena en la que la sociedad de la información será simplemente parte de la sociedad.

No obstante, la proliferación de estos puentes tiende a desdibujar las fronteras entre entornos que en la actualidad no pueden ser gobernados por el mismo marco jurídico, y por lo tanto crea una incertidumbre jurídica que puede socavar la confianza y perjudicar al desarrollo de la sociedad de la información.

Los ejemplos siguientes ilustran algunos de estos puentes.

- ***CCTV (cámaras de televisión en circuito cerrado) inteligentes****: estos sistemas se suelen utilizar para investigar incidentes ocurridos en el pasado y para la posterior persecución de los delitos relacionados. Junto con el software de reconocimiento de rostros y unido a bases de datos públicas o privadas como las redes sociales, las secuencias de CCTV filmadas en tiempo real (el mundo real) se pueden enriquecer con datos en línea adicionales (el mundo digital).*
- ***Internet de los objetos****: este concepto general se define en la Comunicación de la Comisión ([18]) publicada en junio de 2009. Se trata de redes de objetos etiquetados interconectados que establecerán enlaces entre la naturaleza física de tales objetos (por ejemplo, localización, situación, actividades, comportamiento, propiedad) y la información en línea relacionada con ellos, que se facilita continuamente mediante una red de sensores. En este nuevo entorno, el prolongado ciclo de vida de algunos objetos etiquetados (por ejemplo, neumáticos, vidrios) consolidará los vínculos que con el tiempo irán facilitando una información cada vez más precisa tanto sobre los objetos como sobre sus propietarios.*

([18]) «Internet de los objetos: un plan de acción para Europa», COM(2009) 278 final, 18 de junio de 2009 (http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf)

- ***El frigorífico inteligente**: este manido ejemplo relaciona el hogar y los electrodomésticos con los proveedores en línea. Aunque se considera inaceptable realizar un control proactivo del uso del frigorífico en el hogar, el tratamiento de los datos generados por el propio frigorífico y comunicados a los proveedores en línea se puede regir por diferentes legislaciones aplicables.*
- ***Publicidad adaptada al comportamiento en línea**: el tratamiento y la correlación de una amplia variedad de datos relacionados con el comportamiento en línea de las personas produce perfiles precisos que se pueden utilizar para adaptar los anuncios a cada persona. Los navegadores y/o los nuevos dispositivos de comunicación proporcionan datos de localización y patrones de movimiento asociados a otros dispositivos, objetos, personas, tiendas, etc., que, sumados a los datos sobre el comportamiento en línea, pueden ayudar a completar los perfiles de usuario.*

La convergencia de estos dos mundos en un espacio para la persona está creando, sin lugar a dudas, nuevos retos en el marco jurídico de la privacidad y la protección de datos en la UE. Naturalmente, el objetivo es conciliar de una manera clara los entornos en línea y fuera de línea bajo una única estructura armonizada, o al menos mejorar la interoperabilidad entre ellos, con el fin de no poner en peligro la confianza en esta prometedora edad digital.

## 3.9.2. Progresos en materia de política y legislación

Mientras se imprime este Informe Anual se están produciendo (o se han producido) importantes progresos que determinarán el contexto de la política y la legislación en 2010.

Resulta obvio que estos progresos serán más tangibles cuando la nueva Comisión detalle sus ambiciones. El nuevo programa legislativo y de trabajo de la Comisión para 2010 y el plan de acción para la aplicación del Programa de Estocolmo serán documentos importantes a este respecto. Evidentemente, el SEPD está especialmente interesado en el seguimiento de la consulta pública sobre el futuro marco para la protección de datos.

Otros ámbitos en los que se espera que los progresos conseguidos tengan un impacto en el tratamiento de los datos personales incluyen diferentes instrumentos europeos de las esferas de la sanidad pública, la cooperación en materia de fiscalidad, el transporte (incluidas las novedades relativas al control de automóviles) y el proyecto e-Justicia.

## 3.9.3. Prioridades para 2010

El SEPD establecerá sus prioridades para 2010 basándose en el contexto específico de las novedades anuales y seguirá la dirección de su política de asesoramiento de 2009. Las prioridades quedarán recogidas en el inventario de 2010, que se publicará tras el programa legislativo y de trabajo de la Comisión para 2010, adelantado actualmente a finales de marzo de 2010.

- *En primer lugar, la entrada en vigor del **Tratado de Lisboa** reforzó la importancia de la protección de datos en el marco del Tratado e hizo necesaria la acción legislativa.*
- *El **Programa de Estocolmo** insiste considerablemente en la protección de datos. Destaca la importancia de la protección de los derechos fundamentales en la sociedad de la información y establece la protección de datos como requisito previo para el intercambio de información a fin de salvaguardar la seguridad de la sociedad.*
- *Empezó a trabajar una **nueva Comisión** con ambiciones en la protección de datos y la privacidad. La nueva Comisaria de Justicia, Derechos Fundamentales y Ciudadanía sigue incluyendo un marco completo para la protección de datos como una de sus principales líneas de actuación.*
- *La nueva Comisión está trabajando en la **Agenda Digital Europea**, en la que **la privacidad y la protección de datos son condiciones previas necesarias**, e insiste especialmente, por ejemplo, en la intimidad mediante el diseño.*
- *Hay también importantes progresos que permiten a la UE y sus Estados miembros abordar con mayor eficacia la **dimensión externa de la protección de datos**, no solo en relación con los Estados Unidos, como interesado más destacado en el intercambio de datos, sino también a mayor escala mediante un notable desarrollo de las normas globales.*

# 4

# COOPERACIÓN

## 4.1. Grupo de trabajo del artículo 29

El Grupo de trabajo del artículo 29 se creó en virtud del artículo 29 de la Directiva 95/46/CE. Es un órgano consultivo independiente encargado de la protección de datos personales en el ámbito de aplicación de esta Directiva ([19]). Sus funciones se establecen en el artículo 30 de la misma y pueden resumirse como sigue:

- proporcionar 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 comunitaria 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 de la Comunidad en particular, sobre cuestiones relacionadas con la protección de las personas en lo que respecta al tratamiento de datos personales en la Comunidad Europea.

El SEPD es miembro de pleno derecho del Grupo de trabajo del artículo 29 desde principios de 2004. El artículo 46, letra g), del Reglamento (CE) n° 45/2001 dispone que el SEPD ha de participar en las actividades del grupo. El SEPD lo considera una plataforma muy importante de cooperación con las autoridades nacionales de supervisión. Naturalmente, el grupo debe desempeñar también una función central en la aplicación uniforme de la Directiva y en la interpretación de sus principios generales.

En 2009, el grupo centró sus actividades en los temas identificados en su programa de trabajo para 2008-2009, a saber:

- garantizar una mejor aplicación de la Directiva 95/46/CE;
- asegurar la protección de datos en transferencias internacionales;
- asegurar la protección de datos en relación con las nuevas tecnologías;

([19]) El grupo está integrado por representantes de las autoridades nacionales de supervisión de cada Estado miembro, un representante de la autoridad establecida para las instituciones y organismos comunitarios (es decir, el SEPD) y un representante de la Comisión. Esta última presta también servicios de secretaría al grupo. Las autoridades nacionales de supervisión de Islandia, Noruega y Liechtenstein (socios del EEE) están representadas como observadoras.

- aumentar la eficacia del Grupo de trabajo del artículo 29.

El grupo adoptó diversos documentos a este respecto, entre los cuales cabe destacar:

- **Mejor aplicación de la Directiva 95/46/CE**: contribución conjunta sobre el futuro de la privacidad, en respuesta a la consulta de la Comisión Europea sobre el marco jurídico para el derecho fundamental a la protección de los datos personales (WP168).

- **Transferencias internacionales**: Dictamen 3/2009 sobre el proyecto de Decisión de la Comisión relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE (de los responsables a los encargados del tratamiento) (WP161); dictámenes sobre el nivel de protección de datos personales en Andorra (WP166) e Israel (WP165).

- **Nuevas tecnologías**: dictamen sobre las redes sociales en línea (WP163); dictamen sobre las propuestas que modifican la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas (Directiva sobre la privacidad en las comunicaciones electrónicas) (WP159).

El Grupo de trabajo reaccionó a los progresos en el ámbito de las **nuevas tecnologías** y llevó un seguimiento de la aplicación de su dictamen sobre los **motores de búsqueda** adoptado en 2008, en el marco del cual organizó una audición de proveedores de servicios de motores de búsqueda.

El Grupo de trabajo y el SEPD cooperaron estrechamente en cuestiones relacionadas con los nuevos retos que surgen en el ámbito de la protección de datos. Además de la estrecha colaboración respecto del **futuro del marco de la protección de datos**, el Grupo de trabajo y el SEPD redactaron una respuesta conjunta a la consulta de la Comisión sobre el **impacto del uso de los escáneres de personas** en relación con la seguridad aérea en los derechos humanos, la privacidad, la dignidad personal, la salud y la protección de datos.

Por otra parte, el SEPD coopera con las autoridades de control nacionales en la medida necesaria para el ejercicio de sus deberes respectivos, en particular intercambiando toda la información que pueda resultar útil y pidiendo o prestando asistencia en 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 autoridades nacionales está cobrando cada vez mayor importancia en el contexto de grandes sistemas internacionales como Eurodac, que requieren un planteamiento coordinado en materia de supervisión (véase la sección 4.3).

## 4.2. Grupo de trabajo sobre protección de datos del Consejo

En los últimos años, bajo diferentes Presidencias, el Grupo de trabajo sobre protección de datos ha brindado a los Estados miembros la oportunidad de debatir asuntos relacionados con la protección de datos en el contexto del ahora antiguo primer pilar. En 2009, el Grupo de trabajo solo fue convocado una vez, bajo la Presidencia checa. El SEPD aprovechó la ocasión para presentar un panorama general de sus actividades a los representantes de los Estados miembros.

Debido a la ausencia de iniciativas legislativas de carácter general sobre protección de datos en este ámbito, el Grupo de trabajo no pudo alcanzar su potencial pleno. No obstante, actuando como plataforma para la puesta en común de información y ofreciendo sus conocimientos técnicos de forma proactiva, el Grupo de trabajo podría desempeñar un papel constructivo a la hora de ayudar a desarrollar un marco jurídico global para la protección de datos, función que contaría con la aprobación del SEPD.

La Presidencia española previó una nueva reunión del Grupo de trabajo para marzo de 2010.

## 4.3. 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 (en adelante «el grupo»), integrado por representantes de las autoridades nacionales de protección de datos y el SEPD, se reunió tres veces en 2009.

### Segundo informe de inspección

Uno de los logros más significativos del grupo en 2009 fue la adopción en junio de su segundo informe de inspección. El informe presenta los resultados y las recomendaciones basándose en las respuestas recibidas de todos los Estados miembros. Uno de los objetivos de este ejercicio es contribuir eficazmente a la revisión en curso del marco de Eurodac y de Dublín (véase también la sección 3.3.2).

Las dos cuestiones principales analizadas por el grupo fueron el derecho de los solicitantes de asilo a la información y los métodos de evaluación de la edad de los solicitantes de asilo jóvenes. El informe se envió a los principales interesados institucionales de la UE, las organizaciones internacionales y las organizaciones no gubernamentales (ONG) que trabajan en asuntos relacionados con el asilo y la inmigración.

### El derecho a la información

Si no disponen de información clara y accesible, las personas sujetas al sistema Eurodac no pueden ejercer sus derechos respecto de la protección de datos.

La inspección mostró que la información facilitada a los solicitantes de asilo acerca de sus derechos y el uso de sus datos suele ser incompleta, en especial la relativa a las consecuencias de la toma de las huellas dactilares y al derecho al acceso a sus datos y a la rectificación de los mismos. La información facilitada varía enormemente de unos Estados miembros a otros y se han observado diferencias sustanciales en las prácticas en relación con los solicitantes de asilo y las que se aplican a los inmigrantes ilegales.

Por consiguiente, el informe recomendaba que los Estados miembros mejorasen la calidad de la información que facilitan en materia de protección de datos. Dicha información deberá cubrir los derechos de acceso y rectificación, así como el procedimiento que ha de seguirse para aplicarlos. Por otra parte, las autoridades en materia de asilo deben velar por que se informe siempre tanto a los solicitantes de asilo como a los extranjeros en situación irregular y por que la información facilitada resulte clara y de fácil comprensión. Se debe insistir especialmente en las acciones orientadas a garantizar la visibilidad y el acceso a la información. Por otra parte, los Estados miembros deben promover la cooperación y el intercambio de experiencias entre las autoridades nacionales competentes animándolas a constituir un grupo de trabajo encargado de estudiar este asunto y, a su debido tiempo, desarrollar prácticas armonizadas.

### Evaluación de la edad de los solicitantes de asilo

El Reglamento Eurodac establece que se deben tomar las huellas dactilares de los niños de catorce años o más. Sin embargo, a menudo llegan niños desprovistos de documentos de identidad fiables cuya edad resulta, por lo tanto, difícil de determinar. Para solucionar este problema los países aplican diferentes métodos.

La inspección realizada por el grupo se centró tanto en los métodos utilizados para evaluar la edad de los solicitantes de asilo (que incluyen exámenes médicos intrusivos) como en el procedimiento en el que se integran las pruebas.

Una de las conclusiones alcanzadas fue que los métodos utilizados para determinar la edad de los solicitantes de asilo deben estar claramente precisados y accesibles al público. Se sugirió que, en aras a la armonización, la Comisión debía realizar una evaluación global (que incluyera aspectos médicos y éticos) de la fiabilidad de los diferentes métodos aplicados en los Estados miembros para determinar la edad.

Por otra parte, debería concederse al solicitante de asilo la posibilidad de pedir un segundo dictamen, gratuito, en relación con los resultados médicos y las conclusiones extraídas. Al tomar decisiones que afecten a la situación jurídica del solicitante de asilo, las autoridades en materia de asilo deberán tener en cuenta el margen de error que presentan determinados exámenes médicos.

## 4.4. Tercer pilar

El SEPD mantuvo su cooperación con las autoridades comunes de control (ACC) de Schengen, Europol, Eurojust y el Sistema de Información Aduanero, así como con el Grupo de trabajo sobre policía y justicia (GPJ) creado por la Conferencia Europea de Comisarios de Protección de Datos y Privacidad con el fin de observar los progresos alcanzados en materia de protección de datos en el ámbito de la actuación policial y tomar medidas al respecto.

El trabajo con las ACC se centró en mejorar el intercambio de información e impulsar la coherencia e introducir mejoras en la supervisión de la protección de datos, especialmente a la vista de la entrada en vigor del Tratado de Lisboa. El GPJ se puede considerar un complemento informal del Grupo de trabajo del artículo 29 en los ámbitos en que este no es competente, en especial el antiguo tercer pilar. Como miembro del GPJ, el SEPD participó activamente en sus actividades, que incluían:

- contribuir al debate sobre el Programa de Estocolmo;
- evaluar el impacto de la Decisión marco del Consejo relativa a la protección de los datos personales tratados en el marco de la cooperación policial y judicial, centrándose especialmente en las vías que garanticen un enfoque armonizado de la aplicación a escala nacional;
- controlar la aplicación del Convenio sobre la Ciberdelincuencia del Consejo de Europa, el primer tratado internacional que define una política común encaminada a proteger a la sociedad frente a la ciberdelincuencia cometida a través de Internet u otras redes informáticas;
- expresar una profunda preocupación, de conformidad con el dictamen del SEPD, ante la propuesta de la Comisión de permitir el acceso a Eurodac con fines policiales;
- elaborar un registro de cooperación y de supervisión en el ámbito policial en la UE, que posteriormente fue adoptado por la Conferencia Europea;
- supervisar y mejorar los acuerdos bilaterales y multilaterales existentes entre países europeos y no europeos en el ámbito de la cooperación policial y judicial en materia penal, incluida la lucha contra el terrorismo;
- llevar un seguimiento de los avances alcanzados en relación con el acuerdo internacional suscrito con los EE.UU. respecto a la transferencia de datos de mensajería financiera a efectos del Programa de Seguimiento de la Financiación del Terrorismo, así como el debate a mayor escala sobre la creación de unos principios transatlánticos de protección de datos;
- contribuir a un documento conjunto sobre el futuro de la protección de datos en Europa, en respuesta a una consulta pública organizada por la Comisión Europea.

Para garantizar la coherencia entre las autoridades de protección de datos europeas, el GPJ ha colaborado estrechamente con el Grupo de trabajo del artículo 29 y ha consultado las posiciones adoptadas por el SEPD.

## 4.5. Conferencia Europea

Las autoridades responsables de protección de datos de los Estados miembros de la UE y del 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 Edimburgo los días 23 y 24 de abril de 2009**.

Esta conferencia se centró en la necesidad de **revisar el marco europeo de protección de datos**. Se organizaron cuatro sesiones en torno a esta cuestión, que incluyeron:

- La presentación de un proyecto de informe elaborado por Rand Europe encargado por la Oficina del Comisario de Información del Reino Unido, bajo el título «Revisión de la Directiva sobre protección de datos de la UE», comentado por el SEPD.
- ¿Realmente necesitamos una reforma? Otros puntos de vista sobre las fortalezas y las debilidades de la Directiva 95/46/CE.
- ¿Qué mejoras debería aportar la normativa a las personas, la sociedad y los reguladores?
- El contexto internacional de la normativa.

La conferencia adoptó una declaración sobre «autoridad y porvenir de la protección de datos en Europa» que destacaba el papel de las autoridades responsables de la protección de datos en este debate. La conferencia adoptó igualmente una resolución sobre acuerdos bilaterales entre los Estados miembros de la UE y terceros países en el ámbito de la cooperación policial y judicial en materia penal.


Peter Hustinx en la Conferencia Internacional de Comisarios encargados de la Protección de Datos celebrada en Madrid del 4 al 6 de noviembre de 2009.

La conferencia brindó también la oportunidad de informar sobre las reuniones semestrales del Seminario de Tratamiento de Casos, en las que participan miembros del personal de las autoridades europeas responsables de protección de datos con el fin de intercambiar ideas sobre buenas prácticas. Los talleres de 2009 se celebraron en Praga (República Checa) y en Limassol (Chipre). El próximo Seminario de Tratamiento de Casos se celebrará en Bruselas en la primavera de 2010.

La próxima Conferencia Europea se celebrará en Praga los días 29 y 30 de abril de 2010 y la organizará la autoridad checa de protección de datos.

## 4.6. Conferencia Internacional

Las autoridades responsables de protección de datos y los Comisarios encargados de la protección del derecho a la intimidad de Europa y de otras regiones del mundo, incluidas Canadá, América Latina, Australia, Nueva Zelanda, Hong Kong, Japón y otras entidades políticas de la región Asia-Pacífico, han venido reuniéndose anualmente desde hace muchos años con ocasión de una conferencia que se celebra en otoño. En 2009, la **Conferencia Internacional de Comisarios de Protección de Datos se celebró en Madrid, del 4 al 6 de noviembre, y fue organizada por la Agencia Española de Protección de Datos**. La asistencia no había sido nunca tan numerosa: superó con creces el millar de personas. El tema principal fue «Derecho a la intimidad: el hoy ya es mañana».

Se organizaron diversas sesiones plenarias con el fin de debatir las siguientes cuestiones:

- ¿Una sociedad vigilada? En busca del equilibrio entre seguridad y privacidad.
- ¿*Quo vadis*, Internet?
- Derecho a la intimidad y responsabilidad empresarial.
- Proteger el derecho a la intimidad de los menores, una misión prioritaria.
- Intimidad en la concepción.
- Hacia una regulación del derecho a la intimidad a nivel mundial: propuestas y estrategias.

Uno de los principales temas abordados en la conferencia fue el de la protección de datos como elemento estratégico en el ámbito de las transferencias de datos nacionales e internacionales dentro de un mundo globalizado. La conferencia brindó la

oportunidad de constatar una creciente demanda por parte de los interesados, incluidas la sociedad civil y la industria, de un marco armonizado transfronterizo para la protección de datos. A tal fin, la conferencia adoptó una resolución por la que se acogía favorablemente el proyecto de normas internacionales en materia de protección de datos personales y derecho a la intimidad. Estas normas son el resultado de un año de intenso trabajo preparatorio coordinado por la autoridad española y constituyen el primer paso hacia un instrumento internacional vinculante.

Otra de las cuestiones ampliamente debatidas en Madrid fue la de los sistemas de vigilancia, especialmente los basados en aspectos del cuerpo humano, como la biométrica, cuyo uso se está extendiendo a diferentes ámbitos de la vida cotidiana.

Tanto el Supervisor como el Supervisor Adjunto participaron en la conferencia, presidiendo el primero la sesión paralela «Determinación de la ley aplicable en el mundo de la globalización» e interviniendo el segundo en la sesión paralela «¿Tiene usted vida privada en su puesto de trabajo?».

La próxima conferencia se celebrará en Jerusalén del 27 al 29 de octubre de 2010.

## 4.7. Iniciativa de Londres

En la 28ª Conferencia Internacional celebrada en Londres, en noviembre de 2006, se presentó una declaración titulada «Comunicar la protección de datos y hacerla más eficaz», que recibió el apoyo general de las autoridades de protección de datos de todo el mundo. Se trataba de una iniciativa conjunta del presidente de la autoridad francesa de protección de datos (CNIL), el comisario de información del Reino Unido y el SEPD (denominada desde entonces «Iniciativa de Londres»). El SEPD, en tanto que uno de los arquitectos de la iniciativa, está comprometido a contribuir activamente al seguimiento de la misma junto con las autoridades nacionales responsables de la protección de datos ([20]).

En el contexto de la Iniciativa de Londres, se han organizado varios talleres con el fin de intercambiar experiencias y compartir buenas prácticas en diversos ámbitos, tales como la comunicación, el cumplimiento, la planificación estratégica y la gestión de las autoridades de protección de datos.

En abril de 2009, el SEPD organizó en Bruselas un taller para que las autoridades de protección de datos intercambiaran buenas prácticas sobre el tema «Responder a las infracciones de seguridad». Este taller cerrado supuso también una aportación a un seminario con otros interesados en el tema organizado por el SEPD junto con la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) y acogido por el Parlamento Europeo en octubre de 2009.

## 4.8. Organizaciones internacionales

En noviembre de 2009, el SEPD y el Instituto Universitario Europeo (IUE) empezaron los preparativos del tercer taller sobre Protección de Datos en las Organizaciones Internacionales, que tendrá lugar en la primavera de 2010 en Florencia.

A raíz de la adopción en 2003, en la Conferencia Internacional de Sydney, de la resolución sobre protección de datos y organizaciones internacionales ([21]), el SEPD organizó, junto con el Consejo de Europa, la OCDE y la Oficina Europea de Patentes, dos talleres previos en Ginebra (2005) y Múnich (2007). A menudo las organizaciones internacionales exentas de la aplicación del Derecho nacional carecen de un marco jurídico para la protección de datos. En estos actos se hizo hincapié en su interés creciente tanto en la protección de datos personales como en que se vele por el cumplimiento dentro de estas organizaciones.

En este tercer taller, el SEPD pretende centrar el debate en las siguientes cuestiones:

- la gestión de la protección de datos en las organizaciones internacionales;
- el cumplimiento en la práctica, especialmente en la gestión de los datos sobre recursos humanos;
- los retos tecnológicos y las medidas de seguridad relacionadas;
- el uso de la biométrica en las fronteras y con fines de seguridad interna.

([20]) Véase el Informe Anual 2006, apartados 4.5 y 5.1.

([21]) http://www.privacyconference2008.org/adopted_resolutions/5-SYDNEY2003/SYDNEY-EN4.pdf

# 5

# COMUNICACIÓN

## 5.1. Introducción

La información y la comunicación juegan un papel esencial a la hora de conferir notoriedad a las principales actividades del SEPD y mejorar los conocimientos de que disponemos, tanto sobre el trabajo del SEPD como sobre la protección de datos en general. El hecho reviste una importancia particularmente estratégica, ya que el SEPD es aún una institución relativamente joven y, por lo tanto, necesita consolidar la conciencia de su papel entre la instituciones de la UE. Los años posteriores a la creación de la institución se consagraron principalmente a este cometido, con lo que en general fue posible incrementar la notoriedad. Indicadores como el mayor número de solicitudes de información recibidas de ciudadanos de la UE, el aumento del volumen de preguntas recibidas de los medios de comunicación, el incremento en el número de abonados al boletín y de invitaciones para intervenir en conferencias, así como el tráfico cada vez más intenso en el sitio en Internet, respaldan la noción 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 de supervisión en relación con todas las instituciones y organismos comunitarios que participan en el tratamiento de datos personales, el papel asesor en relación con aquellas instituciones que participan en el desarrollo y la adopción de nueva legislación y de políticas que pueden afectar a la protección de datos personales (Comisión, Consejo y Parlamento) y el papel de cooperación en relación con las autoridades nacionales de supervisión y los diversos organismos del ámbito de la seguridad y la justicia.

El aumento de la concienciación y la mejora de la comunicación sobre problemas destacados de la protección de datos fueron también un objetivo importante de la Iniciativa de Londres (véase sección 4.7). Un resultado significativo del primer seminario en este contexto fue la creación de una red de funcionarios encargados de comunicación (con la participación del SEPD). Las autoridades responsables de la protección de datos están utilizando esta red para intercambiar buenas prácticas y llevar a cabo proyectos específicos, como el desarrollo de acciones conjuntas para acontecimientos pertinentes.

En 2009, las actividades se centraron principalmente en mejorar y desarrollar las herramientas de información y de comunicación creadas en los primeros años de la institución, con el fin de instaurar una comunicación más eficaz y lograr un mayor acercamiento tanto a la administración de la UE como al público en general.

El Supervisor y el Supervisor Adjunto han invertido mucho tiempo y grandes esfuerzos en explicar su misión y en sensibilizar respecto a la protección de datos y varias cuestiones concretas en diferentes discursos pronunciados durante el año (véase el anexo G).

## 5.2. Características de la comunicación

Hay que configurar la política de comunicación del SEPD de acuerdo con características específicas pertinentes, teniendo en cuenta la edad 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 diversas limitaciones y requisitos.

### 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 operan 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, los interlocutores en las políticas de la UE y «los homólogos de la protección de datos». Como resultado, la política de comunicación del SEPD no tiene por qué embarcarse en una estrategia de «comunicación de masas». Más bien, la sensibilización respecto de los problemas de protección de datos entre la ciudadanía de la UE en los Estados miembros depende esencialmente de un planteamiento más indirecto, principalmente a través de las autoridades responsables de protección de datos a nivel nacional, y del uso de centros de información y puntos de contacto.

Sin embargo, el SEPD también asume la parte que le toca en la promoción de su perfil entre el público en general, en especial por medio de diversas herramientas de comunicación (sitio en Internet, boletín de noticias y otros materiales informativos), atendiendo con regularidad a las partes interesadas (por ejemplo, a los estudiantes que visitan su oficina) y participando en acontecimientos, reuniones y conferencias públicos.

### Lenguaje utilizado

La política de comunicación del SEPD también debe tener en cuenta la naturaleza específica del ámbito en el que se desarrolla su actividad. Para los profanos en la materia, los problemas ligados a la protección de datos pueden aparecer un tanto técnicos y oscuros, y la lengua en la que el SEPD se comunica 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 la terminología especializada innecesaria. Se hacen por lo tanto esfuerzos constantes en esta dirección, con el objetivo de corregir la imagen excesivamente «jurídica» de la protección de datos.

Cuando consideramos audiencias más especializadas (por ejemplo, los medios de comunicación, los especialistas en protección de datos, las partes interesadas de la UE), el uso de los términos técnicos y jurídicos está más justificado. Por ello, una misma noticia puede obligar a emplear un formato y un estilo de edición adaptados, a fin de reflejar correctamente a las necesidades del público destinatario.

## 5.3. Relaciones con los medios de comunicación

El SEPD aspira a mantener las relaciones más fluidas posibles con la prensa, de manera que la ciudadanía pueda mantenerse al corriente de sus actividades. El SEPD informa regularmente a los medios de comunicación mediante comunicados de prensa, entrevistas, debates de fondo y ruedas de prensa. El frecuente tratamiento de solicitudes procedentes de los medios de comunicación permite un mayor contacto con los medios de comunicación.

En 2009, el servicio de prensa publicó 14 **comunicados de prensa**, la mayoría relacionados con nuevos dictámenes legislativos que guardan un alto grado de interés para el público. Entre las cuestiones abordadas se encuentran la revisión de la Directiva sobre la privacidad en las comunicaciones electrónicas, el acceso del público a los documentos de la UE, el nuevo Programa de Estocolmo en materia de justicia y asuntos de interior, los sistemas de transporte inteligentes en el transporte por carretera, el acceso de los servicios de seguridad a Eurodac y la nueva Agencia para la Gestión Operativa de Sistemas Informáticos a gran Escala en el Ámbito de la Libertad, la Seguridad y la Justicia.

Los comunicados de prensa se publican en el sitio del SEPD en Internet y en la base de datos interinstitucional de comunicados de prensa de la Comisión Europea (RAPID) en inglés y francés. Los

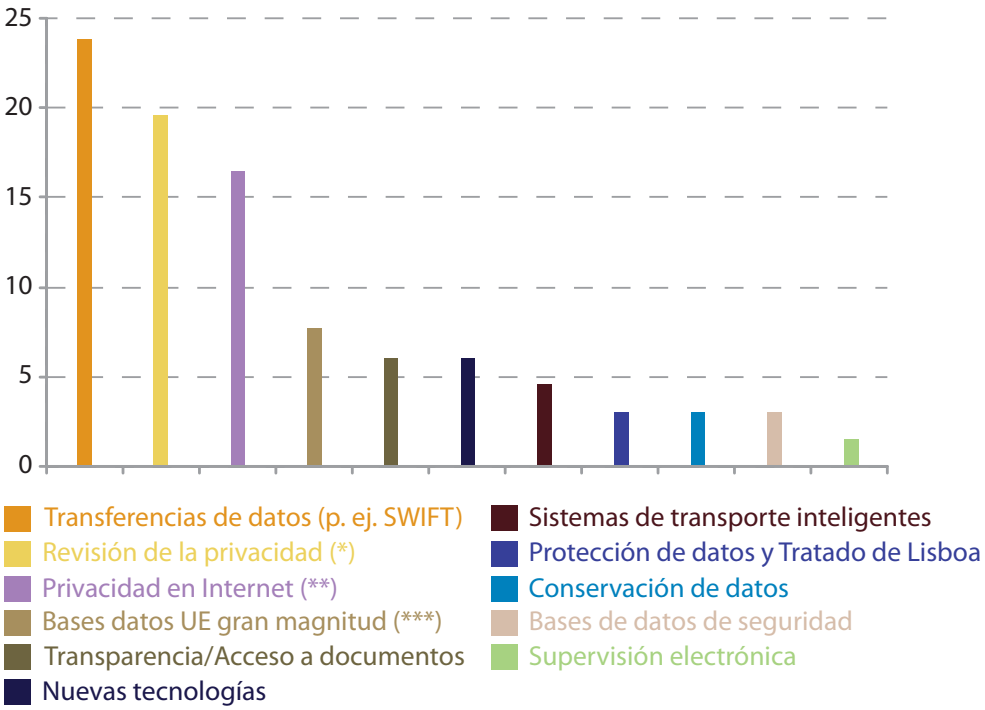
comunicados se distribuyen a una red de periodistas e interlocutores que se actualiza periódicamente. La información proporcionada en los comunicados de prensa genera habitualmente una cobertura significativa en los medios de comunicación, pues a menudo se recogen tanto en la prensa general como en la especializada, además de publicarse en una serie de sitios Internet institucionales y no institucionales que van desde los de instituciones y organismos de la UE, hasta los de las organizaciones no gubernamentales, las instituciones académicas y las empresas de tecnología de la información.

En 2009, el SEPD concedió alrededor de 20 **entrevistas** a periodistas de medios de comunicación impresos, de radiodifusión y electrónicos de toda Europa, en respuesta a un considerable número de peticiones procedentes de la prensa alemana, austriaca, neerlandesa y belga. Ello dio lugar a varios artículos en prensa nacional, internacional y comunitaria, a publicaciones y páginas web especializadas en problemas de tecnologías de la información, así como a entrevistas en la radio y la televisión (por ejemplo, en el canal televisivo franco-alemán ARTE, la radio neerlandesa y las televisiones sueca y neerlandesa). Las entrevistas abarcaron cuestiones transversales tales como la seguridad de los datos europeos, la tendencia hacia una sociedad de la vigilancia y los retos actuales y venideros en el ámbito de la privacidad y la protección de datos. También se abordaron cuestiones más específicas, como el nuevo acuerdo SWIFT entre la UE y los EE.UU., los pasaportes biométricos y las bases de datos de huellas dactilares, el nuevo requisito de notificación de las violaciones de datos de la Directiva sobre privacidad en las comunicaciones electrónicas revisada y el impacto del Tratado de Lisboa sobre la protección de datos.

Se reciben con frecuencia **preguntas de los medios de comunicación** que suelen incluir peticiones de comentarios del SEPD y solicitudes de aclaraciones o información. En 2009, atrajeron principalmente la atención de los medios de comunicación cuestiones relacionadas con la transferencia de datos (por ejemplo, el debate sobre un nuevo acuerdo SWIFT), la revisión de la Directiva sobre privacidad en las comunicaciones electrónicas (en particular, la nueva disposición sobre la notificación obligatoria de las violaciones de la seguridad), las preocupaciones que suscita el derecho a la intimidad en Internet, incluidos los motores de búsqueda, las nuevas aplicaciones en línea y las redes sociales y las bases de datos de la UE a gran escala. El acceso a los documentos de la UE y las nuevas tecnologías (como la identificación por radiofrecuencia (RFID) y la computación en la nube) fueron también cuestiones especialmente destacadas para la prensa.

Peter Hustinx entrevistado por un periodista.

Principales temas de las solicitudes presentadas por la prensa en 2009




(*) Incluidas las nuevas disposiciones sobre violación de datos.

(**) Incluidos los motores de búsqueda, las aplicaciones en línea y las redes sociales.

(***) Principalmente Eurodac, SIA y VIS.

## 5.4. Solicitudes de información y de asesoramiento

El número de solicitudes de información o ayuda recibidas de los ciudadanos permaneció relativamente estable en 2009 (174 solicitudes, en comparación con las 180 de 2008). Estas solicitudes tuvieron origen en un amplio abanico de individuos y partes que abarcan desde los interlocutores 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 (bufetes de abogados, asesores, agentes de grupos de presión, organizaciones no gubernamentales, asociaciones, universidades, etc.) a los ciudadanos que piden más información sobre cuestiones de derecho a la intimidad o que solicitan ayuda para solucionar las cuestiones o problemas a los que se enfrentan. Estas peticiones se reciben fundamentalmente a través de la dirección de correo electrónico general del SEPD.

La primera categoría de solicitudes recibidas en 2009 incluye las reclamaciones formuladas por ciudadanos de la UE en las que el SEPD no tiene competencia. La mayoría de estas reclamaciones se referían a supuestas violaciones en materia de protección de datos por parte de empresas o autoridades públicas nacionales, sitios de Internet extracomunitarios o redes sociales en línea. Otras se referían a una supuesta violación de la privacidad durante un procedimiento judicial nacional y a una solicitud de recurso contra una sentencia de una autoridad nacional de protección de datos. Dado que este tipo de reclamaciones no son competencia del SEPD, se responden especificando 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 2009 corresponde a la legislación sobre protección de datos en los Estados miembros de la UE o 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 competente y, en su caso, con la Unidad de Protección de Datos de la Comisión Europea.

La mayor parte de las categorías de solicitudes información restantes son competencia del SEPD, por lo que esas solicitudes obtuvieron respuestas sustanciales. Incluían preguntas acerca de la legislación

sobre protección de datos de la UE, las actividades del SEPD, los flujos de datos transfronterizos, las nuevas disposiciones sobre protección de datos del Tratado de Lisboa y los problemas de protección de datos relacionados con el uso de los escáneres de personas en los aeropuertos.

## 5.5. Visitas de estudio

Como parte de los esfuerzos dirigidos a aumentar tanto la concienciación en materia de protección de datos, como la interacción con el mundo académico, el SEPD regularmente acoge las visitas de grupos de estudiantes especializados en el ámbito de la legislación europea, la protección de los datos y/o los problemas de seguridad de las tecnologías de la información. Por ejemplo, en octubre de 2009, la oficina del SEPD recibió, por ejemplo, a un grupo de estudiantes de Derecho internacional y europeo de la Universidad de Grenoble, en Francia, a quienes presentó sus funciones y actividades y con quienes debatió sobre asuntos relacionados con la protección de datos en la lucha contra el terrorismo. También se acogió a otros grupos de visitantes, como un grupo de estudiantes austriacos de gestión pública de máster de dirección de empresas y otro de estudiantes de la Universidad de Tilburg, en los Países Bajos.

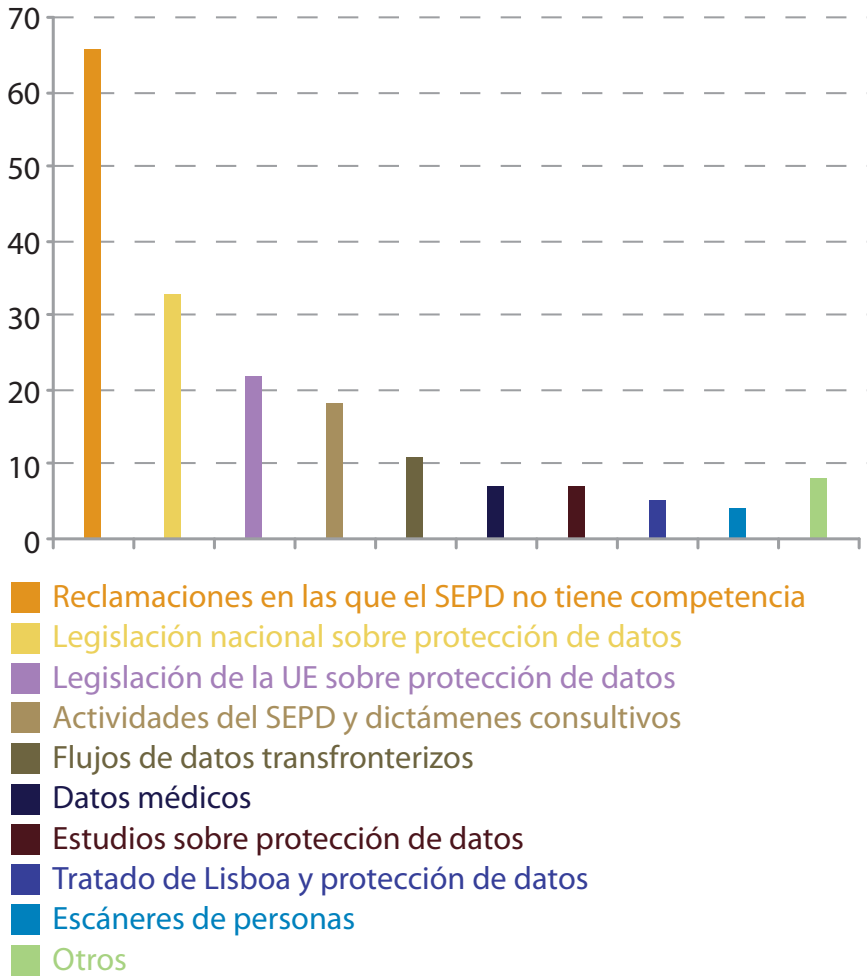
A fin de llegar a un público más joven, la oficina del SEPD recibió a un grupo de estudiantes austriacos de bachillerato con quienes el personal debatió sobre cuestiones de su interés relativas a la protección de datos, como las redes sociales en línea y la protección de los menores en Internet.

## 5.6. Herramientas de información en línea

### Sitio en Internet

El sitio en Internet sigue siendo la herramienta de comunicación e información más importante del

Principales temas de las peticiones de información del público en 2009



SEPD. Se actualiza casi diariamente. Es también el medio de comunicación a través del cual los visitantes pueden acceder a los diversos documentos presentados dentro del marco de las actividades del SEPD (por ejemplo, dictámenes sobre controles previos y propuestas de legislación de la UE, observaciones, prioridades de trabajo, publicaciones, discursos y contribuciones por escrito, comunicados de prensa, boletines e información sobre acontecimientos).

### *Evolución del contenido*

En 2009, además de una actualización que recogía el nombramiento del Supervisor y el Supervisor Adjunto para el segundo mandato del SEPD, se publicaron nuevas herramientas que responden a las expectativas de los visitantes y explican mejor las actividades del SEPD. Tales mejoras incluían la publicación de un glosario de términos relacionados con la protección de datos personales y un apartado de preguntas y respuestas.

También se llevó a cabo una actualización profunda de todas las páginas del sitio en Internet previa a la introducción de una versión alemana que en 2010 se sumará a las ya existentes, inglesa y francesa. También está previsto desarrollar un apartado de preguntas frecuentes, con el fin de dar respuestas a diferentes perfiles y públicos (por ejemplo, personal de la UE, visitantes y solicitantes de empleo en las instituciones y organismos de la UE).

Se han proyectado otras mejoras del sitio en Internet que incluirán la introducción de un formulario de reclamaciones en línea, el desarrollo de un registro de notificaciones y una revisión de la página principal con el fin de destacar las últimas noticias relacionadas con las actividades del SEPD.

### *Adelantos técnicos y tráfico*

En el marco de los esfuerzos por mejorar los resultados del sitio en Internet, 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 2009 el sitio en Internet recibió un total de 92 884 visitas únicas, con más de 8 000 al mes en enero, marzo, abril, octubre y noviembre. Tras la página de inicio, las más visitadas fueron las de «Contacto», «Supervisión» y «Consulta», si bien las de «Noticias», «Publicaciones» y «Acontecimientos» figuran asimismo entre las más consultadas. Las estadísticas muestran asimismo que la mayor parte de los visitantes acceden al sitio en Internet por medio de una dirección directa, un marcador, un vínculo en un correo electrónico o un vínculo en otro sitio en Internet, como el portal Europa o el sitio en Internet de una autoridad nacional de protección de datos. Solo un número muy reducido de visitantes llega al sitio en Internet por medio de un motor de búsqueda. Estas cifras nos dan a entender que el sitio del SEPD en Internet es consultado por un núcleo de visitantes regulares que confían en su contenido.

## Boletín

El boletín del SEPD sigue siendo una herramienta eficaz para informar sobre las últimas actividades del SEPD y para llamar la atención sobre novedades recientes del sitio en Internet. El boletín proporciona noticias relacionadas con los últimos dictámenes del SEPD sobre propuestas legislativas de la UE, así como sobre los controles previos. Incluye información sobre próximas conferencias y otros acontecimientos y discursos recientes del Supervisor y del Supervisor Adjunto. Los boletines se encuentran disponibles en el sitio en Internet del SEPD y también se ofrece un dispositivo automático de suscripción en la página correspondiente.

En 2009 se publicaron cinco números del boletín, con una frecuencia media de uno cada dos meses. El boletín se publica en inglés y en francés y se espera que a lo largo de 2010 se empiece a publicar también una versión en alemán.

El número de abonados se incrementó, pasando de 880 personas a finales de 2008 a unas 1 200 al final de 2009. Entre los abonados figuran miembros del Parlamento Europeo, personal de la UE y personal de autoridades nacionales responsables de protección de datos, así como periodistas, personalidades del mundo académico, empresas de telecomunicación y bufetes de abogados.

Este aumento sustancial y constante en el número de suscripciones ha hecho necesario proporcionar una publicación actualizada y más fácil de utilizar, con una estructura revisada y más accesible. La primera edición de la nueva versión del boletín se publicó en octubre de 2009.


Espacio del SEPD en la Comisión Europea el Día de la Protección de Datos.

## 5.7. Publicaciones

### Informe Anual

El Informe Anual es la publicación principal del SEPD. Proporciona una descripción general de las actividades del SEPD en los principales ámbitos operativos de la supervisión, el asesoramiento y la cooperación durante el año de referencia. También describe lo logrado en términos de comunicación exterior, así como las incidencias relativas a la administración, el presupuesto y el personal.

El Informe Anual puede ser especialmente interesante 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 especial, el sistema institucional de la UE, las autoridades de protección de datos, los especialistas de protección de datos, los grupos de interés 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.

El 16 de abril de 2009, el Supervisor y el Supervisor Adjunto presentaron un resumen del Informe Anual 2008 del SEPD a la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo.

### Folleto informativo

En el contexto del segundo mandato del SEPD (2009-2014), en 2009 se elaboró un nuevo folleto informativo. Este folleto va dirigido al gran público y proporciona información sobre las competencias y funciones del SEPD, los derechos de los titulares de los datos, el papel de los responsables de la protección de datos y el procedimiento de presentación de reclamaciones al SEPD. También contiene directrices y unas breves explicaciones sobre los elementos más importantes de la función del SEPD y la protección de datos personales en la administración de la UE.

En 2010 se elaborarán documentos temáticos sobre cuestiones específicas de protección de datos, con el fin de proporcionar orientación específica tanto al público en general como a las partes interesadas.

## 5.8. Eventos de sensibilización

La participación en eventos relacionados con la UE ofrece una excelente oportunidad para que el SEPD dé a conocer mejor los derechos de los titulares de los datos y las obligaciones de las instituciones y organismos europeos en relación con la intimidad y la protección de datos personales.

### Día de la Protección de Datos

El 28 de enero de 2009 los Estados miembros del Consejo de Europa y las instituciones europeas celebraron el tercer Día Europeo de la Protección de Datos. Esta fecha marca el aniversario del Convenio para la Protección de los Datos de Carácter Personal del Consejo de Europa (Convenio 108), primer instrumento internacional jurídicamente vinculante relacionado con la protección de los datos, que se adoptó en 1981.

El acontecimiento dio al SEPD la oportunidad de insistir en la importancia del derecho a la intimidad y la protección de datos, y en particular de dar a conocer al personal de la UE sus derechos y obligaciones en este ámbito. Durante tres días consecutivos se instaló un espacio de información en los locales del Parlamento Europeo, de la Comisión Europea y del Consejo. El SEPD resaltó sus funciones de supervisión, asesoramiento y cooperación, así como sus logros y sus actividades actuales. El espacio de información del SEPD se creó en cooperación con los responsables de protección de datos de las instituciones correspondientes, que presentaron asimismo sus actividades. Se distribuyeron diversas publicaciones en las que se detallaban la función del SEPD y su trabajo, y los visitantes tuvieron la oportunidad de poner a prueba sus conocimientos sobre protección de datos con un breve juego de preguntas.

Para la próxima edición del Día de la Protección de Datos, el objetivo será seguir desarrollando esta actividad, especialmente mediante el uso de material de vídeo, y diversificar las acciones en este contexto a fin de conectar más eficazmente con los miembros del personal de la UE y otras partes pertinentes.

### Jornada de Puertas Abiertas de la UE

El 9 de mayo de 2009, la oficina del SEPD también participó, como hace ahora cada año, en la Jornada de Puertas Abiertas de las Instituciones Europeas organizada en el Parlamento Europeo en Bruselas.

El SEPD dispuso de un espacio de información situado en el edificio principal del Parlamento Europeo y los miembros de su personal 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 espacio, a quienes propuso también un juego de preguntas sobre derecho a la intimidad y protección de datos.

# 6

# ADMINISTRACIÓN, PRESUPUESTO Y PERSONAL

## 6.1. Introducción

El primer mandato de los dos Supervisores finalizó en enero de 2009. Tras las elecciones celebradas en 2008, el Consejo y el Parlamento Europeo designaron un nuevo equipo para un mandato quinquenal.

Para poder disponer de una reserva de personal con un alto grado de especialización, el SEPD convocó una oposición sobre protección de datos organizada por la Oficina Europea de Selección de Personal (EPSO). La lista de reserva estará disponible en el verano de 2010.

El entorno administrativo se va ampliando paulatinamente en función de las prioridades anuales, teniendo en cuenta las necesidades y el tamaño de la institución.

El SEPD adoptó un nuevo Reglamento interno necesario para el buen funcionamiento de la institución.

La colaboración con otras instituciones (Parlamento Europeo, Consejo y Comisión Europea) siguió mejorando, lo cual permitió realizar importantes economías de escala.

## 6.2. Presupuesto

El presupuesto adoptado por la autoridad presupuestaria para 2009 fue de 6 663 026 euros, lo que supone un aumento respecto de 2008 debido, principalmente, a la creación de nuevos puestos, al cambio de Supervisores y al aumento del espacio debido al crecimiento de la institución.

Además de los salarios y los gastos del edificio, las traducciones absorben una parte considerable del presupuesto. Los dictámenes del SEPD sobre propuestas legislativas se traducen a 23 lenguas oficiales europeas y se publican en el *Diario Oficial de la Unión Europea*. Los dictámenes sobre controles previos y otros documentos publicados se traducen también a las lenguas de trabajo del SEPD.

En su informe sobre el ejercicio presupuestario de 2008, el Tribunal de Cuentas Europeo afirmó que la auditoría no había dado lugar a ninguna observación.

La Comisión siguió prestando asistencia al SEPD, en concreto en los servicios de contabilidad, ya que su contable también es nombrado contable del SEPD. El SEPD aplica las normas internas de la Comisión para la ejecución del presupuesto. Esas normas son aplicables a la institución y en los casos en que no se han fijado normas específicas.

## 6.3. Recursos humanos

El SEPD cuenta con una ayuda muy eficaz de los servicios de la Comisión Europea en lo que se refiere a las tareas relacionadas con la gestión del personal de la institución.

### 6.3.1. Contratación

La creciente proyección pública de la institución está dando lugar a una mayor carga de trabajo y a una ampliación de sus actividades. En los capítulos anteriores se ha descrito ya el importante aumento que registró la carga de trabajo en 2009. Los recursos humanos deben desempeñar un papel fundamental en este contexto; con todo, el SEPD ha optado por limitar la ampliación mediante un crecimiento controlado, a fin de garantizar que el nuevo personal se integre plenamente en la institución y reciba toda la formación necesaria.

El SEPD tiene acceso a los servicios de la Oficina Europea de Selección de Personal (EPSO) y participa en los trabajos de su Consejo de Administración, por el momento en calidad de observador. En cooperación con la EPSO, el SEPD convocó una oposición para reclutar personal responsable de la protección de datos con un alto grado de especialización. La lista de reserva estará disponible en el verano de 2010.

En cuanto a las aplicaciones informáticas de gestión de los recursos humanos (utilizadas principalmente para las misiones, las vacaciones y la formación), la Comisión suspendió su antiguo proyecto en este ámbito y creó Sysper2, que el SEPD podrá empezar a utilizar a finales de 2010.

### 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 en las actividades diarias del SEPD. Como resultado, se ofrece al SEPD la oportunidad de aumentar su proyección pública entre los jóvenes ciudadanos de la UE, en particular los estudiantes universitarios y los jóvenes titulados 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).

Además del programa principal, se han adoptado disposiciones especiales para aceptar estudiantes universitarios y doctorandos no remunerados durante breves periodos de formación. De este modo, se ofrece a los estudiantes una oportunidad de realizar investigaciones para su tesis. Ello se hace con arreglo al proceso de Bolonia y la consiguiente obligación de que dichos estudiantes universitarios completen sus prácticas como parte de sus estudios. Estos periodos de prácticas están limitados a situaciones excepcionales y sujetos a criterios de admisión estrictos.

Todas las personas en prácticas, remuneradas o no, participaron tanto en el trabajo teórico como en el práctico y adquirieron experiencia útil de primera mano.

Con arreglo a los acuerdos de nivel de servicio firmados en 2005 y 2008, el SEPD contó con la asistencia administrativa de la Oficina de Prácticas de la Dirección General de Educación y Cultura de la Comisión, 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 se puso en marcha en enero de 2006. Cada año se ha enviado en comisión de servicio a una media de dos expertos nacionales procedentes de las autoridades nacionales responsables de protección de datos de diferentes Estados miembros. El envío de expertos nacionales hizo posible que el SEPD se beneficiase de las capacidades y la experiencia profesional de dicho personal y permitió incrementar su visibilidad a nivel nacional. Al mismo tiempo, este programa brinda a los expertos nacionales la oportunidad de familiarizarse con asuntos de protección de datos en el entorno de la UE.

Para proveer los puestos de expertos nacionales, el SEPD se dirige directamente a las autoridades nacionales de protección de datos. Se informa asimismo a las representaciones permanentes nacionales y se las invita a participar en la búsqueda de los candidatos adecuados.

### 6.3.4. Organigrama

El organigrama del SEPD no ha variado desde 2004 y se compone de una unidad, que actualmente consta de ocho miembros, encargada de la administración, el personal y el presupuesto, y los restantes miembros de la plantilla, que incluyen un pequeño equipo de coordinadores encargados de los aspectos operativos y organizados en dos ámbitos de actividad principales: supervisión y consulta. Un responsable de prensa coordina un reducido equipo de información. Todos ellos trabajan bajo la autoridad directa del Supervisor, el Supervisor Adjunto y un Director en tanto que Jefe de Secretaría.

A finales de 2009 se introdujo a este último como primer paso para la reestructuración de la organización que se prevé en el transcurso de 2010.

### 6.3.5. Formación

En 2009, la política interna de formación siguió orientada a ampliar y mejorar los conocimientos y las competencias del personal con el fin de contribuir más eficazmente al logro de los objetivos de la institución.

Los miembros de la plantilla del SEPD tienen acceso a los cursos de formación organizados a escala interinstitucional. Además, algunos de ellos asistieron a cursos de formación externa con el fin de desarrollar la excelencia en el ámbito de la protección de datos.

El plan de formación de 2009 tuvo en cuenta las necesidades expresadas por el personal en una encuesta y se centró en las principales áreas de aprendizaje identificadas en las orientaciones generales anexas a la decisión sobre formación interna.

Los cursos de lenguas ocuparon una parte considerable del número total de días dedicados a la formación en 2009. El elevado índice de participación confirma el principio de que el aprendizaje de lenguas en el SEPD debería servir en primer lugar para mejorar la eficacia profesional y satisfacer las necesidades en materia de empleo, incluida, naturalmente, la integración armoniosa de nuevo personal en la organización.

El SEPD siguió participando en los comités interinstitucionales (grupo de trabajo interinstitucional de la Escuela Europea de Administración, comité interinstitucional de formación lingüística, etc.) con la finalidad de poner en común un planteamiento conjunto en un sector en que las necesidades son básicamente las mismas en todas las instituciones y permiten economías de escala.

En 2009, el SEPD firmó, junto con las instituciones restantes, el protocolo sobre la armonización del coste de los cursos interinstitucionales de lenguas y el nuevo protocolo sobre la distribución por instituciones de los costes de los proyectos pedagógicos sobre lenguaje interinstitucional.

Asimismo, el SEPD firmó con la Escuela Europea de Administración (EAS) un acuerdo de nivel de servicio que permitió a los miembros de su personal seleccionados para el ejercicio de certificación participar en el programa de formación obligatoria para el procedimiento de certificación.

### 6.3.6. Actividades sociales

El Supervisor y el Supervisor Adjunto dan personalmente la bienvenida a todos los miembros del personal recién llegados. Estos se reúnen, además de con su mentor, con los miembros de la unidad administrativa, que les informan sobre las características específicas de la institución y les entregan la guía administrativa del SEPD. El SEPD ha firmado un acuerdo de cooperación con la Comisión para ayudar a los nuevos colegas a integrarse, por ejemplo, facilitándoles asistencia jurídica en cuestiones privadas (contratos de alquiler, adquisición de vivienda, etc.) y brindándoles la oportunidad de participar en diversas actividades sociales y en red.

El SEPD está tomando parte, en calidad de observador, en el Comité Consultivo de Prevención y Protección en el Trabajo del Parlamento Europeo, cuyo objetivo es mejorar el entorno de trabajo. Se ha iniciado una reflexión sobre el bienestar en el trabajo.

Lamentablemente, el diálogo social dentro del SEPD se interrumpió temporalmente por la dimisión del Comité de Personal, que no se renovó. No obstante, fue posible organizar una actividad social fuera de la oficina.

El SEPD continuó con el desarrollo de la cooperación interinstitucional en el ámbito de las infraestructuras sociales: los hijos del personal del SEPD tienen acceso a las guarderías, a las guarderías postescolares y a las guarderías al aire libre de la Comisión, así como a las Escuelas Europeas.

## 6.4. Funciones de control

### 6.4.1. Control interno

El sistema de control interno, que funciona desde 2006, vela por que los objetivos del SEPD se alcancen con eficacia y de conformidad con sus Reglamentos. El SEPD ha adoptado procedimientos de control interno específicos que se adaptan mejor a sus necesidades y al tamaño y las actividades de la institución. El sistema no está diseñado para eliminar el riesgo de no lograr los objetivos empresariales, sino para gestionarlo.

En 2009, la evaluación de los riesgos asociados a las actividades del SEPD siguió orientada a diseñar un

sistema de gestión del riesgo para identificar, evaluar y, en su caso, actuar para contrarrestar los riesgos asociados a sus actividades.

El SEPD tomó nota del Informe Anual de actividad y la declaración de garantía asociada firmada por el ordenador delegado. En general, el SEPD considera que los sistemas de control interno aplicados ofrecen una garantía razonable de la legalidad y la regularidad de las operaciones de las que la institución es responsable.

### 6.4.2. Auditoría interna

El auditor interno de la Comisión fue designado auditor interno del SEPD.

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

En 2009 se recibió y se adoptó el informe correspondiente a la auditoría de seguimiento efectuada en diciembre de 2008 por el Servicio de Auditoría Interna. El informe confirmaba la capacidad del sistema de control interno del SEPD de ofrecer una garantía razonable del logro de los objetivos de la institución, si bien identificó algunos aspectos que se habían de mejorar. En algunos de ellos ya se ha actuado, mientras que en otros se irá trabajando a medida que las funciones del SEPD evolucionen.

### 6.4.3. Seguridad

A finales de 2008, el SEPD adoptó una decisión sobre las medidas de seguridad aplicables en su institución. Esta decisión incluye medidas sobre la gestión de la confidencialidad de la información, la seguridad informática y las condiciones de salud y seguridad de la plantilla y los locales. En 2009 se organizó una sesión informativa para promover la sensibilización respecto de la sensibilidad y asegurarse de que el personal está enterado de las medidas de seguridad establecidas.

### 6.4.4. Responsable de protección de datos

La aplicación interna de las disposiciones establecidas en el Reglamento (CE) nº 45/2001, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos prosiguieron en 2009.

Las notificaciones al responsable de protección de datos (RPD) de las operaciones de tratamiento de datos personales identificadas en el inventario del SEPD también siguieron en 2009. En los casos sujetos a notificaciones de control previo se aplicó un procedimiento simplificado que tiene en cuenta la posición específica del SEPD. Se creó un registro de notificaciones.

La participación en las reuniones de la red de RPD permite al SEPD compartir experiencias y debatir cuestiones comunes.

## 6.5. Infraestructura

En cumplimiento del acuerdo de cooperación administrativa, el SEPD ocupa locales del Parlamento Europeo, lo que representa una ayuda adicional al SEPD, principalmente en materia de tecnologías de la información (TI) e infraestructura.

El SEPD siguió gestionando de modo independiente su inventario de mobiliario y de equipo de tecnologías de la información, asistido por los servicios del Parlamento Europeo.

## 6.6. Entorno administrativo

### 6.6.1. Asistencia administrativa y cooperación interinstitucional

El SEPD se acoge al acuerdo de cooperación interinstitucional en numerosos ámbitos administrativos en virtud del acuerdo de cooperación administrativa celebrado en 2004, y prorrogado en 2006 por un periodo de tres años, con las Secretarías Generales de la Comisión, el Parlamento y el Consejo. Esta cooperación aporta al SEPD un valor añadido considerable en términos de aumento de la eficacia y de economías de escala. Ello permite también evitar la multiplicación innecesaria de infraestructuras administrativas y la reducción de gastos administrativos a la vez que se garantiza una administración de servicio público de alto nivel.

Basándose en esto, en 2008 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, distintos

servicios del Parlamento Europeo (servicios de información y tecnología, particularmente en lo que se refiere a la nueva versión del sitio del SEPD en Internet, adaptación de los locales, seguridad de los edificios, imprenta, correo, teléfono, material de oficina, etc.) y el Consejo (traducción).

Se firmó un acuerdo de nivel de servicio con la Oficina de Gestión y Liquidación de los Derechos Individuales que abarca diferentes actividades, incluidos la determinación, el cálculo y el pago de los derechos individuales de los miembros del personal actuales y antiguos, así como el reembolso de los gastos de misiones, asistencia sanitaria y expertos.

En virtud de la evaluación positiva, se firmó una prórroga de dos años, de enero de 2010 al mismo mes de 2012. El acuerdo con el Consejo Europeo sobre los servicios de traducción vencerá EN enero de 2010. Un nuevo acuerdo se firmó con el Centro de Traducción de los Órganos de la Unión Europea, que asumirá las tareas de traducción a partir de 2010.

Los acuerdos de nivel de servicio existentes se actualizan con regularidad. En noviembre de 2009, el SEPD firmó un nuevo acuerdo de nivel de servicio con la Escuela Europea de Administración relativo al programa de formación del personal para el procedimiento de certificación.

El acceso directo desde los locales del SEPD a algunas aplicaciones de gestión financiera de la Comisión facilitó la cooperación y el intercambio de información entre los departamentos de la Comisión y el SEPD.

La cooperación con el Parlamento Europeo permitió llevar a cabo el mantenimiento del sitio del SEPD en Internet y añadirle nuevas funcionalidades.

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 SEPD es miembro de diversos comités interinstitucionales, como el Comité de Gestión del Seguro de Enfermedad (CGSE), el Comité de Preparación de las Cuestiones Estatutarias (CGCE), el Comité del Estatuto, el Grupo de trabajo interinstitucional/EAS, el Grupo de evaluación de la formación interinstitucional y el Comité Interinstitucional de Formación Lingüística. Esta participación contribuyó a que el SEPD tuviera una mayor proyección entre otras instituciones y propició el intercambio de buenas prácticas.

### 6.6.2. Normas internas

Continuó el proceso de adopción de nuevas normas internas y de nuevas disposiciones de aplicación del Estatuto de los funcionarios.

Dichas disposiciones, cuando afectan a temas en los que el SEPD cuenta con la asistencia de la Comisión, son similares a las adoptadas por esta, con ciertas adaptaciones para atender a las características particulares de la oficina del SEPD.

Con ocasión de la jornada de bienvenida, se hace entrega a los nuevos colegas de una guía administrativa que contiene todas las normas internas del SEPD e información sobre las especificidades de la institución. Ese documento se actualiza periódicamente.

Se adoptó una nueva guía para las misiones basada en la que aplica la Comisión.

En 2009 se adoptaron cinco importantes decisiones internas relativas al periodo de prueba en casos de licencia parental o familiar, licencia especial para madres lactantes y licencia especial por enfermedad grave de un hijo.

El SEPD es una institución relativamente joven que ha crecido rápidamente. En consecuencia, las normas y procedimientos que son convenientes durante los primeros años de actividad pueden resultar menos efectivos en el futuro en el marco de una estructura más grande y compleja. Por ello, las normas vigentes se someterán a una evaluación a los dos años de su adopción y podrán modificarse en consecuencia.

### 6.6.3. Gestión de los documentos

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 llevaron a cabo estudios dirigidos al establecimiento de un sistema apropiado de gestión de documentos y casos para el departamento de protección de datos.

# 7

# PRINCIPALES OBJETIVOS PARA 2010

En 2009 se dieron los primeros pasos hacia una evaluación estratégica de las funciones y tareas del SEPD, con el fin de establecer las principales líneas de desarrollo en los próximos cuatro años. Ello tendrá consecuencias en diferentes ámbitos, pero especialmente en el de la supervisión y la organización interna. La evolución en otros ámbitos será más gradual y se ceñirá a las líneas descritas en el presente Informe Anual.

Para 2010 se han seleccionado los siguientes objetivos principales. El año próximo se informará de los resultados que en ellos se alcancen.

- Apoyo a la red de RPD

El SEPD seguirá prestando un firme apoyo a los responsables de la protección de datos (RPD), especialmente en las agencias de reciente creación, y fomentando el intercambio de experiencias y buenas prácticas, incluida la posible adopción de normas profesionales, con el fin de consolidar su eficacia.

- Función de control previo

El SEPD insistirá en la aplicación de las recomendaciones de los dictámenes en materia de control previo y llevará un seguimiento adecuado. El control previo de las operaciones de tratamiento comunes a la mayor parte de las agencias seguirá recibiendo una atención especial.

- Orientación horizontal

El SEPD seguirá elaborando orientaciones sobre cuestiones pertinentes y poniéndolas a disposición general. Se publicarán directrices sobre videovigilancia, investigaciones administrativas y procedimientos disciplinarios, así como modalidades de aplicación relativas a las tareas y funciones de los responsables de protección de datos.

- Política de inspecciones

El SEPD publicará una política global de control del cumplimiento y la aplicación de las normas de protección de datos en las instituciones y organismos. En este sentido se aplicarán todos los medios necesarios para medir y garantizar el cumplimiento de las normas de protección de datos y fomentar la responsabilidad institucional en la buena gestión de los datos.

- Ámbito de consulta

El SEPD seguirá publicando puntualmente dictámenes o comentarios sobre las propuestas de nueva legislación y realizará un seguimiento adecuado en todos los ámbitos pertinentes. Se prestará una atención especial al plan de acción para la aplicación del Programa de Estocolmo.

- Revisión del marco jurídico

El SEPD dará prioridad al desarrollo de un marco normativo completo de la protección de datos que cubra todos los ámbitos de la política de la UE y garantice una protección eficaz en la práctica, además de contribuir al debate público cuando sea necesario y oportuno.

- Agenda Digital

El SEPD prestará una atención especial a la Agenda Digital de la Comisión en todos los ámbitos que tengan un impacto obvio en la protección de datos. Se apoyará firmemente el principio de intimidad mediante el diseño y su aplicación práctica.

- Actividades de información

El SEPD seguirá mejorando sus herramientas de información en línea (sitio en Internet y boletín electrónico) a fin de responder mejor a las peticiones de los visitantes. Se elaborarán nuevas publicaciones temáticas (*fact sheets*).

- Organización interna

El SEPD revisará la estructura organizativa de su Secretaría con el fin de garantizar una ejecución más efectiva y eficaz de las diferentes funciones y tareas. Las líneas generales de la nueva estructura se publicarán en el sitio en Internet.

- Gestión de recursos

El SEPD seguirá realizando actividades relacionadas con la gestión de los recursos financieros y humanos y potenciará otros procesos de trabajo internos. Se prestará una atención especial a la necesidad de espacio adicional en la oficina y al desarrollo de un sistema de gestión de asuntos.

# Anexo A. Marco normativo

El artículo 286 del Tratado CE, adoptado en 1997 como parte del Tratado de Amsterdam, 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).

En virtud 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 lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, que entró en vigor en 2001 ([22]). Este Reglamento dispone también normas apropiadas para las instituciones y órganos en línea con las dos Directivas.

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 base jurídica 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 se aplica al «tratamiento de datos personales por parte de todas las instituciones y organismos comunitarios, en la

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

medida en que dicho tratamiento se lleve a cabo para el ejercicio de actividades que pertenecen al ámbito de aplicación del Derecho comunitario». Desde la entrada en vigor del Tratado de Lisboa, esto significa que las instituciones y organismos de la UE que se consideraban «instituciones y organismos comunitarios» están sujetos a las funciones y competencias de supervisión del SEPD. No está claro si el Reglamento tiene un ámbito de aplicación más amplio y se extiende a partes del antiguo tercer pilar.

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 los interesados, 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 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 tarea 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 comunitarios cuentan ya con estos RPD, y algunos de ellos llevan trabajando ya varios 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 muy importante y muy apreciada de colaboración 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 da 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 aplicarse a nivel nacional o incorporarse al Derecho nacional. Esta es una función estratégica que permite al SEPD examinar anticipadamente la incidencia de dichas medidas en la intimidad y debatir las posibles alternativas, también en el tercer pilar (cooperación policial y judicial en materia penal). El seguimiento de las novedades que puedan repercutir en la protección de datos personales y la intervención en asuntos presentados ante el Tribunal de Justicia son también funciones de importancia. Estas actividades consultivas del SEPD se abordan con mayor detenimiento en el capítulo 3 del presente informe.

En la misma línea se encuentra el deber de cooperar con las autoridades nacionales de supervisión y 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 la oportunidad de contribuir a ese nivel. La cooperación con organismos de supervisión del tercer pilar le permite observar las novedades que se producen en ese contexto y contribuir a un marco más coherente y constante de protección de 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 velará por 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 garantizará y supervisará 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 hechos nuevos de interés, en la medida en que tengan repercusiones sobre la protección de datos personales, en particular de la evolución de 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 |
| ACCP | Agencia Comunitaria de Control de la Pesca |
| AESA | Autoridad Europea de Seguridad Alimentaria |
| AESM | Agencia Europea de Seguridad Marítima |
| ANS | Autoridad Nacional de Seguridad |
| APD | Autoridad de protección de datos |
| ARES | *Advanced Records System* (sistema avanzado de ficheros) |
| BCE | Banco Central Europeo |
| BEI | Banco Europeo de Inversiones |
| CCI | Centro Común de Investigación |
| CCTV | *Closed circuit television* (televisión en circuito cerrado) |
| CDR | Comité de las Regiones |
| CDT | Centro de Traducción de los Órganos de la Unión Europea |
| CE | Comunidades Europeas |
| Cedefop | Centro Europeo para el Desarrollo de la Formación Profesional |
| CEDH | Convenio Europeo de Derechos Humanos |
| CES | Comité Económico y Social Europeo |
| CIG | Conferencia Intergubernamental |
| CML | Centro de Medicina Laboral |
| CPD | Coordinador de Protección de Datos (solo en la Comisión Europea) |
| ECRIS | Sistema Europeo de Información de Antecedentes Penales |
| EAS | Escuela Europea de Administración |
| EMA | Agencia Europea de Medicamentos |
| ENISA | Agencia Europea de Seguridad de las Redes y de la Información |
| EPSO | Oficina Europea de Selección de Personal |
| ETF | Fundación Europea de Formación |
| Eurofound | Fundación Europea para la Mejora de las Condiciones de Vida y de Trabajo |
| FIDE | Fichero de identificación de los expedientes de investigaciones aduaneras |
| FRA | Agencia de Derechos Fundamentales de la Unión Europea |
| G 29 | Grupo de trabajo del artículo 29 |
| GPJ | Grupo de trabajo sobre policía y justicia |
| I+D | Investigación y desarrollo |
| IMI | Sistema de Información del Mercado Interior |
| IMS | Servicio de Gestión de la Identidad |
| OAMI | Oficina de Armonización del Mercado Interior |
| OCDE | Organización de Cooperación y Desarrollo Económicos |
| OCVV | Oficina Comunitaria de Variedades Vegetales |
| OEDT | Observatorio Europeo de las Drogas y las Toxicomanías |
| OLAF | Oficina Europea de Lucha contra el Fraude |
| PNR | Registro de nombres de los pasajeros |
| RFID | Identificación por radiofrecuencia |
| RPD | Responsable de Protección de Datos |

| | |
|---|---|
| SAI | Servicio de Auditoría Interna |
| SAR | Sistema de Alerta Rápida |
| SCPC | Sistema de Cooperación en Materia de Protección de los Consumidores |
| SIA | Sistema de Información Aduanero |
| SIR | Sistemas Informatizado de Reserva |
| SIS | Sistema de Información de Schengen |
| SWIFT | Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales |
| TCE | Tribunal de Cuentas Europeo |
| Tercer pilar | Cooperación policial y judicial en materia penal |
| TFUE | Tratado de Funcionamiento de la Unión Europea |
| TIM | *Time management system* (sistema de gestión del tiempo) |
| TJUE | Tribunal de Justicia de la Unión Europea |
| UE | Unión Europea |
| VIS | Sistema de Información de Visados |

# 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 | Jan KILB | Data-Protection@eca.europa.eu |
| Comité Económico y Social Europeo (CESE) | Maria ARSENE | Data.Protection@eesc.europa.eu |
| Comité de las Regiones (CDR) | Petra CANDELLIER | 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) | Giuseppina LAURITANO | Giuseppina.Lauritano@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 (EMA) | Vincenzo SALVATORE | Data.Protection@emea.europa.eu |
| Oficina Comunitaria de Variedades Vegetales (OCVV) | Véronique DOREAU | Doreau@cpvo.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@emcdda.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) | Terry TAYLOR | Taylor@osha.europa.eu |
| Agencia Comunitaria de Control de la Pesca (ACCP) | Clara FERNÁNDEZ/Rieke ARNDT | cfca-dpo@cfca.europa.eu |
| Autoridad de Supervisión del GNSS Europeo (GSA) | Triinu VOLMER | Triinu.Volmer@gsa.europa.eu |
| Agencia Ferroviaria Europea (AFE) | Guido STÄRKLE | 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 de los Estados Miembros de la Unión Europea (Frontex) | Sakari VUORENSOLA | Sakari.Vuorensola@frontex.europa.eu |
| Agencia Europea de Seguridad Aérea (AESA) | Francesca PAVESI | Francesca.Pavesi@easa.europa.eu |
| Agencia Ejecutiva de Competitividad e Innovación (EACI) | Elena FIERRO SEDANO | Elena.Fierro-Sedano@ec.europa.eu |
| Agencia Ejecutiva de la Red Transeuropea de Transporte (TEN-T EA) | Elisa DALLE MOLLE | Elisa.Dalle-Molle@ec.europa.eu |
| Agencia Europea de Sustancias y Preparados Químicos (ECHA) | Minna HEIKKILA | Minna.Heikkila@echa.europa.eu |

>>>

| ORGANIZACIÓN | NOMBRE | CORREO ELECTRÓNICO |
|---|---|---|
| Agencia Ejecutiva del Consejo Europeo de Investigación (ERCEA) | Donatella PIATTO | Donatella.Piatto@ec.europa.eu |
| Agencia Ejecutiva de Investigación (REA) | Evangelos TSAVALOPOULOS | Evangelos.Tsavalopoulos@ec.europa.eu |
| Empresa Común Fusion for Energy | Radoslav HANAK | Radoslav.Hanak@f4e.europa.eu |
| Empresa Común SESAR (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 IMI | Estefania RIBEIRO | Estefania.Ribeiro@imi.europa.eu |
| Empresa Común Fuel Cells & Hydrogen | Nicolas BRAHY | Nicolas.Brahy@fch.europa.eu |

# Anexo E. Lista de dictámenes de control previo

**Procedimientos de evaluación. EMA**

Dictamen de 18 de diciembre de 2009 sobre los procedimientos de evaluación de los resultados de la Agencia Europea de Medicamentos (asunto 2007-421)

**Puestos individuales. Parlamento**

Dictamen de 17 de diciembre de 2009 sobre la notificación de un control previo relativo a los puestos individuales (asunto 2009-650)

**Procedimiento de informe. Consejo**

Dictamen de 15 de diciembre de 2009 sobre la notificación de un control previo relativo al procedimiento de informe de los funcionarios del Consejo (asunto 2009-042)

**Selección del director del Instituto Europeo de la Igualdad de Género. Parlamento**

Dictamen de 8 de diciembre de 2009 sobre la notificación de un control previo relativo a la selección del director del Instituto Europeo de la Igualdad de Género (asunto 2008-785)

**Sistema de gestión de la calidad de los datos de EudraVigilance. EMA**

Dictamen recogido en una carta de 7 de diciembre de 2009 sobre la notificación de un control previo relativo al sistema de gestión de la calidad de los datos de EudraVigilance (asunto 2009-740)

**Gestión de licencias. EFSA**

Dictamen de 1 de diciembre de 2009 sobre la notificación de un control previo relativo a la gestión de las licencias en la EFSA (asunto 2009-455)

**Movilidad interna. Banco Europeo de Inversiones**

Dictamen de 18 de noviembre de 2009 sobre la notificación de un control previo relativo a la movilidad interna (asunto 2009-253)

**Comprobación de los fichajes y flexibilización del horario laboral. Consejo**

Dictamen de 12 de noviembre de 2009 sobre la notificación de un control previo relativo a la comprobación de los fichajes en caso de flexibilización del horario laboral en relación con los datos sobre el acceso físico (asunto 2009-477)

**Investigaciones administrativas y procedimientos disciplinarios. CESE**

Dictamen de 9 de noviembre de 2009 sobre la notificación de un control previo relativo a las investigaciones administrativas y los procedimientos disciplinarios internos en el CESE (asunto 2008-569)

**Evaluación de 360 grados de la inteligencia emocional de la EAS. Comisión**

Dictamen de 30 de octubre de 2009 sobre la notificación de un control previo relativo a la EAS (Escuela Europea de Administración).. Evaluación de 360 grados de la inteligencia emocional (asunto 2009-100)

**Seguros de los diputados. Parlamento**

Dictamen de 27 de octubre de 2009 sobre la notificación de un control previo relativo a los seguros de los diputados (asunto 2009-434)

**«e-Performance». Banco Europeo de Inversiones**

Dictamen de 19 de octubre de 2009 sobre la notificación de un control previo relativo a «e-Performance» (asunto 2008-379)

**Uso de las listas de reserva. Tribunal de Cuentas**

Dictamen de 5 de octubre de 2009 sobre la notificación de un control previo relativo al uso de las listas de reserva y de aptitud para la contratación de funcionarios y agentes temporales y contractuales (asunto 2008-433)

**Gestión del Centro Infantil Polivalente. Comisión**

Dictamen de 29 de septiembre de 2009 sobre la notificación de un control previo relativo a la gestión del Centro Infantil Polivalente. Guardería y Centro de Estudios: sistema de información Loustic e historiales médicos (Luxemburgo) (asunto 2009-089)

**Sistema de apoyo a la seguridad. Parlamento**

Dictamen de 29 de septiembre de 2009 sobre la notificación de un control previo relativo al Sistema de Apoyo a la Seguridad (asunto 2009-225)

**Selección de personal permanente y temporal. Consejo**

Dictamen de 28 de septiembre de 2009 sobre la notificación de un control previo relativo a la selección de personal permanente y temporal en la Secretaría General del Consejo de la Unión Europea (asunto 2009-197)

**Selección y contratación de agentes temporales y contractuales. FRA**

Dictamen de 24 de septiembre de 2009 sobre la notificación de un control previo relativo a la selección y la contratación de los agentes temporales y contractuales de la FRA (asunto 2008-589)

**Consejo de Disciplina. Comisión**

Dictamen de 21 de septiembre de 2009 sobre la notificación de un control previo relativo al Consejo de Disciplina (asunto 2009-087)

**Seguro de accidentes. Consejo**

Dictamen de 14 de septiembre de 2009 sobre la notificación de un control previo relativo al tratamiento de datos en relación con el seguro de accidentes (asunto 2009-257)

**Base de datos EudraVigilance. EMA**

Dictamen de 7 de septiembre de 2009 sobre la notificación de un control previo relativo a la base de datos EudraVigilance (asunto 2008-402)

**Evaluación del Presidente y el Vicepresidente. OCVV**

Dictamen de 28 de julio de 2009 sobre la notificación de un control previo relativo a la evaluación del Presidente y el Vicepresidente de la OCVV (asuntos 2009-355 y 2009-356)

**Tiempo parcial. Comité de las Regiones**

Dictamen de 27 de julio de 2009 sobre la notificación de un control previo relativo a las solicitudes de ejercicio de la actividad a tiempo parcial (asunto 2009-396)

**Tiempo parcial. Comité Económico y Social**

Dictamen de 24 de julio de 2009 sobre la notificación de un control previo relativo a las solicitudes de ejercicio de la actividad a tiempo parcial (asunto 2009-322)

**Contratación. Tribunal de Cuentas Europeo**

Dictamen de 23 de julio de 2009 sobre la notificación de un control previo relativo a los procedimientos de selección para la contratación de funcionarios, agentes temporales y agentes contractuales (asunto 2008-313)

**Audiciones de los Comisarios designados. Parlamento**

Dictamen de 3 de julio de 2009 sobre la notificación de un control previo relativo al tratamiento de los datos personales en las audiciones de los Comisarios designados (asunto 2009-0332)

**Evaluación de la formación. Banco Central Europeo**

Dictamen de 1 de julio de 2009 sobre la notificación de un control previo relativo a la evaluación de la formación (asunto 2009-220)

**Procedimientos de licitación. CESE**

Dictamen de 30 de junio de 2009 relativo a los procedimientos de licitación y la gestión de los contratos (asunto 2009-323)

**Gestión del tiempo y de las ausencias. ECDC**

Dictamen de 22 de junio de 2009 sobre la notificación de un control previo relativo a la gestión del tiempo y de las ausencias (asunto 2009-072)

**Selección de mandos medios y asesores. Comisión**

Dictamen de 17 de junio de 2009 sobre la notificación de un control previo relativo a la selección de mandos medios y asesores en la Comisión (asunto 2008-751)

**Reclutamiento de personal contractual. Comité de las Regiones**

Dictamen de 16 de junio de 2009 sobre la notificación de un control previo relativo al reclutamiento de personal contractual (asunto 2008-696)

**Contratación de funcionarios. Comité de las Regiones**

Dictamen de 16 de junio de 2009 sobre la notificación de un control previo relativo a la contratación de funcionarios (asunto 2008-694)

**Contratación de personal temporal. Comité de las Regiones**

Dictamen de 16 de junio de 2009 sobre la notificación de un control previo relativo a la contratación de personal temporal (asunto 2008-695)

**Documentos facilitados durante la contratación. Comisión**

Dictamen de 5 de junio de 2009 sobre la notificación de un control previo relativo a los documentos facilitados durante la contratación (asunto 2008-755)

**Declaraciones de interés específicas. EFSA**

Dictamen de 5 de junio de 2009 sobre la notificación de un control previo relativo al tratamiento de las declaraciones de interés anuales y específicas (asunto 2008-737)

**Administración de periodos de prácticas. Comisión**

Dictamen de 5 de junio de 2009 sobre la notificación de un control previo relativo a la solicitud de administración de periodos de prácticas (asunto 2008-485)

**Seguridad en el trabajo en el CCI. Comisión**

Dictamen de 20 de mayo de 2009 sobre la notificación de un control previo relativo a la gestión de la seguridad en el trabajo en el Instituto de Sanidad y Protección de los Consumidores del Centro Común de Investigación de Ispra (asunto 2008-541)

**Centro de Datos de la Dirección General de Empresa. Comisión**

Dictamen de 19 de mayo de 2009 sobre la notificación de un control previo relativo al tratamiento de datos personales en el Centro de Datos de la Dirección General de Empresa (asunto 2008-487)

**Prevención del acoso. Parlamento**

Dictamen de 19 de mayo de 2009 sobre la notificación de un control previo relativo a la prevención del acoso (asunto 2008-477)

**Solicitudes de prácticas y reclutamiento. EMA**

Dictamen de 18 de mayo de 2009 sobre la notificación de un control previo relativo a las solicitudes de prácticas y el reclutamiento (asunto 2008-730)

**Procedimiento de promoción y reclasificación. CDT**

Dictamen de 18 de mayo de 2009 sobre la notificación de un control previo relativo al procedimiento de promoción y reclasificación (asunto 2009-018)

**Servicio de Mediación. Comisión**

Dictamen de 18 de mayo de 2009 sobre la notificación de un control previo relativo al Servicio de mediación de la Comisión Europea (asunto 2009-010)

**TFlow y Profil. Parlamento**

Dictamen de 8 de mayo de 2009 sobre la notificación de un control previo relativo a la operación de tratamiento TFlow y Profil (asunto 2009-069)

**Procedimientos de contratación de personal en ciertas agencias comunitarias**

Dictamen de 7 de mayo de 2009 sobre las notificaciones de controles previos relativos a los procedimientos de contratación de personal de ciertas agencias comunitarias (asunto 2009-287)

**Evaluación e informes de prácticas. EFSA**

Dictamen de 6 de mayo de 2009 sobre la notificación de un control previo relativo a las evaluaciones e informes de prácticas (asunto 2009-030)

**Horario flexible. Tribunal de Justicia**

Dictamen de 6 de mayo de 2009 sobre la notificación de un control previo del Tribunal de Justicia en relación con el horario flexible (asunto 2007-437)

**Diálogo anual. ETF**

Dictamen de 4 de mayo de 2009 sobre la notificación de un control previo relativo al diálogo anual de la ETF (asunto 2009-168)

**Registro vocal del CCI-IE. Comisión**

Dictamen de 29 de abril de 2009 sobre la notificación de un control previo relativo al registro vocal del Instituto de la Energía del Centro Común de Investigación (JRC-IE) de Petten (asunto 2008-014)

**Datos médicos de los niños que asisten a las guarderías interinstitucionales. Comisión**

Dictamen de 27 de abril de 2009 sobre la notificación de un control previo relativo la gestión de los datos médicos de los niños que asisten a las guarderías interinstitucionales gestionadas por la OIB (Oficina de Estructuras y Logistica de la Comisión Europea, Bruselas) (asunto 2009-088)

**Procedimientos de selección de los expertos nacionales en comisión de servicios. FRA**

Dictamen de 27 de abril de 2009 sobre la notificación de un control previo relativo a los procedimientos de selección de los expertos nacionales en comisión de servicios (asunto 2008-747)

**Jóvenes expertos en delegación. Comisión**

Dictamen de 22 de abril de 2009 sobre la notificación de un control previo relativo a los jóvenes expertos en delegación (asunto 2008-754)

**Jubilación anticipada. Comité Económico y Social Europeo**

Dictamen de 1 de abril de 2009 sobre la notificación de un control previo relativo al ejercicio anual de jubilación anticipada sin reducción de los derechos de pensión (asunto 2008-719)

**Becarios estructurales. Comisión**

Dictamen de 30 de marzo de 2009 sobre la notificación de un control previo relativo a los becarios estructurales (asunto 2008-760)

**Suspensión de la inmunidad en las actuaciones judiciales y de la inviolabilidad de los locales y archivos de la Comisión. Comisión**

Dictamen de 25 de marzo de 2009 sobre la notificación de un control previo relativo al tratamiento de las peticiones de suspensión de la inmunidad en las actuaciones judiciales y la inviolabilidad de los locales y archivos de la Comisión (asunto 2008-645)

**Gestión de la información remitida por la OLAF. Comisión**

Dictamen de 23 de marzo de 2009 sobre la notificación de un control previo relativo la gestión de la información remitida por la OLAF en el marco del memorándum de acuerdo (asunto 2009-011)

**Procedimiento de fin de prácticas. Comisión**

Dictamen de 10 de marzo de 2009 sobre la notificación de un control previo relativo al fin del periodo de prácticas (asunto 2008-720)

**Horario flexible. ETF**

Dictamen de 26 de febrero de 2009 sobre la notificación de un control previo relativo al procedimiento de la ETF. Flexibilización del horario laboral (asunto 2008-697)

**Reintegración y orientación profesional. Consejo**

Dictamen de 23 de febrero de 2009 sobre la notificación de un control previo relativo al grupo de reintegración y orientación profesional (asunto 2008-746)

**Agentes temporales. Oficina Comunitaria de Variedades Vegetales**

Dictamen de 20 de febrero de 2009 sobre la notificación de un control previo relativo a la contratación y el recurso a agentes temporales (asunto 2008-315)

**Jubilación anticipada. Parlamento**

Dictamen de 18 de febrero de 2009 sobre la notificación de un control previo relativo al procedimiento de jubilación anticipada sin reducción de los derechos de pensión (asunto 2008-748)

**Herramienta de verificación y concordancia ART. Tribunal de Cuentas Europeo**

Dictamen de 9 de febrero de 2009 sobre la notificación de un control previo relativo a la herramienta de verificación y concordancia ART (asunto 2008-239)

**Amenazas contra los intereses de la Comisión en los ámbitos de la contrainteligencia y la lucha contra el terrorismo. Comisión**

Dictamen de 26 de enero de 2009 sobre la notificación de un control previo relativo a las amenazas contra los intereses de la Comisión en los ámbitos de la contrainteligencia y la lucha contra el terrorismo (asunto 2008-440)

**Capacidad de trabajar en una tercera lengua antes de la primera promoción. Parlamento**

Dictamen de 21 de enero de 2009 sobre la notificación de un control previo relativo a la evaluación de la capacidad del personal de trabajar en una tercera lengua antes de la primera promoción (asunto 2008-690)

**Informe de prácticas. Parlamento**

Dictamen de 21 de enero de 2009 sobre la notificación de un control previo relativo al informe del periodo de prácticas (asunto 2008-604)

**Comité de Invalidez. Consejo**

Dictamen de 16 de enero de 2009 sobre la notificación de un control previo relativo al procedimiento del Comité de Invalidez (asunto 2008-626)

**Formación SYSLOG. Comisión**

Dictamen de 16 de enero de 2009 sobre la notificación de un control previo relativo a la gestión de la formación central y local Syslog (asunto 2008-481)

**Gestión de la guardería. Consejo**

Dictamen de 15 de enero de 2009 sobre la notificación de un control previo relativo a la gestión y la facturación de la guardería de la Secretaría General del Consejo (asunto 2007-441)

**Jubilación anticipada. Tribunal de Cuentas Europeo**

Dictamen de 9 de enero de 2009 sobre la notificación de un control previo relativo al ejercicio anual de jubilación anticipada sin reducción de los derechos de pensión (asunto 2008-552)

# Anexo F. Lista de dictámenes sobre propuestas legislativas

**Medidas restrictivas respecto de Somalia, entre otros**

Dictamen de 16 de diciembre de 2009 relativo a varias propuestas legislativas que imponen determinadas medidas restrictivas específicas respecto de Somalia, Zimbabue, la República Democrática de Corea y Guinea

**Agencia para la Gestión Operativa de Sistemas Informáticos a gran Escala en el Ámbito de la Libertad, la Seguridad y la Justicia**

Dictamen de 7 de diciembre de 2009 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establece una Agencia para la Gestión Operativa de Sistemas Informáticos a gran Escala en el Ámbito de la Libertad, la Seguridad y la Justicia, y sobre la propuesta de Decisión del Consejo por la que se asignan a la Agencia las tareas relativas a la gestión del SIS II y el VIS en aplicación del título VI del Tratado UE

**Lucha contra el fraude en el ámbito del impuesto sobre el valor añadido**

Dictamen de 30 de octubre de 2009 sobre la propuesta de Reglamento del Consejo relativo a la cooperación administrativa y la lucha contra el fraude en el ámbito del impuesto sobre el valor añadido (refundición)

**Acceso de las fuerzas de seguridad a Eurodac**

Dictamen de 7 de octubre de 2009 sobre las propuestas relativas al acceso de las fuerzas de seguridad a Eurodac

**Medidas restrictivas respecto de Al-Qaida y los talibanes**

Dictamen de 28 de julio de 2009 sobre la propuesta de Reglamento del Consejo por el que se modifica el Reglamento (CE) nº 881/2002 por el que se imponen determinadas medidas restrictivas específicas dirigidas contra determinadas personas y entidades asociadas con Usamah bin Ladin, la red Al-Qaida y los talibanes, DO C 276, 17.11.2009, p. 1

**Sistemas de transporte inteligentes**

Dictamen de 22 de julio de 2009 sobre la Comunicación de la Comisión relativa a un plan de acción para el despliegue de sistemas de transporte inteligentes en Europa y a la propuesta que lo acompaña de Directiva del Parlamento Europeo y del Consejo por la que se establece el marco para el despliegue de los sistemas de transporte inteligentes en el sector del transporte por carretera y para sus interfaces con otros modos de transporte

**Programa de Estocolmo. Un espacio de libertad, seguridad y justicia al servicio de los ciudadanos**

Dictamen de 10 de julio de 2009 sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo relativa a un espacio de libertad, seguridad y justicia al servicio de los ciudadanos, DO C 276, 17.9.2009, p. 8

**Farmacovigilancia**

Dictamen de 22 de abril de 2009 sobre las propuestas de Reglamento y de Directiva sobre farmacovigilancia, DO C 229, 23.9.2009, p. 19

**Utilización de la tecnología de la información a efectos aduaneros**

Dictamen de 20 de abril de 2009 sobre la iniciativa de la República Francesa relativa a la Decisión del Consejo sobre la utilización de la tecnología de la información a efectos aduaneros, DO C 229, 23.9.2009, p. 12

**Obtención de información estadística por el Banco Central Europeo**

Dictamen de 8 de abril de 2009 sobre la recomendación de Reglamento del Consejo que modifica el Reglamento (CE) nº 2533/98 del Consejo, de 23 de noviembre de 1998, sobre la obtención de información estadística por el Banco Central Europeo, DO C 192, 15.8.2009, p. 1

**Trasplante de órganos**

Dictamen de 5 de marzo de 2009 relativo a la propuesta de Directiva del Parlamento Europeo y del Consejo sobre normas de calidad y seguridad de los órganos humanos destinados a trasplantes, DO C 192, 15.8.2009, p. 6

**Política pesquera común**

Dictamen de 4 de marzo de 2009 sobre la propuesta de Reglamento del Consejo por el que se establece un régimen de control comunitario para garantizar el cumplimiento de las normas de la política pesquera común, DO C 151, 3.7.2009, p. 11

**Asilo: Reglamento Eurodac**

Dictamen de 18 de febrero de 2009 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la creación del sistema Eurodac para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento (CE) nº […/…] (por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida) [COM(2008) 825], DO C 229, 23.9.2009, p. 6

**Asilo: Reglamento de Dublín**

Dictamen de 18 de febrero de 2009 relativo a la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida [COM(2008) 820 final], DO 229, 23.9.2009, p. 1

**Reservas mínimas de petróleo crudo y productos petrolíferos**

Dictamen de 3 de febrero de 2009 sobre la propuesta de Directiva del Consejo por la que se obliga a los Estados miembros a mantener un nivel mínimo de reservas de petróleo crudo y/o productos petrolíferos, DO C 128, 6.6.2009, p. 42

**Segundo dictamen sobre la privacidad en las comunicaciones electrónicas**

Segundo dictamen de 9 de enero de 2009 sobre la revisión de la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), DO C 128, 6.6.2009, p. 28

# Anexo G. Discursos del Supervisor y del Supervisor Adjunto

El Supervisor y el Supervisor Adjunto siguieron dedicando un tiempo y un esfuerzo importantes a la explicación de su misión y a la sensibilización sobre la protección de datos en general, así como sobre diversos problemas específicos, en discursos y otras contribuciones similares para diversas instituciones y en distintos Estados miembros a lo largo del año.

El Supervisor compareció frecuentemente en la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo o en acontecimientos conexos. El 5 de marzo, habló en una audición sobre los retos que se plantean en relación con los derechos fundamentales en Internet. El 16 de abril presentó, junto con el Supervisor Adjunto, las líneas generales del Informe Anual 2008 del SEPD. El 27 de abril habló sobre la revisión en curso del Reglamento (CE) nº 1049/2001 relativo al acceso del público a los documentos. El 22 de julio presentó el dictamen del SEPD sobre la Comunicación de la Comisión relativa al Programa de Estocolmo. El 3 de septiembre habló en la reunión conjunta de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior y de la Comisión de Asuntos Económicos y Monetarios sobre el acuerdo provisional entre la UE y los EE.UU. acerca de SWIFT. El 29 de septiembre, el Supervisor Adjunto habló en la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del uso de la tecnología de la información a efectos aduaneros. El 30 de marzo habló en la Comisión de Medio Ambiente, Salud Pública y Seguridad Alimentaria del Parlamento Europeo de cuestiones sobre protección de datos en relación con la propuesta de Directiva sobre el trasplante de órganos.

El SEPD también compareció en otras reuniones con el Parlamento Europeo. El 22 de enero de enero habló en la Comisión de Transportes y Turismo en una audición sobre sistemas de transporte inteligentes. El 28 de enero contribuyó a la celebración del Día de la Protección de Datos en el Parlamento. El 10 de febrero presentó en la Comisión de Medio Ambiente, Salud Pública y Seguridad Alimentaria el dictamen del SEPD sobre los derechos de los pacientes en la asistencia sanitaria transfronteriza. El 29 de septiembre habló en una reunión de la European Privacy Association en cooperación con diferentes miembros del Parlamento Europeo.

El 26 de enero, el Supervisor contribuyó a la celebración del Día de la Protección de Datos en la Representación permanente de Polonia en Bruselas. El 5 de marzo habló en el Consejo de la revisión del Reglamento (CE) nº 1049/2001 relativo al acceso del público a los documentos. El 23 de marzo habló de las prioridades de supervisión y consulta en el Grupo de trabajo sobre protección de datos del Consejo. El 6 de julio pronunció un discurso sobre la necesidad de una Estrategia de gestión de la información de la UE en la primera reunión del Grupo de trabajo sobre el intercambio de información del Consejo celebrada durante la Presidencia sueca. El 15 de julio, el Supervisor Adjunto habló en el Grupo de trabajo del Consejo de la e-Justicia y la interconexión de los registros de insolvencia. El 7 de diciembre, el Supervisor asistió a la audición de la Comisión de Protección de Datos y Actuación Policial de la Cámara de los Comunes en la Representación permanente del Reino Unido en Bruselas. El 28 de octubre, el Supervisor Adjunto pronunció un discurso en el Parlamento del Estado de Berlín en la celebración del trigésimo aniversario de la protección de datos y el décimo aniversario de la libertad de información en Alemania.

El 26 de marzo, el Supervisor Adjunto habló en una audición del Comité Económico y Social Europeo del despliegue de sistemas de transporte inteligentes en Ostrava. El 28 de abril, el Supervisor presentó diversas cuestiones estratégicas sobre protección de datos en una reunión de Riseptis, el grupo consultivo de la Comisión en materia de investigación e innovación para la seguridad, la intimidad y la fiabilidad en la sociedad de la información. El 12 de mayo habló de cuestiones relacionadas con la protección de datos en una reunión del Comité SIS-VIS. El 14 de mayo pronunció un discurso en la Conferencia de la Comisión acerca de la evaluación de la Directiva sobre conservación de datos. El 20 de mayo, el Supervisor y el Supervisor Adjunto hablaron en la Conferencia de la Comisión sobre Protección de Datos. El 14 de septiembre, el Supervisor Adjunto habló de las redes sociales en Bruselas, en la audición del Comité Económico y Social Europeo. El 16 de septiembre, el Supervisor habló en una conferencia organizada por la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) en Heraklion. El 30 de septiembre, el Supervisor Adjunto habló en el Taller del SEPD sobre videovigilancia en las instituciones y órganos comunitarios. El 13 de mayo habló de la protección de datos en las instituciones y órganos comunitarios en la 12ª reunión de la red jurídica interagencias (IALN), organizada por la Oficina de Armonización del Mercado Interior (OAMI) en Alicante. El

4 de abril habló en la Conferencia Internacional sobre Libertad de Información y Protección de Datos en Viareggio. El 23 de octubre, el Supervisor y el Supervisor Adjunto contribuyeron a un seminario sobre violación de datos organizado por el SEPD en cooperación con la ENISA.

El 16 de enero, el Supervisor habló en la Universidad de Friburgo, Suiza, de la protección de datos en el contexto de Schengen y Dublín. El 17 de enero intervino en la Conferencia anual sobre Informática, Privacidad y Protección de Datos en Bruselas. El 27 de enero participó en una conferencia sobre protección de datos y actuación policial en el Instituto Clingendael en La Haya. El 11 de febrero habló en una conferencia de la Trans European Policy Studies Association (TEPSA), en Bruselas, de los retos a los que actualmente se enfrenta la protección de datos. El 19 de febrero asistió a la Conferencia sobre Sanidad Electrónica 2009 en Praga. El 27 de febrero asistió a un Consejo consultivo sobre administración electrónica en La Haya. El 19 de marzo participó en conferencia del PES sobre Internet en Atenas. El 26 de marzo habló en una conferencia de la British Bankers' Association en Londres. El 3 de noviembre, el Supervisor Adjunto habló en un taller de la fundación española FIDE (Fundación para la Investigación sobre el Derecho y la Empresa), en Madrid, de la evolución reciente de la protección de datos a nivel europeo. El 14 de diciembre pronunció un discurso en la Universidad de Florencia sobre la protección de datos y los códigos de conducta, y el 17 de abril habló en la Alma Graduate School de Bolonia de la supervisión electrónica en el lugar de trabajo.

El 28 de abril, el Supervisor Adjunto pronunció un discurso sobre privacidad y seguridad en el Centro de Estudios de Política Europea de Bruselas. El 8 de mayo, el Supervisor contribuyó a una conferencia sobre Internet de los objetos en Bruselas. El 18 de mayo habló en Bruselas en la Conferencia sobre la Protección de Datos en la UE. El 21 de mayo pronunció un discurso en la Conferencia de Primavera de la Comisión Austríaca de Juristas en Weissenbach am Attersee. El 8 de junio habló en la 11ª Conferencia sobre la Protección de Datos y Seguridad de los Datos en Berlín. El 19 de junio, el Supervisor Adjunto intervino en una conferencia de poderes judiciales sobre vigilancia y protección de los derechos fundamentales celebrada en Viena. El 23 de junio (privacidad y seguridad globales) y el 10 de septiembre (asuntos sobre protección de datos presentados ante los tribunales europeos) habló en dos conferencias organizadas para jueces y fiscales por el Consejo Superior de la Magistratura Italiana.

El 8 se septiembre, el Supervisor pronunció un discurso en el Seminario «Transparencia y lenguaje jurídico claro en la UE», organizado en Estocolmo por la Presidencia sueca. El 21 de septiembre habló en una conferencia sobre gobierno y tecnologías de la información en Amberes. El 24 de septiembre realizó una visita a la autoridad eslovaca de protección de datos en Bratislava. El 8 de octubre habló en el 35º aniversario de la sección neerlandesa de la Comisión Internacional de Juristas (NJCM) en La Haya. Los días 8 y 9 de octubre, el Supervisor y el Supervisor Adjunto participaron en un taller sobre protección de datos en procesos penales en Estrasburgo. El 13 de octubre, el Supervisor habló en una reunión del Grupo de trabajo de seguridad de la información y privacidad de la OCDE en París. El 14 de octubre contribuyó a una conferencia sobre seguridad y privacidad en Oslo. El 26 de octubre habló en una comida de la Asociación Belgo-Neerlandesa (BENEV) en Bruselas. El 28 de octubre habló en una conferencia de Missing Children Europa en Bruselas.

El 2 de noviembre, el Supervisor habló en un taller de intimidad mediante el diseño en Madrid. El 3 de noviembre dio una conferencia sobre la Sociedad Civil en Madrid. El 12 de noviembre habló en un seminario sobre el Programa de Estocolmo organizado por la Fundación Robert Schuman en Bruselas, y en una conferencia de la BEUC, también en Bruselas, sobre la Vida Privada de los Consumidores. El 20 de noviembre pronunció un discurso en Amsterdam en la Conferencia Nacional Neerlandesa sobre Privacidad. El 2 de diciembre habló sobre sanidad electrónica en una conferencia organizada en Bruselas por Amigos de Europa. El 3 de diciembre habló sobre sistemas de transporte inteligentes en la 9ª Conferencia de Transitarios en Bruselas.

El Supervisor y el Supervisor Adjunto intervinieron también en las relaciones transatlánticas. El 12 de marzo, el Supervisor asistió a la Cumbre de la Privacidad de la IAPP en Washington DC. El 26 de mayo, el Supervisor Adjunto pronunció un discurso en el I Seminario Euro-Iberoamericano de Protección de Datos en Cartagena de Indias, Colombia. Del 16 al 18 de noviembre, el Supervisor y el Supervisor Adjunto participaron en la Conferencia Safe Harbor organizada por el Departamento de Comercio de los EE.UU. en Washington DC.

# Anexo H. Composición de la Secretaría del SEPD

Monique LEENS-FERRANDO
*Jefa de Secretaría (desde noviembre de 2009)*

## • Supervisión

| | |
|---|---|
| Sophie LOUVEAUX<br>*Administradora/jurista*<br>*Coordinadora de relaciones entre RPD y controles previos* | Manuel GARCÍA SÁNCHEZ<br>*Experto nacional/encargado técnico (hasta octubre de 2009)* |
| | Delphine HAROU<br>*Asistente de supervisión* |
| Zsuzsanna BELENYESSY<br>*Administradora/jurista* | John-Pierre LAMB<br>*Experto nacional (desde octubre de 2009)* |
| Isabelle CHATELIER<br>*Administradora/jurista* | Xanthi KAPSOSIDERI<br>*Asistente de supervisión* |
| Eva DIMOVNÉ KERESZTES<br>*Administradora/jurista*<br>*Coordinadora de inspecciones (hasta octubre de 2009)* | Sylvie PICARD<br>*Asistente de supervisión* |
| Jaroslaw LOTARSKI<br>*Administrador/jurista*<br>*Coordinador de reclamaciones* | Kim Thien LÊ<br>*Asistente de secretaría* |
| María Verónica PÉREZ ASINARI<br>*Administradora/jurista*<br>*Coordinadora de medidas administrativas* | Pierre FALLER<br>*Becario (de abril de 2009 a julio de 2009)* |
| Tereza STRUNCOVA<br>*Administradora/jurista* | Evangelia MESAIKOU<br>*Becaria (de marzo de 2009 a julio de 2009)* |
| Michaël VANFLETEREN<br>*Administrador/jurista* | Eleni ATHERINOU<br>*Becaria (desde octubre de 2009)* |
| Athena BOURKA<br>*Experta nacional/encargada técnica (hasta octubre de 2009)* | Mathias POCS<br>*Becario (desde octubre de 2009)* |

## • Política e información

| | |
|---|---|
| Hielke HIJMANS<br>*Administrador/jurista*<br>*Coordinador de procedimientos de consulta ante los tribunales* | Roberto LATTANZI<br>*Experto nacional (desde octubre de 2009)* |
| Rosa BARCELÓ<br>*Administradora/jurista* | Martine BLONDEAU (*)<br>*Asistente de documentación* |
| Laurent BESLAY<br>*Administrador/encargado técnico*<br>*Coordinador de seguridad y tecnología* | Francisco Javier MOLEÓN GARCÍA<br>*Asistente de documentación* |
| Katarzyna CUADRAT-GRZYBOWSKA<br>*Administradora/jurista* | Andrea BEACH<br>*Asistente de secretaría* |
| Bénédicte HAVELANGE<br>*Administradora/jurista*<br>*Coordinadora de grandes sistemas de tecnologías de la información y de política de fronteras* | Anna-Maria VANHOYE<br>*Asistente de secretaría*<br>*(desde octubre de 2009)* |
| Herke KRANENBORG<br>*Administrador/jurista* | Vasiliki MYLONA<br>*Becaria (de marzo de 2009 a julio de 2009)* |
| Anne-Christine LACOSTE<br>*Administradora/jurista*<br>*Coordinadora del Grupo de trabajo del artículo 29* | Mario VIOLA DE AZEVEDO CUNHA<br>*Becario (de marzo de 2009 a julio de 2009)* |
| Alfonso SCIROCCO<br>*Administrador/jurista* | Maria-Grazia PORCEDDA<br>*Becaria (desde octubre de 2009)* |
| Nathalie VANDELLE (*)<br>*Administradora/encargada de prensa*<br>*Coordinadora del equipo de información* | |

(*) Equipo de información.

# • Unidad de personal, presupuesto y administración

Monique LEENS-FERRANDO
*Jefa de unidad (hasta octubre de 2009)*

## • Recursos humanos

| | |
|---|---|
| Giuseppina LAURITANO<br>*Administradora/asuntos estatutarios*<br>*Responsable del control de cuentas y la protección de datos* | Guido CAGNONI<br>*Becario (de marzo de 2009 a julio de 2009)* |
| Vittorio MASTROJENI<br>*Asistente de recursos humanos* | Livia HARSEU<br>*Becaria (desde octubre de 2009)* |
| Anne LEVÊCQUE<br>*Asistente de recursos humanos* | |

## • Presupuesto y finanzas

| | |
|---|---|
| Tonny MATHIEU<br>*Administrador financiero (hasta octubre de 2009)* | María SÁNCHEZ LÓPEZ<br>*Asistente financiera y de contabilidad* |
| Raja ROY<br>*Asistente financiero y de contabilidad* | |

## • Administración

| |
|---|
| Anne-Françoise REYNDERS<br>*Asistente administrativa, de actividades sociales y de infraestructuras* |

El SEPD y el SEPD Adjunto con su personal.

Supervisor Europeo de Protección de Datos

**Informe Anual 2009**

Luxemburgo: Oficina de Publicaciones de la Unión Europea

2011 — 116 pp. — 21 x 29.7 cm

ISBN 978-92-95073-09-8
doi:10.2804/13085

## 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).

QT-AA-10-001-ES-N

SUPERVISOR EUROPEO
DE PROTECCIÓN DE DATOS

# *El guardián europeo de la protección de datos personales*

**www.edps.europa.eu**

Oficina de Publicaciones

ISBN 978-92-95073-08-1