

En virtud de las atribuciones establecidas por el artículo 37. 1) de la Ley Orgánica 15/1999 de Protección de Datos la Agencia Española de Protección de Datos tiene encomendada la labor de "...desempeñar las funciones de cooperación internacional en materia de protección de datos personales".

En cumplimiento de esa competencia, la Agencia Española de Protección de Datos, lleva a cabo una intensa actividad internacional en Europa, EEUU e Iberoamérica centrada en su participación en muy diversos foros de debate multinacionales y en actividades de supervisión y cooperación internacional en materia de protección de datos.

TENDENCIAS LEGISLATIVAS, JURISPRUDENCIALES Y DOCTRINALES EN MATERIA DE PROTECCIÓN DE DATOS EN OTROS PAÍSES

Además de analizar nuestra propia actividad y objetivos en el ámbito internacional en los cuatro siguientes apartados, de acuerdo con lo previsto en el artículo 8.1.b del Estatuto de la AEPD vamos a ver en este epígrafe inicial cuáles han sido las principales tendencias legislativas, jurisprudenciales y doctrinales en materia de protección de datos en otros países.

En este sentido conviene subrayar que en el seno de la UE, la Comisión Europea ha desarrollado una importante actividad encaminada a supervisar y examinar el cumplimiento de los acuerdos que podríamos llamar "transatlánticos" de transferencia de datos. En el año 2005 se hizo una primera revisión conjunta de la Decisión sobre PNR (transferencia de Datos de pasajeros de aerolíneas con destino a los Estados Unidos) y un seminario sobre el funcionamiento del Acuerdo Safe Harbor, también para la transferencia de datos a aquél país. En relación con este último se pide por parte de la Comisión una mayor implicación de la Autoridades competentes de los Estados Unidos en la supervisión a las compañías acogidas a este Acuerdo pero no se detectan graves problemas o deficiencias en su funcionamiento. La información pormenorizada sobre las actividades de la Comisión se pueden consultar en el 9º Informe Anual del Grupo del Artículo 29¹.

Sobre las novedades legislativas en otros países europeos hay que decir que las Repúblicas de Eslovenia y de Eslovaquia han transpuesto este año la Directiva 95/46 mediante dos nuevas leyes² (Information Commissioner Act nº 113/2005 y Law nº 90/2005) cuyo texto en inglés puede consultarse en la web del GT29.

Además conviene destacar que si bien el año 2004 fue el primer año de actividad del Supervisor Europeo de Protección de Datos, en el 2005 inicia propiamente su actuación supervisora. Entre sus competencias de supervisión cabe destacar la puesta en

¹ http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2006_en.htm

² Todas las nuevas leyes aprobadas en 2005 se incluyen en la página web del GT29, en la dirección antes referenciada

marcha de la red de oficiales de protección de datos en cada una de las instituciones de la UE, la elaboración de las primeras autorizaciones previas para el tratamiento de datos por parte de instituciones comunitarias, la elaboración de dictámenes sobre acceso a los documentos que obran en archivos de la UE y sobre el uso de las comunicaciones electrónicas y su incidencia en la privacidad. La descripción pormenorizada de su trabajo se incluye también en el 9º Informe Anual del GT29.

En cuanto a las iniciativas legislativas más importantes en curso en Europa, nos remitimos al contenido del apartado que con ese nombre se incluye a continuación en la parte de Europa de esta Memoria.

En el ámbito Iberoamericano, como novedades legislativas importantes en 2005 podemos destacar la aprobación en Bolivia, el 25 de mayo, del Anteproyecto de Ley de Comunicación de Datos y Comercio Electrónico cuyo texto puede consultarse la sección de la Red Iberoamericana de Protección de Datos de la página web de esta Agencia.

Asimismo, merece ser destacado el caso de Perú, donde durante el año 2005 se continuaron los trabajos de elaboración de un proyecto de Ley de protección de datos personales, en el que, además ha colaborado esta Agencia en el marco de la Red Iberoamericana de Protección de Datos y que ha sido presentado ya oficialmente en el momento de elaborar la presente Memoria.

Por lo que se refiere a Estados Unidos lo más destacable se encuentra en el ámbito jurisprudencial y se concreta en la Sentencia sobre el caso conocido como "ChoicePoint" en el que la empresa de dicho nombre (broker de datos de consumidores con fines comerciales) tras una investigación realizada por la Comisión Federal del Comercio (Federal Trade Commission-FTC), por falta de medidas de seguridad y violación de los fines legítimos para los que se había recogido la información personal, fue condenada por un tribunal federal a una multa de 10 millones de dólares y a pagar indemnizaciones a los afectados por importe de 5 millones de dólares³.

Es también importante mencionar el informe que la FTC aprobó ese año sobre las "short privacy notices" o cláusulas de información. La FTC y otras Agencias federales recomiendan una redacción clara y sucinta sobre cómo se van a proteger los datos de los consumidores⁴.

EUROPA

ACTIVIDAD DERIVADA DE LA DIRECTIVA EUROPEA DE PROTECCIÓN DE DATOS: EL GRUPO DE TRABAJO DEL ARTÍCULO 29

El Grupo de Trabajo del Artículo 29 (en adelante GT29), creado por la Directiva 95/46/CE tiene carácter de órgano consultivo independiente y está integrado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor

³ Más información sobre este caso se puede obtener en: <http://www.ftc.gov/opa/2006/01/choicepoint.htm>

⁴ Mas información sobre este informe en : <http://www.ftc.gov/opa/2006/03/jointprprivacy.htm>

Europeo de Protección de Datos y la Comisión Europea - que realiza funciones de secretariado-. Asimismo, los Estados candidatos a ser miembros de la Unión y los países miembros del EEE acuden a las reuniones del GT 29 en condición de observadores. La Agencia Española de Protección de Datos forma parte del mismo desde su inicio, en febrero de 1997 y su Director ostenta desde 2004 la Vicepresidencia⁵.

El GT 29 se reúne en plenarios con una periodicidad bimensual y se organiza en diversos subgrupos de trabajo para analizar todas aquellas cuestiones que inciden, o pueden llegar a afectar, a la protección de datos personales. El GT 29 emite sus observaciones a través de Decisiones, Dictámenes, Documentos de Trabajo, Informes o Recomendaciones. Estos documentos son posteriormente transmitidos a la Comisión y al Comité contemplado en el Artículo 31 de la Directiva 95/46/CE.

Durante el año 2005, el GT29 aprobó 15 documentos, que se enumeran a continuación.

- Octavo informe sobre la situación de la protección de las personas en el tratamiento de sus datos en la Unión Europea y Terceros Países (año 2004), adoptado el 25 de noviembre de 2005.
- Dictamen sobre las propuestas de Reglamento del Parlamento Europeo y del Consejo y de Decisión del Consejo sobre el establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II) y sobre una propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al acceso al Sistema de Información de Schengen de segunda generación (SIS II) por los servicios de los Estados miembros responsables de la expedición de los certificados de matriculación de vehículos. Adoptado el 25 de noviembre de 2005 (WP 116)
- Dictamen sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido. Adoptado el 25 de noviembre de 2005 (WP 115)
- Documento de trabajo relativo a una interpretación común del artículo 26.1 de la Directiva 95/46/CE Adoptado el 25 de noviembre de 2005 (WP 114)
- Dictamen sobre la Propuesta de Directiva sobre la Retención de Datos, adoptado el 21 de octubre de 2005 y modificación de la Directiva 2002/58/EC. Adoptado el 25 de noviembre de 2005 (WP 113)
- Dictamen sobre la aplicación del Reglamento (CE) n° 2252/2004 del Consejo, de 13 de diciembre de 2004, sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros. Adoptado el 30 de septiembre de 2005 (WP 112)
- Resultados de la Consulta del Grupo de Trabajo del Artículo 29 sobre el documento de trabajo 105 relativo a la tecnología RFID. Adoptado el 28 de junio de 2005 (WP 111).

⁵ A fecha de cierre de la Memoria, Mayo de 2005, el Director de la AEPD ha sido reelegido Vicepresidente del Grupo de Trabajo del Artículo 29 por unanimidad.

- Dictamen sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros COM(2004) 835 final. Adoptado el 23 de junio de 2005 (WP 110)
- Programa de trabajo de 2005. Aprobado el 14 de abril de 2005 (WP 109)
- Documento de trabajo por el que se establece un modelo en forma de lista de control para solicitar la aprobación de normas corporativas vinculantes. Aprobado el 14 de abril de 2005 (WP 108)
- Documento de trabajo por el que se expone un procedimiento de cooperación para la emisión de dictámenes comunes sobre las salvaguardas adecuadas que resultan de las "normas corporativas vinculantes". Aprobado el 14 de abril de 2005 (WP 107)
- Informe del GT 29 sobre la obligación de notificar a las autoridades nacionales el mejor uso de las excepciones y simplificación y el papel de los Oficiales de Protección de Datos de la Unión Europea. Adoptado el 18 de enero de 2005 (WP 106)
- Documento de trabajo relacionado sobre tecnología RFID y protección de datos. Adoptado el 19 de enero de 2005 (WP 105)
- Documento de trabajo sobre propiedad intelectual y protección de datos. Adoptado el 18 de enero de 2005 (WP 104)
- Dictamen 1/2005 sobre el nivel de protección garantizado por Canadá para la transmisión de expedientes de viajeros y de información anticipada sobre viajeros por parte de las compañías aéreas. Adoptado el 19 de enero de 2005 (WP 103)

Todos ellos se pueden consultar en el siguiente hipervínculo:

http://www.europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm

ASUNTOS MÁS IMPORTANTES TRATADOS EN EL AÑO 2005 EN EL MARCO DEL GT 29

Es importante resaltar la interesante iniciativa llevada a cabo por la Comisión Europea de incluir en la página Web de la Unidad de Protección de Datos de la Dirección General de Libertad, Justicia y Seguridad, un apartado destinado a la consulta de documentos de las autoridades de protección de datos nacionales. Con esta iniciativa se facilita la consulta de las diferentes legislaciones nacionales, sus novedades y desarrollos, permitiendo un conocimiento más exacto de la evolución que las iniciativas en materia de protección de datos personales están teniendo en todo el territorio de la Unión. De la misma forma, el visitante tiene acceso a informes y resoluciones que sobre diferentes materias han emitido las autoridades. Ejemplo de esa documentación son los textos de desarrollo e interpretación relativos a marketing directo, spam, datos sensibles, derechos de los afectados, etc...

Se puede acceder a los diferentes textos en el siguiente vínculo:

http://www.europa.eu.int/comm/justice_home/fsj/privacy/policy_papers/policy_papers_en.htm

Como se comentaba con anterioridad, el GT29 está constituido en diversos subgrupos en los que se analizan los temas asignados por el Programa de Trabajo Anual. En el programa de trabajo de 2005, el GT 29 fijaba como prioridades diversas cuestiones tales como las implicaciones que, en materia de protección de datos, tienen los historiales médicos electrónicos, la retención de datos, la administración electrónica o los datos biométricos. Durante el año 2005 el GT 29 se organizó en los siguientes subgrupos:

- SUBGRUPO DE TRABAJO PARA LA PREVENCIÓN DEL FRAUDE (FRAUD PREVENTION TASK FORCE)-

El GT 29 fue consultado en relación a las implicaciones en materia de protección de datos personales que tendría la creación de una base de datos sobre fraudes detectados en los pagos con tarjeta de crédito.

- SUBGRUPO DE TRABAJO SOBRE INTERNET (INTERNET TASK FORCE)

En este subgrupo se analizan las repercusiones que las nuevas tecnologías puedan tener en la esfera privada de las personas. Los temas que se estudiaron a lo largo de 2005 estuvieron centrados en el uso de los datos de localización, definidos por la Directiva 2002/58/CE como "cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público". En el documento de trabajo relativo a los datos de localización, el GT 29 interpreta las directivas con disposiciones en materia de protección de datos estableciendo las condiciones generales para tratar esos datos en servicios de valor añadido. En este documento, además, se fijan condiciones y recomendaciones para la implementación de servicios de localización para una determinada finalidad, como es la localización de menores o trabajadores. Asimismo, el subgrupo analizó asuntos relativos a la filtración de comunicaciones por e-mail, diferenciando los siguientes supuestos: filtración de e-mails para fines de detección de virus, para fines de eliminación de Spam, para propósitos de detección de material ilegal y para finalidades de marketing.

- SUBGRUPO BINDING CORPORATE RULES (BCR)

Las BCR's o cláusulas corporativas vinculantes cubren los procedimientos de transferencia internacional de datos sobre la base de una excepción a la exigencia de nivel adecuado de protección o de autorización previa, creando unas garantías de seguridad mediante una declaración unilateral de derechos y obligaciones que asumen los miembros de un grupo corporativo de empresas. Tras un primer documento al respecto (WP 74, aprobado en junio de 2003), el GT 29 trabajó durante el año 2005 en esta fórmula de transferencia internacional. Con el fin de estudiar este procedimiento de autorizaciones basado en la autorregulación y la cooperación entre autoridades, el subgrupo adoptó dos documentos en los que se aprueba el procedimiento coordinado para aprobar estas cláusulas por las Autoridades de Protección de Datos y el modelo de Check list a cumplimentar por las compañías.

- SUBGRUPO "ENFORCEMENT TASK FORCE"

Conviene señalar que en el año 2005, la AEPD participó activamente y coordinó, junto a la autoridad de protección de datos holandesa, el grupo de trabajo de Enforcement Task Force, subgrupo que analiza la capacidad de aplicar y ejecutar las normas de protección de datos por parte de las Autoridades supervisoras.

En una declaración del 25 de noviembre de 2004⁶, el GT 29 estableció que uno de sus objetivos estratégicos y permanentes era promover el cumplimiento armonizado de la legislación sobre protección de datos en todos los Estados Miembros. La citada declaración enfatiza la importancia del control de la aplicación de la legislación como un medio de incrementar su cumplimiento y por ello, el GT 29 llevaría a cabo acciones en todos los estados miembros de forma sincronizada para el control de tal aplicación.

Asimismo, como consecuencia de la evaluación de la Directiva 95/46/CE en mayo de 2003, la Comisión Europea solicitó al GT 29 que considerase el lanzamiento de investigaciones sectoriales de alcance europeo para la aproximación de las legislaciones en este sentido. Esta petición se ha materializado con la puesta en marcha de una investigación bajo la forma de una acción coordinada emprendida por las Autoridades de Protección de Datos nacionales de los Estados Miembros en el contexto de sus actividades en el GT 29. Cubriendo el mismo período y centrándose en los mismos tipos de tratamiento en todos los Estados Miembros, un cuestionario único permitirá obtener esta información.

El GT 29 decidió, a propuesta de la autoridad española, que la primera acción nacional sincronizada de control de la aplicación de las normas europeas de protección de datos se realizaría en el sector de seguros de salud privados. Este sector fue el seleccionado por ser el tratamiento de datos personales sensibles un elemento clave de sus actividades y por el potencial impacto que tendría un eventual incumplimiento sobre un número significativo de personas en la Unión Europea.

Tras el lanzamiento de la acción, las respuestas recibidas se evaluarán tanto a nivel nacional como europeo, publicándose posteriormente un resumen de todos los resultados nacionales como parte de un informe del GT 29. Dentro de esta acción, el GT 29 podría emitir recomendaciones adicionales y guías prácticas para el sector en general e identificar áreas para acciones futuras, en línea con las funciones descritas en el artículo 30 de la Directiva 95/46/CE.

- SUBGRUPO "SARBANES OXLEY ACT"

Por otro lado, y como muestra de algunas de las actividades de asesoramiento y colaboración internacional que la AEPD ha llevado a cabo durante el año 2005, resultan de interés los trabajos llevados a cabo sobre las obligaciones legales establecidas por la Sarbanes Oxley Act, ley federal americana aprobada en el año 2002 fruto de una serie de escándalos corporativos relacionados con el maquillaje de cuentas en grandes empre-

⁶ Declaración del Grupo de Trabajo del Artículo 29 sobre el Control de la Aplicación de la Legislación, WP101, 12067/04/ES, WP101, de 25 de noviembre de 2004.

sas. Esta Ley obliga a las empresas multinacionales que cotizan en la Bolsa de Nueva York a notificar cualquier situación que pueda suponer una infracción en materia financiera, por desviación de fondos u ocultación de resultados económicos. Asimismo establece una política de "integrity lines" o líneas de integridad en las que se plantea la creación de ficheros con información sobre posibles vulneraciones de la legalidad por parte de los trabajadores de la empresa. Se puede destacar que la S.O.A. permite informar anónimamente por teléfono, vía correo electrónico o por correo postal sobre los comportamientos que puedan suponer una infracción de las políticas de la empresa. De este modo, se establecen una serie de disposiciones con vistas a lograr una mayor transparencia en la actividad empresarial, pero dando también cobertura a la posibilidad de realizar denuncias sobre situaciones de acoso, discriminación, o conductas criminales.

En definitiva, y aunque esta Ley puede contribuir a la seguridad en los mercados financieros internacionales estas líneas de integridad podrían vulnerar la esfera privada de los trabajadores y la legislación en materia de protección de datos de carácter personal. Estos ficheros, comúnmente llamados en la jerga europea como "*Whistleblowing*"-cuya traducción al español puede ser "ficheros de soplon"- se asemejan a otras iniciativas llevadas a cabo por la Comisión⁷ y que tienen el mismo objetivo que la Sarbanes Oxley Act, es decir, reforzar la seguridad en los mercados financieros.

En la última reunión plenaria del GT 29 del año 2005 se acordó la creación de un subgrupo para analizar esta Ley y así poder elaborar una opinión sobre la implantación de este tipo de políticas en las empresas.

PROPUESTAS LEGISLATIVAS DE INTERÉS

■ ESPACIO DE LIBERTAD, SEGURIDAD Y JUSTICIA: PROGRAMA DE LA HAYA

En el año 2005 se aprueba el Plan de Acción de La Haya que, en base a la identificación de 10 líneas prioritarias, pretende dar continuidad al programa adoptado en noviembre de 2004 con vistas a la consolidación y desarrollo del Espacio europeo de Libertad, Seguridad y Justicia.

Este Plan de Acción nace con la intención de ser el marco de referencia del trabajo a desarrollar por la Comisión y el Consejo durante los próximos 5 años, para lo que establece un calendario y unas medidas concretas que permitan impulsar definitivamente un área en la que los ciudadanos puedan disfrutar plenamente de sus derechos y libertades y hacer frente a las cada vez más globalizadas amenazas a los valores de la sociedad democrática. Derechos fundamentales y ciudadanía, lucha contra el terrorismo, política de inmigración y asilo, privacidad y seguridad en el intercambio de información y gestión de las fronteras exteriores son algunas de las materias tratadas por el documento.

⁷ La Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a libre circulación de estos datos

■ RETENCIÓN DE DATOS

Como ya se hacía constar en la memoria del año 2004, la retención de datos de tráfico ha supuesto un asunto ineludible en la agenda de trabajo del GT 29⁸, motivado por las iniciativas legislativas presentadas con el fin de hacer frente al posible uso de los servicios de la sociedad de la información para fines criminales.

Tras los atentados de Madrid, en una primera Declaración sobre la lucha contra el terrorismo, adoptada por el Consejo Europeo el 25 de marzo de 2004, se encargó al Consejo que examinara medidas para establecer normas sobre la conservación por los prestadores de servicios de datos de tráfico de las comunicaciones.

En el año 2004 el Consejo proponía un Proyecto de Decisión Marco sobre retención de datos de tráfico de las comunicaciones electrónicas con fines de prevención, investigación y represión de la delincuencia y las infracciones penales. Esta propuesta fue objeto de una Opinión por parte del GT 29 que consideraba que tal Decisión Marco incumplía los principios establecidos por la Directiva de protección de datos. El Parlamento Europeo, por su parte, rechazaba también esta iniciativa alegando la improcedencia de los fundamentos jurídicos, los artículos 31 y 34 del Tratado de la Unión Europea (III pilar -Cooperación policial y judicial en materia penal-) y señalando ciertas reticencias en cuanto al contenido de la propuesta.

En septiembre de 2005, tras los atentados de julio en Londres, la Comisión Europea presentó una nueva iniciativa cuyo fundamento jurídico era el Artículo 95 del Tratado de la Comunidad Europea (I pilar, Mercado Interior). La forma jurídica elegida en esta ocasión fue la de una Directiva, utilizada en aquellos casos en los que se pretende una armonización mínima de las legislaciones nacionales y no la imposición directa de medidas. El cambio de base jurídica supuso también una modificación en el procedimiento legislativo a seguir: pasaba a ser de aplicación el artículo 251 del Tratado, el llamado procedimiento de codecisión, con el que el Parlamento Europeo se situaba en una posición igualitaria a la del Consejo a la hora de aprobar la norma.

Ante la nueva propuesta de Directiva, el GT 29 se interesó por el contenido de la misma y emitió, en octubre de 2005, una opinión al respecto (WP 113) en la que precisa veinte medidas específicas para asegurar el derecho a la confidencialidad en el uso de servicios de comunicaciones electrónicas.

A modo de resumen, podemos sintetizar estas medidas en las siguientes:

- Los fines han de ser específicos y centrados la lucha contra el terrorismo y crimen organizado.

⁸ Entre ellas se pueden mencionar el Dictamen 1/2003 sobre el almacenamiento de los datos de tráfico a efectos de facturación; el Dictamen 5/2002 sobre la Declaración de los Comisarios Europeos responsables de protección de datos en la Conferencia Internacional celebrada en Cardiff (9-11 de septiembre de 2002) sobre la retención sistemática obligatoria de datos sobre tráfico de telecomunicaciones; en el Documento de Trabajo Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea; el Dictamen 4/2001 sobre el borrador de Convenio sobre Cibercrimen del Consejo de Europa; el Dictamen 10/2001 sobre la necesidad de un enfoque equilibrado en la lucha contra el terrorismo; el Dictamen 7/2000 sobre la propuesta de la Comisión Europea de Directiva del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas de 12 de julio de 2000 COM (2000) 385; la Recomendación 3/99 sobre la conservación de los datos sobre tráfico por los proveedores de servicio Internet a efectos de cumplimiento de la legislación; la Recomendación 2/99 sobre la protección de la intimidad en el contexto de la interceptación de las telecomunicaciones y la Recomendación 3/97 sobre anonimato en Internet.

- Limitación de los usos posteriores de esos datos y del acceso por parte de otros organismos públicos y para usos propios.
- El acceso de esos datos debe autorizarse, en principio, caso por caso por la autoridad judicial sin perjuicio de los países en donde exista una posibilidad específica de acceso autorizada por ley.
- Deben tenerse en cuenta las medidas de seguridad establecidas en la Directiva 2002/58/CE.
- Los sistemas de almacenamiento de estos datos deberán estar separados de aquellos sistemas que las compañías utilicen a efectos empresariales y deberán estar sometidos a unas medidas de seguridad más rigurosas.

Por su parte, el Parlamento Europeo aprobó su informe, esta vez vinculante, el 14 de diciembre de 2005. En el mismo, a pesar de que hacía ver una serie de salvedades a la propuesta e indicaba una serie de salvaguardas que debían ser adoptadas, se mostraba favorable a la aprobación de la Directiva.

A pesar de que el acuerdo ya había sido alcanzado, la norma no ha sido aprobada formalmente hasta febrero de 2006. Sus líneas generales son las siguientes:

- Objetivo: la armonización de la obligación de retener datos de tráfico y localización generados o procesados con vistas a asegurar que esos datos sean disponibles con el fin de investigar, detectar y perseguir crímenes graves (tal y como estén definidos en la legislación de cada Estado miembro).
- Sujetos obligados a retener los datos: proveedores de servicios de comunicaciones electrónicas de acceso público y proveedores de redes públicas de comunicaciones.
- Los datos a retener son aquellos necesarios para identificar la fuente, el destino y el tipo de comunicación; su fecha, hora y duración; el equipo de comunicación o para la localización del equipo de comunicación móvil. Se puede destacar aquí que todos estos datos deberán ser conservados también en el caso de las llamadas perdidas, es decir, aquellas en que no haya habido respuesta a la comunicación realizada.
- Períodos de retención: de seis meses a dos años⁹. No obstante, los Estados miembros pueden justificar una extensión de este período basándose en "circunstancias especiales".
- Otras obligaciones: asegurar la calidad y seguridad de los datos retenidos y transmisión de los datos solicitados sin demora. En lo que se refiere al acceso a los datos retenidos, cabe señalar que las condiciones y procedimiento para el acceso a estos datos se encuentran fuera del ámbito de aplicación de la Directiva.

⁹ NOTA: En la propuesta original se diferenciaba entre la retención de datos de telefonía (fija o móvil) para la que se establecía un período de 12 meses y datos de Internet, a los que se le aplicaba un período de retención de 6 meses.

- Se otorga un papel de supervisión a las Autoridades Nacionales de Protección de Datos.
- La eficacia de la medida deberá ser objeto de una evaluación antes de haber transcurrido 3 años desde su transposición.

El plazo de transposición se fijaba en 18 meses, con la posibilidad de aplazar otros 18 meses más las medidas relativas a los datos de Internet¹⁰.

■ PROPUESTA DE DECISIÓN MARCO RELATIVA A LA PROTECCIÓN DE DATOS PERSONALES TRATADOS EN EL MARCO DE LA COOPERACIÓN POLICIAL Y JUDICIAL EN MATERIA PENAL

Como consecuencia del Programa de La Haya, en el año 2005 se presenta la propuesta de Decisión Marco del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (III pilar). La propuesta tiene su base jurídica en los artículos 31.1.c) y 34.2.b) del Tratado de la Unión Europea, tras la recomendación realizada por el Parlamento Europeo con vistas a armonizar la normativa existente en materia de datos personales en el conjunto del Tercer pilar, agrupándola en un solo instrumento que garantice el mismo nivel de protección de datos que el establecido para las materias propiamente comunitarias.

La propuesta de Decisión Marco contiene normas generales sobre la legalidad del tratamiento de datos personales y disposiciones relativas a formas específicas de tratamiento, derechos del afectado, garantías respecto a la confidencialidad y la seguridad del tratamiento, delimitación de responsabilidad y régimen de sanciones. Además, regula la autoridad de control, un grupo de personas con responsabilidad en lo que respecta al tratamiento de datos personales con fines de prevención, investigación, detección y enjuiciamiento de delitos que, con carácter de órgano consultivo, estudiará la aplicación de las disposiciones nacionales adoptadas en virtud de la Decisión Marco para contribuir a una aplicación homogénea en todos los Estados miembros.

ACTIVIDAD DERIVADA DE LOS CONVENIOS DE EUROPOL, SCHENGEN, SISTEMA DE INFORMACIÓN ADUANERO Y EUROJUST

En el marco de las actividades de cooperación intergubernamental (III pilar), 2005 ha sido el año en el que se han presentado las propuestas sobre la segunda generación del Sistema de Información Schengen (SIS). Este sistema, creado en 1985, permite a las autoridades competentes de los Estados miembros disponer de información relativa a algunas categorías de personas y objetos, constituyendo una herramienta esencial en el buen funcionamiento del Espacio de Libertad, Seguridad y Justicia. Teniendo en cuenta las nuevas circunstancias acaecidas tras su creación en 1985, sobre todo los avances tecnológicos y la incorporación de 10 nuevos Estados miembros a la UE, una revisión del Sistema se hacía necesaria para asegurar su correcto funcionamiento.

¹⁰ A fecha de cierre de esta memoria, el GT 29 ha aprobado una nueva Opinión, la 3/2006 en la que señala la conveniencia de que las autoridades nacionales de protección de datos tengan un papel señalado en la transposición de la Directiva, favoreciendo que ésta sea lo más homogénea y uniforme posible en todo el territorio de la UE

En mayo de 2005, la Comisión presentó tres propuestas diferentes de actos jurídicos. Por un lado, un Reglamento y una propuesta de Decisión relativos al establecimiento, funcionamiento y utilización del Sistema Schengen de segunda generación (SIS II), que sustituirían al título VI del Convenio y contienen disposiciones obligatorias para los estados miembros y tienen una estructura común. Por otro lado, una tercera propuesta referida al acceso al SIS II por los servicios de los Estados miembros con vistas a la expedición de los certificados de matriculación de los vehículos.

La razón para la utilización de dos instrumentos jurídicos diferenciados se encuentra en las diferentes características de los datos incluidos en el SIS: por un lado, el sistema recoge datos utilizados por las autoridades competentes en la gestión de las fronteras y la libre circulación de personas (I pilar) y, por otro, se incluyen datos relevantes para la cooperación policial y judicial entre los Estados miembros (III pilar).

El GT 29 emitió un Dictamen en noviembre de 2005 (WP 116) con el fin de examinar si las nuevas propuestas garantizaban un nivel adecuado de protección. Para ello, analizó los requisitos de acceso al sistema y su finalidad, expresando su preocupación con respecto al tratamiento de las nuevas categorías de datos y su descripción y haciendo especial referencia a la utilización de datos biométricos. Asimismo, analiza los períodos de conservación de los datos, los derechos de los afectados y la misión de control. A modo de conclusión, el GT 29 estima que es necesario garantizar una aplicación estricta del principio de especificación de los fines y del uso de los datos biométricos.

Puede consultarse el documento en el siguiente hipervínculo:

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp116_es.pdf

En relación con la unidad europea de cooperación judicial Eurojust, la Agencia participa en su Autoridad Común de Control en materia de protección de datos. En noviembre de 2005, bajo Presidencia Británica, se llevó a cabo la primera inspección del sistema. Las inspecciones en Eurojust se organizan entre el miembro del país que en ese momento ostente la Presidencia del Consejo y quien le haya precedido y le suceda (troika). El objeto principal de la inspección fue la seguridad de la red donde se incluye el Sistema de Gestión de Casos.

Por otro lado, en 2005 también se presentó la propuesta por la que se pretende dar acceso a los responsables de seguridad interior y a Europol de los datos contenidos en el Sistema de Información de Visados (VIS) con fines de prevención, detección e investigación de los delitos de terrorismo y otros delitos graves. Este sistema permite el intercambio de datos sobre visados de corta duración entre los Estados miembros y el acceso a la información por diferentes autoridades, lo que plantea cuestiones importantes en cuanto a los derechos fundamentales y las libertades individuales, y en especial el derecho a la intimidad relativa a un gran número de personas.

El Sistema de Información de Visados, creado en 2004 ¹¹, se enmarca dentro de las medidas destinadas a mejorar la gestión de la política común de visados, contribuyen-

¹¹ Decisión del Consejo de 8 de junio de 2004 por la que se establece el Sistema de Información de Visados (VIS)

do, al mismo tiempo, a desarrollar el acervo de Schengen. A finales de 2004 se presentó una propuesta de Reglamento¹² con vistas a crear el marco jurídico completo bajo el que entrará en funcionamiento el sistema. En dicha propuesta, cuya tramitación aún no se ha completado, se establecen disposiciones detalladas sobre el sistema y su funcionamiento, se enumeran las categorías de datos que deben introducirse en el sistema, las autoridades de los Estados miembros que pueden introducir datos en el sistema y acceder a los datos en él contenidos, el período de conservación de los datos, el derecho de acceso y los derechos de corrección y de supresión del afectado, las medidas de seguridad que deben adoptarse y la supervisión en la UE y a escala nacional.

La Comisión solicitó formalmente la opinión del GT 29 sobre la propuesta de Reglamento y éste se pronunció en el "Dictamen sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros", adoptado en junio de 2005¹³.

En su Dictamen, el GT 29 recuerda que deben observarse los principios de finalidad y proporcionalidad y que el tratamiento de datos biométricos debe realizarse de forma que garantice un nivel alto de fiabilidad, concretamente para prevenir el robo de identidad. Además, el almacenamiento en una base de datos centralizada deberá ser muy limitado- con acceso en casos absolutamente necesarios y por autoridades identificadas- y estar sujeto a controles especialmente muy rigurosos.

■ ACTIVIDAD DERIVADA DEL CONVENIO 108 DEL CONSEJO DE EUROPA

La Agencia Española de Protección de Datos participa en el Comité Consultivo (T-PD) establecido en el artículo 18 del Convenio para la protección de las personas físicas en relación con el tratamiento automatizado de datos personales (Convenio 108)¹⁴. El citado Comité celebró su reunión plenaria número 21 en febrero de 2005, en el que se repasó la actividad llevada a cabo por el Consejo de Europa¹⁵ y se aprobó el "Informe sobre la Aplicación de los principios del Convenio 108 a la recogida y tratamiento de datos biométricos". Como ya se adelantaba en la Memoria del año 2004, se presentó el informe definitivo sobre "La autodeterminación informativa en los tiempos de Internet", que analiza los riesgos que para la privacidad tienen las redes de telecomunicaciones y el equilibrio de intereses entre quienes tienen que tratar esas informaciones y los titulares de la misma.

El Bureau del Comité Consultivo (T-PD-BUR) es el órgano de preparación y discusión previa de los documentos que se someten posteriormente al plenario. El citado Bureau se reunió tres veces a lo largo de 2005 y, además del seguimiento de los documentos

12 COM (2004) 835 Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros.

13 Dictamen 2/2005

14 Puede consultarse su estructura y normas de procedimiento en el siguiente vínculo http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/background/13Rules%20of%20procedure%20T-PD.asp#TopOfPage

15 La información mas detallada sobre las actividades y Convenios adoptados por el Consejo de Europa se pueden consultar en : http://www.coe.int/T/E/legal_affairs/Legal_co-operation/Data_protection/

adoptados en el Plenario, es de destacar la propuesta de formalización del derecho a la protección de datos como derecho fundamental (que ya se ha declarado autónomo en algunos países como España o Portugal) mediante un instrumento propio del Consejo de Europa para garantizar el acceso al Tribunal Europeo de Derechos Humanos (TEDH). Se planteó esta posibilidad a través de tres opciones: la primera sería mediante un protocolo adicional al Convenio Europeo de Derechos Humanos (estableciendo un derecho independiente al derecho de privacidad), la segunda a través de un protocolo adicional al Convenio 108 que otorgara al TEDH jurisdicción para las infracciones del Convenio 108 y una tercera opción supondría un protocolo adicional para otorgar al TEDH un rol consultivo similar al que tiene en el Convenio sobre Biomedicina y Derechos Humanos. En la **Reunión Plenaria celebrada en febrero de 2006** se acordó comenzar con los trabajos llevados a cabo por los representantes franceses sobre la jurisprudencia del TEDH.

■ RELACIONES BILATERALES EN EL ÁMBITO EUROPEO

En el apartado de las relaciones bilaterales hay que destacar la cooperación bilateral que se inicia en el 2005 con la Oficina del Ombudsman de **Finlandia** que participa en diversas Conferencias organizadas por la Agencia en España y a su vez promueve la intervención del Director de la Agencia Española ante la Comisión de Asuntos Administrativos del Parlamento de Finlandia, el Foro de Tampere y la Universidad de Rovaniemi.

Tanto la Autoridad Finlandesa de Protección de Datos como la Española cuentan con un amplio abanico de competencias que les permite ejercer sus funciones de supervisión con total autonomía respecto de otros poderes públicos. Igualmente, el Ombudsman finlandés ha asumido la supervisión de las normas nacionales que transponen la Directiva de Privacidad en Telecomunicaciones (D 2002/58/CE) al igual que la Agencia Española. La colaboración en materia de intercambio legislativo y la elaboración de directrices sobre buenas prácticas en materia de privacidad en telecomunicaciones constituirán el inicio de una futura cooperación entre ambas autoridades.

Igualmente se mantienen en 2005 las tradicionales relaciones con la Autoridad de **Portugal** con la que se proyecta una actuación sincronizada conjunta que afectará al sector de laboratorios médicos y que se desarrollará durante el siguiente año. El Encuentro Ibérico anual, de común acuerdo y para combinar de la mejor manera posible las agendas de ambos responsables, se celebró en los primeros meses del siguiente año.

Las fluidas relaciones bilaterales con la Autoridad de Protección de Datos de la **República Checa** que se iniciaron con motivo del twining project que se desarrolló en los años 2003 y 2004, se han consolidado en el año 2005 en el que se ha celebrado en Praga el I Encuentro Hispano-Checo de protección de datos personales, entre ambas autoridades.

La agenda de la reunión incluyó temas relacionados con los datos de salud en la historia clínica, la cooperación para hacer frente a las comunicaciones comerciales

electrónicas no solicitadas (SPAM) y el programa de colaboración que realizarán ambas entidades con la Comisión de Protección de Datos de **Bosnia-Herzegovina**.

Durante las reuniones, los máximos responsables de ambas instituciones, mantuvieron la cordialidad y colaboración que siempre ha presidido las ya fuertes relaciones entre ambas autoridades, cuya continuidad se reafirmó con la convocatoria del II Encuentro a celebrar en España en el año 2006.

En este apartado conviene mencionar el inicio de la cooperación con la Autoridades de Protección de datos de **Andorra**, cuyo responsable visitó este año la Agencia Española.

■ CONFERENCIA DE PRIMAVERA DE AUTORIDADES EUROPEAS DE PROTECCIÓN DE DATOS

La Conferencia Europea de Autoridades de Protección de Datos, que se celebra cada primavera, tuvo lugar los días 25 y 26 de abril de 2005 en Cracovia (Polonia). En este encuentro los debates se estructuraron en torno a varias sesiones, tratando temas como el impacto de la jurisprudencia del Tribunal Europeo de Justicia en la aplicación de la Directiva 95/46/EC o los nuevos instrumentos de transferencia internacional de datos personales (Binding Corporate Rules). La Conferencia finalizó con la aprobación de la "Declaración de Cracovia" en la que se afirmó la necesidad de estrechar la cooperación entre las autoridades de protección de datos y la exigencia de adoptar una serie de principios guía de aplicación en el tratamiento de los datos personales bajo el tercer pilar cuya base sea los estándares de protección de datos contenidos en la Directiva 95/46/CE.

Asimismo, la Conferencia se pronunció sobre el llamado principio de disponibilidad de información en la UE, señalando las salvaguardas que debían adoptarse a la hora de tramitar todas las iniciativas en curso que, implicando la cooperación entre las autoridades policiales y judiciales, tenían incidencia en el tratamiento de datos personales.

■ COLABORACIÓN DE LA AEPD CON LA COMISIÓN EUROPEA EN EL PROCESO DE AMPLIACIÓN DE LA UNIÓN EUROPEA

Dentro de la línea de colaboración permanente de la AEPD con la Comisión Europea, y con el fin de apoyar el proceso de ampliación de la UE y cooperar en la consolidación de instituciones y mecanismos de protección de datos en los nuevos Estados Miembros, la Agencia participó en diversos seminarios organizados por la Dirección General de Ampliación de la Comisión Europea (Instrumento de Asistencia Técnica e Intercambios de Información-TAIEX). La primera de ellas tuvo lugar en Chipre y la segunda en Ankara (Turquía) que ha iniciado ya las negociaciones de adhesión.

Los seminarios, en los que, junto con Autoridades Europeas de Protección de Datos participaban representantes del Tribunal de Justicia de las Comunidades, del mundo universitario y de la Dirección General de Libertad, Seguridad y Justicia de la Comisión Europea, se dirigía a representantes del Parlamento, de los Ministerios de Tecnología,

Interior, Justicia y Empleo de los países que inician negociaciones de adhesión o se han incorporado recientemente a la UE.

IBEROAMERICA

LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS

La Red se creó en junio de 2003, con ocasión de la celebración del II Encuentro Iberoamericano de Protección de Datos, que tuvo lugar en La Antigua (Guatemala).

Este Encuentro contó con la participación de 15 de los entonces 21 Estados que conformaban la Comunidad Iberoamericana. (Actualmente la Comunidad Iberoamericana está integrada por 22 Estados, tras la reciente incorporación de Andorra). Los participantes, en la Declaración firmada al finalizar este Encuentro, resaltaron la necesidad de dotar de una estructura permanente a este foro con el objeto de reforzar la mutua y continua colaboración entre todos y de abrirla a la incorporación de representantes de todos los países Iberoamericanos.

En esta Declaración de La Antigua, los participantes reiteraron la consideración de la protección de datos personales como un auténtico derecho fundamental y declararon que el tratamiento de los datos personales puede impulsar el desarrollo de los Países Iberoamericanos, en el marco de la sociedad de la información y para la consecución de sus legítimos fines por parte de los sectores público y privado, reconociendo los grandes beneficios que las nuevas tecnologías de la Información y las Comunicaciones puede suponer para el desarrollo social y económico de los países.

Tras reconocer que todavía en Iberoamérica se producen situaciones que impiden o dificultan el ejercicio efectivo del derecho, constatan la necesidad de adoptar medidas que garanticen un elevado nivel de protección de datos y tener marcos normativos que garanticen una adecuada protección en todos los países iberoamericanos que deberán tomar en consideración los principios esenciales de protección de datos reconocidos en los Instrumentos Internacionales.

En esta Declaración, en la que se plasma la creación de la Red, se establece una Presidencia y una Secretaría Permanente, que radican en la Agencia Española de Protección de Datos.

Tan sólo unos meses después, la Red sería expresamente reconocida al más alto nivel político. Efectivamente, los días 14 y 15 de noviembre de 2003 tuvo lugar la XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno, en Santa Cruz de la Sierra (Bolivia), y en la Declaración Final, en su apartado 45, se recogió expresamente lo siguiente:

"Asimismo somos conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas

regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la Declaración de La Antigua por la que se crea la Red Iberoamericana de Protección de Datos, abierta a todos los países de nuestra Comunidad."

En la actualidad son 19 los países que cuentan con representación en la Red.

■ IV ENCUENTRO IBEROAMERICANO DE PROTECCIÓN DE DATOS

En el III Encuentro Iberoamericano, celebrado en 2004 en Cartagena de Indias, Colombia, los participantes reconocieron que, una vez superada la fase inicial, caracterizada fundamentalmente por el intercambio de información y experiencias en esta materia, había que plantearse unos objetivos más ambiciosos, y adaptar la estructura y funcionamiento de la Red para posibilitar actuaciones concretas.

Con base en esta idea y, tal y como se refleja en la Memoria del año anterior, en dicho Encuentro se crearon los cuatro subgrupos de trabajo que se relacionan a continuación, abiertos a la incorporación de los miembros de la Red que estuvieran interesados:

- Gobierno electrónico y Telecomunicaciones, creado a iniciativa de la representación de Chile, que ejerce su coordinación.
- Acceso a la Información pública y protección de datos, a iniciativa de la representación de México, que ejerce asimismo, su coordinación.
- Estrategia de la Red, a iniciativa de la representación de Colombia, y coordinado por la Agencia Española de Protección de Datos,.
- Viabilidad de creación de Autoridades de Control en el entorno Iberoamericano, a iniciativa de El Salvador y cuya coordinación recayó en la representación de Argentina.

Estos grupos de trabajo tuvieron ocasión de reunirse en un Seminario organizado al efecto por la AEPD, en el Centro de Formación de la Cooperación Española de Cartagena de Indias, que tuvo lugar durante los días 6 a 9 de junio de 2005, y en él se aprobaron los documentos de trabajo correspondientes a cada uno de los temas citados y que fueron objeto de debate y aprobación en IV Encuentro Iberoamericano de Protección de Datos, que tuvo lugar en México, los días 2 a 4 de noviembre del mismo año.

Este último Encuentro abordó, entre otras, cuestiones relacionadas con el derecho fundamental a la protección de datos personales, las nuevas exigencias de las tecnologías de la información, desarrollos normativos y globalización, los datos de salud como datos especialmente protegidos y la Red Iberoamericana de Protección de Datos.

Además, este Encuentro aportó tres novedades destacadas. En primer lugar, el hecho mismo de que, por primera vez, una entidad miembro de la Red distinta de la Agencia

Española de Protección de Datos, se encargara de acoger en su país y organizar el Encuentro anual.

En segundo lugar, también fue una novedad la apertura de las sesiones a la participación de asistentes que no están integrados en la Red. El amplio número de personas asistentes demuestra la creciente sensibilidad e importancia de las cuestiones relativas a la protección de datos personales.

Y, por último, la presentación para su aprobación formal de documentos de trabajo. Se trata de los documentos elaborados por los Grupos de Trabajo "ad hoc" creados en el III Encuentro y que, tal y como se ha indicado, versaban sobre las siguientes materias: "La Estrategia de la Red", "La viabilidad de creación de Autoridades de Protección de Datos en los países del entorno iberoamericano", "El Acceso a la Información Pública y la Protección de Datos Personales" y "Gobierno Electrónico y Telecomunicaciones".

De entre todos ellos, en este lugar, cabe hacer una referencia especial al documento estratégico de la propia Red, ya que con él se da un paso decisivo en la consolidación estructural de la misma, al establecerse ya formalmente los aspectos relativos a su naturaleza, organización y funcionamiento.

De acuerdo con lo establecido en el Documento Estratégico de la Red, los miembros de la misma representan a instituciones, administraciones y organismos de los países que conforman la Comunidad Iberoamericana que, de alguna forma, contribuyan a promover, impulsar y tomar decisiones en esta tarea legislativa y reglamentaria, así como a los Gobiernos que implementan las políticas de protección de datos y privacidad en cada país.

El documento distingue entre miembros natos, plenos y asociados, recogiendo, asimismo, la figura de los observadores.

Por lo que se refiere al funcionamiento de la Red, el documento estratégico prevé la creación de Grupos de Trabajo, distinguiendo entre los de carácter permanente y los de carácter temporal.

Dentro de los permanentes, se apreció la conveniencia de poner en marcha dos Grupos: uno, de Impulso Normativo y Armonización y otro, sobre la Red "on-line". El primero se encargaría de realizar la labor de asesoramiento y consulta de los responsables gubernamentales y legislativos de cada país, al haberse incorporado dentro de su estrategia una evaluación y asesoramiento continuado sobre las iniciativas regulatorias relacionadas con la protección de datos personales que se produzcan en la región. A través del segundo, la Red llevaría a cabo su papel de educar en el respeto a la protección de datos y difundir la información de los distintos Estados participantes, contando con una tribuna de publicaciones e ideas.

Además se crearon otros dos grupos de trabajo, éstos de carácter temporal: uno, sobre instrumentos de autorregulación y otro, sobre el tratamiento de los datos de salud en relación con la historia clínica, cuyos trabajos se habrán de presentar en el próximo Encuentro Iberoamericano.

Los textos completos de los documentos elaborados por los Grupos de Trabajo, así como la Declaración de México, pueden consultarse en la página web de la Agencia, en la que se encuentran disponibles tanto en castellano como en inglés.

ESTADOS UNIDOS

COOPERACIÓN CON LA COMISIÓN FEDERAL DE COMERCIO LOS ESTADOS UNIDOS

Como ya se informaba en las memorias anteriores, la Ley de Servicios de la Sociedad de la Información y la Ley General de Telecomunicaciones atribuyeron a la AEPD la competencia en materia de supervisión de las comunicaciones comerciales no deseadas o "spam".

Desde entonces, y dada la naturaleza de este fenómeno sin fronteras, la AEPD ha querido fomentar la cooperación global en materia de spam, materializándose esa idea en febrero de 2005 con la firma de un Acuerdo de Cooperación Administrativa para luchar contra el Spam -Memorando Of Understanding (MOU)¹⁶ - con la Comisión Federal del Comercio de los Estados Unidos (Federal Trade Comisión - FTC) organismo federal con competencias supervisoras y de control en los Estados Unidos.

En virtud de este Convenio ambas partes acordaron las siguientes formas de colaboración:

- Facilitar la formación de usuarios y empresas en relación con el spam.
- Promover códigos de conducta sobre buenas prácticas.
- Intercambiar información sobre las soluciones técnicas más avanzadas y mantenerse informados de las novedades.
- Asistencia mutua en las investigaciones.
- Colaboración con las universidades de los respectivos países para promover la investigación, conferencias y cursos formativos sobre la materia así como el establecimiento de prácticas estudiantiles.

En el marco de este acuerdo, y bajo el título "Privacy Protection on Both Sides of the Atlantic" la AEPD impartió conjuntamente con representantes de la FTC un Seminario de postgrado sobre Protección de Datos en la Facultad de Derecho de Georgetown (Washington DC). Este curso es el primero que esta prestigiosa universidad realiza sobre las normas de protección de datos en Europa y su estudio comparado con la legislación de los Estados Unidos. Se llevó a cabo también de forma novedosa ya que buena parte de las sesiones se desarrollaron por video-conferencia y en él participaron como profesores invitados representantes de la Comisión Europea y del Departamento de Seguridad Nacional de los Estados Unidos. A lo largo del seminario se analizaron los

¹⁶ Su texto íntegro se encuentra en:
https://www.agpd.es/upload/Canal_Documentacion/Convenios/Otras_Autoridades/8.%20ACUERDO%20CASTELLANO%20MOU.pdf

temas más importantes que suscita la protección de datos: transferencias internacionales de datos, el Acuerdo de Puerto Seguro (Safe Harbor), así como las medidas destinadas a la prevención y lucha contra el terrorismo.

OTRAS ACTIVIDADES EN EL ÁMBITO INTERNACIONAL

CONFERENCIAS INTERNACIONALES DE PROTECCIÓN DE DATOS

Entre las actividades internacionales de la Agencia, cabe destacar su participación en la Conferencia Internacional de Protección de Datos de Otoño, celebrada en 2005 en Montreux, Suiza.

Esta Conferencia tuvo como resultado la elaboración de la "Declaración de Suiza", que supuso también la continuación de dos seminarios anteriores celebrados en Venecia y Wrocław. En la citada declaración se acuerda garantizar y reforzar la cooperación entre las autoridades de protección de datos, por ello que se solicita a los gobiernos y a las organizaciones internacionales que cumplan con los principios de protección de datos y que cooperen con las autoridades encargadas de su supervisión.

Asimismo, se aprobaron otras dos importantes resoluciones relativas al uso de los datos personales en las comunicaciones con fines políticos y el uso de datos biométricos en pasaportes, documentos de identidad y documentos de viaje¹⁷.

LUCHA CONTRA EL SPAM: CONTACT NETWORK OF SPAM AUTHORITIES Y LONDON ACTION PLAN

En el ámbito europeo, la Agencia Española de Protección de Datos forma parte del grupo Contact Network of Spam Authorities (CNSA). Este grupo, compuesto por las Autoridades nacionales responsables de la regulación y control de las comunicaciones no solicitadas de la Unión Europea y del Espacio Económico Europeo, ha estado preparando durante el año 2005 un documento cuyo objetivo era establecer un marco europeo para el intercambio de información sobre denuncias de Spam entre las autoridades competentes, con indicaciones claras sobre los pasos a seguir ante la recepción de una denuncia de este tipo.

Asimismo, la AEPD ha participado en grupos de trabajo¹⁸ multilaterales sobre la lucha contra el Spam. La primera reunión tuvo lugar en Londres en octubre de 2004, y culminó con la firma del London Action Plan (LAP) por parte de las agencias independientes, ministerios responsables y sectores industriales implicados. Con el LAP se pretende impulsar y favorecer la comunicación para supervisar más eficazmente el cumplimiento

¹⁷ Puede encontrarse más información en la siguiente página web:
<http://www.privacyconference2005.org/>

¹⁸ Para más información sobre estos grupos pueden consultarse las siguientes páginas web:
London Action Plan <http://www.londonactionplan.org/>
OECD Task Force on Spam <http://www.oecd-antispam.org/>

de la ley, informar y educar a los usuarios y consumidores así como favorecer el diálogo con las agencias públicas y el sector privado para actuar conjuntamente e impulsar iniciativas de cooperación.

En 2005 tuvo lugar un taller conjunto entre los miembros del CNSA y los miembros del LAP, en el que se aprobó un modelo de remisión de denuncias de Spam entre autoridades competentes.

GRUPO INTERNACIONAL DE PROTECCIÓN DE DATOS EN TELECOMUNICACIONES (INTERNACIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS- IWGPDPT)

Este grupo de trabajo fue creado por la Autoridad de Protección de Datos de Berlín en 1983 y se reúne con carácter semestral, en primavera y septiembre. El Grupo de Berlín de Telecomunicaciones se configura como un foro de debate abierto que reúne a representantes tanto de las autoridades de protección de datos como de organizaciones internacionales públicas y privadas.

El Grupo de Berlín se caracteriza por anticiparse a los problemas que, en la esfera privada, pueden provocar las nuevas tecnologías y la potencial invasión que éstas pueden producir en la esfera de la intimidad personal.

En la reunión celebrada en septiembre de 2005, el Grupo de Berlín centró su atención en el análisis de los riesgos provocados por el Catching, (recogida temporal en memoria o disco de una determinada información o datos con el objetivo de agilizar el acceso a la información), las etiquetas de identificación por radiofrecuencia RFID o el Weblogging,. Asimismo, se estudiaron las posibles repercusiones que, en materia de privacidad y protección de datos, pueden plantear la tecnología de satélite artificial o la geolocalización de Internet.¹⁹

¹⁹ Para más información puede consultarse la página:
<http://www.datenschutz-berlin.de/doc/int/iwgdpdt/>