

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 el ejercicio de esa competencia, la AEPD lleva a cabo una intensa actividad internacional en distintos ámbitos geográficos participando en diversos foros de debate y consultivos, así como desarrollando actividades de supervisión y cooperación tanto multilateral como bilateralmente.

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, de acuerdo con lo previsto en el artículo 8.1.b del Estatuto de la AEPD, se describen en este apartado de la Memoria cuáles han sido las principales tendencias legislativas, jurisprudenciales y doctrinales en materia de protección de datos en otros países e instituciones.

La Comisión Europea ha seguido la tendencia iniciada en el año anterior de vigilancia de los acuerdos que podríamos llamar "transatlánticos" de transferencia de datos. Además, en este año 2006 ha iniciado la negociación, por mandato de los Estados Miembros, de un Convenio con las autoridades competentes norteamericanas que regulará la transferencia de datos de pasajeros de aerolíneas desde Europa a aquél país con una vocación de permanencia (frente al acuerdo temporal que existe actualmente con vigencia hasta julio de 2007). En esta misma línea de actividad, la Comisión Europea interviene, desde la aparición en julio de 2006 de un nuevo caso de transferencias transatlánticas no autorizadas en materia financiera, junto con las autoridades de protección de datos de los Estados Miembros, para poner fin a la posible situación de ilegalidad creada. La información pormenorizada sobre las actividades de la Comisión se puede consultar en el 10º Informe Anual del Grupo del Artículo 29.

En el entorno de los Estados Miembros de la Unión Europea se observa la creciente tendencia de las autoridades encargadas de la lucha contra delitos de terrorismo y formas graves de criminalidad a disponer en sus investigaciones del mayor número posible de información personal relacionada con el uso de las telecomunicaciones, posibilidad prevista en la Directiva Europea de Retención de Datos (D 2006/24/EC). La transposición a los ordenamientos internos de esta Directiva ha constituido durante este año una tarea esencial de los legisladores nacionales. Se observa igualmente una creciente actividad normativa en el ámbito de los documentos y sistemas

de identificación digital (ya sean a los efectos de simple identificación o para acceder a servicios sanitarios o de gobierno electrónico). Los diferentes desarrollos normativos en los distintos países se incluyen en el informe anual del Grupo de Autoridades Europeas de Protección de Datos correspondiente al año 2006 .

En el ámbito Iberoamericano se observa un desplazamiento desde el sector jurídico-público al económico para impulsar sus estándares de protección de datos a los de la Unión Europea, favoreciendo de esta forma el libre de flujo de información entre los actores económicos, requisito necesario para las transacciones comerciales en ambos continentes. En este proceso, la AEPD ha iniciado en 2006 los contactos con la Corporación para el Fomento de la Economía de Chile para prestar la asistencia técnica necesaria para alcanzar dichos objetivos y con el Instituto Federal de Acceso a la Información Pública de México. Los desarrollos normativos en materia de protección de datos producidos en los distintos países de la región pueden consultarse en la información comparada elaborada por la Secretaría de la Red Iberoamericana, labor que desarrolla esta AEPD.

Por lo que se refiere a los Estados Unidos, desde la aprobación de la CAN SPAM ACT en 2003 por la que se establecieron claras normas de protección de la privacidad en las comunicaciones comerciales electrónicas y se encomendó dicha misión a la Comisión Federal del Comercio de los US (FTC), la tendencia a incrementar y hacer efectiva esta protección ha sido creciente. En el año 2006 se ha producido un nuevo desarrollo normativo que favorece una cooperación internacional efectiva con otras autoridades de protección de datos, la SAFE WEB ACT, ya que permite a la FTC mantener la confidencialidad de la información facilitada por otra autoridad en el curso de investigaciones relacionadas con infracciones de privacidad en telecomunicaciones.

I. 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 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.

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.

Uno de los temas de los que el GT29 se ha ocupado repetidamente desde el año 2002 ha sido la transferencia de datos de pasajeros con destino a los Estados Unidos, el asunto PNR. En 2006 la evolución ha sido la siguiente:

El 30 de mayo de 2006, el Tribunal de Justicia de la Unión Europea emitió la sentencia por la que se resolvía los dos recursos de anulación presentados por el Parlamento Europeo en julio de 2004. Los recursos argumentaban la anulabilidad tanto de la Decisión de la Comisión Europea declarando el nivel adecuado de protección de datos de EEUU como de la Decisión sobre el Acuerdo Internacional firmado con las autoridades americanas para dotar de base legal a la transmisión de datos PNR de los pasajeros. Ambos recursos fueron presentados individualmente pero fueron acumulados por el Tribunal de Justicia, que estimó, por defecto de forma, los dos recursos y ordenó la denuncia del acuerdo con EEUU.

En junio de 2006, el GT 29 aprobó una opinión en la que ponía de manifiesto los principales elementos de preocupación que surgían tras esta nueva situación, en la que a partir del 30 de septiembre de 2006, fecha límite en la que el Acuerdo debía ser denunciado, las transmisiones de datos por parte de las aerolíneas dejaban de tener base legal. Los principales aspectos señalados por la opinión fueron:

- Los acuerdos bilaterales entre EEUU y los Estados miembros de la UE deben evitarse.
- Todo nuevo acuerdo debe, al menos, preservar e integrar el actual nivel de protección de los datos tal y como se recoge en los compromisos de EEUU de 2004 y tener en cuenta las consideraciones críticas hechas públicas por el GT 29 en sus opiniones previas sobre PNR, incluyendo la cuestión de la reducción de datos.
- El sistema "push", por el que los datos son enviados en vez de permitir el acceso a los sistemas de reserva (sistema "pull"), es el que debe ser implementado.
- Es necesaria la limitación estricta de la finalidad para la transmisión que se haga a partir de ahora de datos PNR.
- El GT29 espera que el mecanismo de una revisión conjunta anual se mantenga, en línea con el actual acuerdo.

Otro asunto importante referido a las relaciones transatlánticas que ha sido objeto de especial atención por parte del GT29 durante el año 2006 es el conocido como caso SWIFT.

En junio de 2006 diversas informaciones en los medios de comunicación desvelan la existencia de un programa por el que el Gobierno de EEUU ha tenido acceso a los datos

relativos a transferencias bancarias internacionales realizadas a través de la Sociedad SWIFT en el marco de la lucha contra el terrorismo. Asimismo, una denuncia fue formalmente presentada ante las autoridades de protección de datos de 33 países, entre ellos España, con vistas a destapar un caso en el que la privacidad de los ciudadanos europeos se veía seriamente dañada. SWIFT es una sociedad cooperativa con sede en Bélgica, cuyo Derecho le es de aplicación, pero tiene oficinas, que se desvelaron de carácter puramente comercial, en otros países, entre ellos España. Es por ello que la AEPD ha participado activamente en la investigación de los hechos denunciados, pero ello en el marco de las actuaciones de inspección realizadas por la autoridad belga, competente en este caso.

El GT 29, por su parte, aprobó una opinión en la que se estableció tanto la responsabilidad de SWIFT como de las instituciones financieras que utilizan sus servicios en la transmisión de los datos a EEUU para una finalidad distinta de para la que fueron recabados. Y ello porque, mientras los datos eran recogidos por los bancos con vistas a realizar la transferencia solicitada por los clientes, esa información era posteriormente enviada al Departamento del Tesoro de EEUU que la podía utilizar en su lucha contra el terrorismo.

Asimismo, el GT 29 instaba a SWIFT a cesar esa transferencia ilegal de datos, máxime cuando los clientes de las entidades financieras ni siquiera tenían información de que la transmisión de los datos se estuviera produciendo.

Una cuestión de especial relevancia analizada en 2006 por el GT 29 ha sido la retención de datos en las comunicaciones electrónicas.

Como ya mencionamos en las memorias de la Agencia Española de Protección de Datos de 2004 y 2005, la cuestión de la retención de datos de las comunicaciones electrónicas ha estado situada al más alto nivel en la agenda política europea hasta la adopción final de la Directiva 2006/24 CE de 15 de marzo de 2006. En marzo de 2006, el GT 29 aprobó una nueva opinión con la que reaccionaba a la aprobación formal de la Directiva. En la misma, se reiteraban las garantías que debían ser adoptadas para evitar la vulneración de los derechos fundamentales de los ciudadanos y se instaba a las autoridades nacionales a desarrollar un papel activo en la defensa de los mismos en los procesos de transposición interna de la Directiva. En definitiva, las autoridades volvieron a señalar los siguientes elementos de preocupación:

- Toda restricción al derecho fundamental a la confidencialidad de las comunicaciones, debe estar justificada por una necesidad apremiante, sólo debe permitirse en casos excepcionales y deberá contar con las garantías adecuadas. La finalidad debe ser la lucha contra el terrorismo y la delincuencia organizada, dejando atrás términos excesivamente ambiguos.
- El acceso a los datos deberá ser autorizado caso por caso por una autoridad judicial, sin perjuicio de aquellos países en los que sea posible el acceso autorizado por ley y bajo una supervisión independiente. Los destinatarios de la información debe ser únicamente las autoridades policiales específicamente designadas.

- 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.

Otros asuntos de interés examinados por el GT29 se refieren a las siguientes materias:

■ LOS FICHEROS CREADOS EN APLICACIÓN DE LA LEY SARBANES-OXLEY

En virtud de esta ley norteamericana los Comités de Auditoría de las empresas que cotizan en la Bolsa de Nueva York deben dar curso a todas aquellas informaciones de sus empleados que denuncien casos de corrupción o malas prácticas en la empresa. A los efectos de protección de datos esto supone la creación de ficheros con información sobre posibles vulneraciones de la legalidad por parte de los trabajadores de una empresa (ficheros de integridad).

El GT 29 analizó las implicaciones de estos ficheros en su Dictamen 1/2006 y puso de relieve que el establecimiento de estos sistemas debían hacerse de acuerdo con los principios establecidos en la Directiva 95/46/CE, garantizando el derecho fundamental a la protección de datos personales, tanto respecto del denunciante como del denunciado.

■ FILTRACIÓN DE CORREO ELECTRÓNICO

Consciente de la expansión de los distintos servicios de comunicación en línea -como los servicios de correo electrónico gratuitos de la red- en febrero de 2006, el GT 29 adoptó el "Dictamen 2/2006 del Grupo de trabajo 29 sobre el respeto de la privacidad en relación con la prestación de servicios de cribado de correo electrónico" en el que examina las disposiciones sobre confidencialidad de las comunicaciones electrónicas previstas en la Directiva 2002/58 CE sobre la privacidad en las telecomunicaciones, transpuesta a la legislación española en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Tanto los proveedores de servicios de Internet, como los prestadores de servicios de correo electrónico llevan a cabo una práctica habitual de inspección y filtración de las comunicaciones con el fin de eliminar el correo masivo no solicitado, virus, así como la detectar contenidos concretos.

El principal objetivo de este documento es servir de guía para que estas prácticas se lleven a cabo respetando la intimidad de las comunicaciones por correo electrónico y, más en concreto, en el del filtrado de las comunicaciones en línea, estableciendo, por ejemplo, la obligación de informar a los abonados sobre el tratamiento de sus datos personales.

■ E-CALL

El servicio e-call supone un servicio paneuropeo de llamada desde el vehículo que utiliza el número de llamada de urgencia europeo 112 en caso de accidente, y que se crea bajo la iniciativa "eSafety" en una Comunicación de la Comisión del año 2002.

A fin de responder a las cuestiones relativas a la intimidad y la protección de datos que plantea el despliegue de este sistema, se consideró necesario el análisis de la situación, por lo que el GT 29 aprobó el "Documento de trabajo sobre la protección de datos y las consecuencias para la intimidad en la iniciativa eCall". El objetivo del presente documento de trabajo se enfoca a exponer las preocupaciones que en materia de protección de datos y derecho a la intimidad suscitan estos servicios, recomendando su posible introducción con carácter voluntario.

■ REVISIÓN DEL PAQUETE REGULADOR DE TELECOMUNICACIONES

En contestación a la Consulta Pública que realizó la Comisión Europea concerniente al paquete regulador de las Directivas de Telecomunicaciones, entre las que se encuentra la Directiva 2002/58/CE de privacidad en las comunicaciones, el GT 29 contribuyó con la aprobación del "Dictamen 8/2006 sobre la revisión del marco regulador de las redes y los servicios de comunicaciones electrónicas, con especial atención a la Directiva sobre la privacidad y las comunicaciones electrónicas", en el que se aportaban una serie de observaciones, tanto generales, en torno al tratamiento de los datos personales que se realizan en comunicaciones electrónicas o a través de las mismas, como específicas, sugiriendo, por ejemplo, que se abordaran en la Directiva temas relacionados con las aplicaciones en línea, entre los que se incluyen cuestiones de seguridad o la responsabilidad de los operadores, así como una aclaración de la personalidad jurídica tanto de los proveedores de infraestructuras de acceso y de los proveedores de servicios como de los responsables del tratamiento de los datos. Además, el GT 29, propone la mejora de las medidas de seguridad, pero no apoya ninguna medida que lleve o pueda llevar a incrementar la vigilancia o a bloquear los contenidos.

■ DIRECTORIOS WHOIS

Los directorios Whols permiten obtener acceso público e información sobre direcciones IP y nombres de dominio registrados, con la finalidad de facilitar información en caso de incidentes informáticos y así contactar con el responsable técnico de otra red o de otro dominio. No obstante, este servicio puede asimismo ser utilizado por un potencial atacante con el fin de recabar información y enviarle spam. Debido a los problemas que de forma intrínseca plantean este tipo de sistemas, los directorios Whols ya habían sido analizados con anterioridad por el GT 29 en el dictamen 2/2003 (WP 76), en el que se examinaban los aspectos jurídicos que se plantean cuando son los particulares los que registran nombres de dominio y estos no son los mismos que las empresas u otras personas jurídicas las que lo hacen.

La AEPD, que tiene la competencia de investigación en materia de lucha contra el spam, ha participado en los debates que han surgido en el seno del Governmental Advisory

Committee, que asesora a ICANN (Internet Corporation for Assigned Names and Numbers) en el que se han dado unas pautas para la utilización de los servicios globales de Whols. Durante el año 2006, los debates han estado centrados en la publicidad o no de todos los datos Whols puesto que, si bien entre las finalidades iniciales de estos directorios no estaba contemplada la investigación, en muchas ocasiones estos servicios suponen la base para la averiguación de un delito y son utilizados por las autoridades competentes. Por otro lado, la publicación de estos datos puede provocar una invasión en la esfera privada del individuo, debiendo estos directorios de observar las disposiciones que en materia de protección de datos establece no sólo la Directiva, sino también las distintas leyes nacionales, que recogen principios como la finalidad.

La AEPD, en línea con el GT 29, ha defendido en estas reuniones, que si bien existe la necesidad de acceso a estos datos por parte de las autoridades competentes, de esta no subyace la exigencia de un acceso online, por lo que la solución ideal sería un acceso por niveles o privilegios a estas bases de datos, tal y como se hace en Reino Unido y Francia.

■ DATOS DE SALUD

El GT 29 ha venido trabajando en los últimos dos años en aportar directrices de protección de datos que se tengan en cuenta al regular la incorporación de las historias clínicas a soportes electrónicos, ya que este sistema de historia clínica electrónica se está generalizando en todos los Estados Miembros.

Al cierre de esta Memoria se ha aprobado el documento de trabajo que se ha sometido a consulta pública y que puede encontrarse en la página web del GT 29.

■ ENFORCEMENT TASK FORCE

El primer informe sobre la implementación de la Directiva 95/46/CE (mayo de 2003) puso de manifiesto un déficit de capacidad efectiva para hacer cumplir la ley (enforcement) en varios Estados Miembros e importantes carencias en la función supervisora de algunas autoridades. En este contexto el GT 29 acordó realizar una actuación coordinada, emprendida por todas las Autoridades de los Estados Miembros, y que se planificaría en el marco del subgrupo de trabajo de Enforcement Task Force. Este subgrupo analiza la capacidad de aplicar y ejecutar las normas de protección de datos por parte de las Autoridades supervisoras y se crea a raíz de la "Declaración del Grupo del artículo 29 sobre el control de la aplicación de la legislación", del 25 de noviembre de 2004.

La actuación sincronizada se dirige al sector del seguro privado de salud, y se centra en el análisis de la información obtenida a través de un cuestionario común que se cumplimentará por las compañías seleccionadas en todos los Estados Miembros. Durante el año 2006, con las respuestas al cuestionario, las autoridades de protección de datos elaboraron un informe nacional en el que se analizaban los resultados obtenidos. La AEPD ha contribuido de manera especial en todas las fases de esta actuación conjunta dada su amplia experiencia en inspecciones sectoriales.

PROPUESTAS LEGISLATIVAS RELEVANTES

A continuación se recogen las novedades normativas más importantes en el ámbito comunitario:

PROPUESTA DE MODIFICACIÓN DEL PAQUETE DE DIRECTIVAS DE TELECOMUNICACIONES

En junio del año 2006, la Comisión Europea aprobó una Comunicación en relación con la revisión que se ha llevado a cabo del marco regulador de las telecomunicaciones (SEC (2006) 81). En esta comunicación se informaba sobre el funcionamiento del paquete de directivas que regulan las redes y servicios de comunicaciones electrónicas, y se identifican áreas en las que es necesario introducir algún cambio.

La Comunicación se complementaba con un Documento de Trabajo de los servicios de la Comisión ("Comission Staff Working Document"), que establece en mayor detalle los posibles cambios al marco regulador y un documento de Valoración del Impacto ("Impact Assesment"). En estos dos documentos se recogen las conclusiones de las aportaciones realizadas por los agentes implicados.

Con todas las aportaciones, la Comisión elaboraría propuestas legislativas para la modificación del marco regulador, y que se presentarán al Parlamento Europeo y al Consejo.

El actual marco europeo de las comunicaciones electrónicas está formado por un paquete de 5 Directivas relativas a los servicios de comunicación que se transfieren electrónicamente, por tecnología wireless o fija, por datos o por voz, basada en Internet o en circuito cerrado, empresarial o personal. Estas normas europeas están creadas para estimular la competencia y crear oportunidades para las nuevas compañías. Pretenden una reducción de precios y a una gama más amplia de productos y de servicios para el consumidor. Este marco normativo entró en vigor en el año 2002 teniendo que ser transpuesto en los Estados miembros antes de julio de 2003. Las Directivas son las siguientes:

- Directiva 2002/19/CE de 7 de marzo de 2002 relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (Directiva acceso).
- Directiva 2002/20/CE de 7 de marzo de 2002 relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva autorización).
- Directiva 2002/21/CE de 7 de marzo de 2002 relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónica (Directiva marco).

- Directiva 2002/22/CE de 7 de marzo de 2002 relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal).
- Directiva 2002/58/CE de 12 de julio de 2002 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).

Es precisamente respecto a esta última, la denominada Directiva de privacidad en las telecomunicaciones, sobre la que se proponen los cambios que a continuación se resumen:

- Mejora de los mecanismos de aplicación previstos en el marco regulador,
- Seguridad,
- Obligación de adoptar medidas de seguridad y concesión de competencias a las Autoridades nacionales de regulación para que puedan determinar y controlar la aplicación técnica, y
- Notificación de las violaciones de la seguridad por los operadores de la red y los proveedores de servicios de Internet.

Como se avanzaba en el punto relativo al trabajo llevado a cabo por el Grupo de Trabajo del Artículo 29, este contestó a la Consulta pública con el fin de interpretar y desarrollar los cambios propuestos a la Directiva 2002/58/CE de privacidad en las comunicaciones.

Las observaciones del GT 29, así como toda la documentación relativa a la consulta pública llevada a cabo por la Dirección General de la Sociedad de la Información está disponible en el siguiente hipervínculo:

http://ec.europa.eu/information_society/policy/ecommm/info_centre/documentation/public_consult/index_en.htm#communication_review

EL TRATADO DE PRÜM

El Tratado de Prüm, firmado en la ciudad alemana del mismo nombre en mayo de 2005, tiene como objetivos la profundización de la cooperación fronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la inmigración ilegal. Los actuales países signatarios son Bélgica, Holanda, Luxemburgo, Francia, España, Alemania y Austria (siendo estos dos últimos los únicos que ya han completado el proceso de ratificación del Tratado), pero ya han mostrado su interés en participar en el mismo Italia, Finlandia, Portugal y Polonia.

El Tratado prevé el intercambio de datos de ADN, huellas dactilares, matriculación de vehículos y otros datos que pudieran ser ulteriormente necesitados con vistas al cumplimiento de los fines del Tratado. Respecto de los datos de ADN se deberán crear índices de referencia sobre los datos contenidos en los ficheros de análisis de ADN nacionales a los que podrán acceder de forma automatizada las otras partes contratantes. La consulta de índices de referencia se realizará sólo para casos concretos y de acuerdo con el Derecho de la parte que realice la consulta. En caso de concordancia, la transmisión de otros datos de carácter personal se hará de acuerdo con el derecho interno de la parte requerida y siguiendo los mecanismos de cooperación policial previstos en el Tratado de la Unión Europea. Las consultas automatizadas de los datos de huellas dactilares también se harán a través del acceso a índices de referencia.

Otras disposiciones del Tratado se refieren a:

- Medidas para la prevención de atentados terroristas: se prevé la transmisión de datos, sin que medie petición previa, cuando existan hechos que justifiquen la presunción de que la persona en cuestión vaya a cometer alguno de los delitos contenidos en la Decisión Marco de lucha contra el terrorismo.
- Medidas contra la migración ilegal: incluyendo la organización de vuelos conjuntos de repatriación.
- Asistencia en caso de catástrofes, accidentes graves y grandes eventos de carácter transfronterizo, así como otras formas de intervención conjunta.

El Tratado recoge, en un capítulo específico, unas pautas para la protección de los datos manejados en el curso de la aplicación del Tratado cuyos rasgos más destacados son: un nivel mínimo de protección fijado en el Convenio 108 del Consejo de Europa, limitación estricta del principio de finalidad, cancelación de los datos una vez haya desaparecido la finalidad de la transmisión, acceso a los datos a través de un único punto de contacto nacional, así como el reconocimiento al titular de los datos de los derechos de acceso, rectificación y cancelación y de acudir a un Tribunal o a una autoridad de control independiente en caso de vulneración de los derechos.

Por su parte, la AEPD ha participado en diversas reuniones a nivel europeo con vistas a hacer valer los principales elementos de preocupación detectados en este Tratado, sobre todo relativos a las necesarias salvaguardias que deben adoptarse en lo que a la transmisión de datos de ADN se refiere y el escrupuloso cumplimiento del principio de finalidad.

MODIFICACIÓN DE LA BASE JURÍDICA DE EUROPOL

El 20 de diciembre de 2006 fue presentada la propuesta de Decisión del Consejo por la que se crea la Oficina Europea de Policía (EUROPOL) (COM(2006) 817). La idea que subyace de la modificación de la base jurídica por la que se regula Europol es

la necesidad de dotarle de nuevas competencias que le permitan hacer frente a las demandas en materia de seguridad en el marco de la coordinación y colaboración entre Estados miembros. Esta necesidad de ir adecuando la actividad de Europol a las materias en el ámbito de la cooperación policial que vayan manifestándose como imprescindibles hace necesario dotar a Europol de un instrumento de adaptación y funcionamiento ágil que evite procedimientos extremadamente complejos que dificulten su actuación.

El Convenio Europol, aprobado en 1995, ha sido objeto de modificación hasta el momento por tres protocolos, ninguno de los cuales está aún en vigor, y ello precisamente por la necesidad de que sean ratificados por todos los Estados miembros. Una lentitud en la tramitación que obstaculiza en gran medida la eficacia de la labor de Europol.

La propuesta de Decisión, actualmente en fase de tramitación en la que se contará con la intervención del Parlamento Europeo, ha sido también abordada por la Autoridad Común de Control de Europol, que el 5 de marzo de 2007 aprobó una opinión cuyos elementos más esenciales son:

- El proyecto distingue entre los objetivos de Europol-apoyar y reforzar la cooperación entre Estados Miembros para la lucha contra el terrorismo y los delitos graves- y las competencias de Europol, que quedan limitadas a los casos que afecten a dos o más Estados Miembros. En juicio de la ACC el objeto de esta distinción debe clarificarse, así como las consecuencias que pueda conllevar para las estructuras de información de Europol.
- El tratamiento por Europol de datos puestos a disposición por entidades públicas y privadas debe hacerse bajo la condición de que las solicitudes de información se dirijan a las unidades nacionales, que examinarán la solicitud.
- Deben especificarse las diferentes responsabilidades de Europol en materia de protección de datos cuando el tratamiento de los datos tenga lugar fuera de sus instalaciones (en el seno de equipos conjuntos de investigación).
- El texto de la Decisión debe mencionar la finalidad del Sistema de Información Europol, así como la necesidad de consultar la ACC.
- También se debe introducir la obligación de consultar la Autoridad Común de Control y otras Autoridades de Supervisión afectadas antes de que se adopte cualquier decisión relativa a la interconexión del sistema de información de Europol con otros sistemas.
- Se debe realizar una revisión anual de los datos contenidos en los ficheros de análisis.
- La comunicación de datos a órganos terceros debe contar con un procedimiento de consulta a la ACC.

- El derecho de acceso debe garantizarse, debiendo Europol responder a la solicitud en un plazo breve.

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

La Autoridad Común de Control (ACC) de Schengen mantuvo a lo largo de 2006, continuados debates sobre la modificación de la base jurídica del Sistema de Información Schengen (SIS). A las opiniones que ya se aprobaron cuando la propuesta fue presentada en 2005 se unió otra opinión a probada en septiembre de 2006 que incidía sobre los elementos de preocupación que se iban poniendo de manifiesto a medida que avanzaban las negociaciones en el Consejo. Estos aspectos preocupantes eran, principalmente, el acceso al SIS por parte de los servicios secretos de los Estados miembros, la supervisión del sistema una vez que desaparezca la ACC tras la entrada en vigor del nuevo SIS y el acceso a la información por parte de EUROPOL.

Por su parte, la ACC de Europol organizó el 17 de octubre una Conferencia en la que se pretendía abordar el futuro de la Oficina Europea de Policía, sobre todo en el marco de la posible modificación de su base jurídica - lo que se materializó con la propuesta de 20 de diciembre de 2006 expuesta anteriormente-. En esta Conferencia se puso de manifiesto que toda nueva atribución de competencias a Europol debía estar unida al establecimiento de nuevas medidas para proteger los datos que sean objeto de tratamiento. Asimismo, Europol debía seguir siendo objeto de inspecciones periódicas por parte de las Autoridades de control con vistas a salvaguardar que tanto los ficheros de análisis como el Sistema de Información Europol contaban con un sistema adecuado de garantías.

Por último, la AEPD ha colaborado durante el 2006 en la inspección del sistema central Eurodac que está llevando a cabo el Supervisor Europeo de Protección de Datos, responsable del sistema. Esta colaboración se ha materializado a través del envío de información sobre los mecanismos de obtención de las huellas dactilares de los solicitantes de asilo o extranjeros detectados en situación irregular en España así como su transmisión al sistema central.

OTRAS ACTIVIDADES EN EL MARCO EL TERCER PILAR

La AEPD participa activamente en las reuniones del denominado Grupo de Trabajo de Policía que, en el marco del mandato otorgado anualmente por la Conferencia de Primavera, centra sus debates en las propuestas legislativas en curso sobre el tratamiento de datos con fines policiales. Durante el año 2006, el Grupo de Trabajo de Policía ha debatido sobre el concepto de disponibilidad, utilizado para describir el

marco en el que se debe producir el intercambio de información entre las fuerzas del orden público. Y ello por cuanto las últimas propuestas legislativas ya incluyen en su texto que toda información en manos por la policía de un Estado Miembro debe poder estar disponible para sus homólogos de otro Estado Miembro. Los mecanismos en que se articula esta disponibilidad y las garantías que deben proteger esa información han sido debatidas por las autoridades de protección de datos que han puesto reiteradamente de manifiesto que el intercambio de información no puede derivar, en ningún momento en una disminución en las garantías de protección de los datos personales de los ciudadanos.

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). El citado Comité celebró su reunión plenaria número 22 los días 8 a 10 de marzo de 2006.

En dicha reunión se repasó la actividad llevada a cabo por el Consejo de Europa y se adoptaron las futuras líneas de actuación del Comité.

Así, a partir de la adopción en 2005 del 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, se encomendó al Bureau del comité Consultivo (T-PD-BUR), en su condición de órgano de preparación y discusión previa de los documentos que se someten posteriormente al plenario, la elaboración de un documento que estableciera los principios básicos para la determinación de los conceptos de tratamiento automatizado y responsable del tratamiento en el marco de las redes globales de telecomunicaciones. Del mismo, se acordó la realización de distintos documentos con la aplicación de los criterios de adecuación en materia de transferencias internacionales de datos, tomando en consideración los trabajos llevados a cabo en el seno de la OCDE, y los tratamientos que implican el establecimiento de perfiles.

Por otra parte, se continuaron los trabajos, iniciados durante el año anterior, en relación con la propuesta de formalización del derecho a la protección de datos como derecho fundamental (que se ha declarado autónomo en algunos países como España y Portugal) mediante un instrumento propio del Consejo de Europa para garantizar el acceso al Tribunal Europeo de Derechos Humanos (TEDH), tomando esencialmente en consideración el análisis ya realizado de la jurisprudencia del Tribunal en esta materia.

Igualmente, durante la reunión del plenario, fueron objeto de debate cuestiones relacionadas con la aplicación de los principios del Convenio 108 al tratamiento de datos biométricos, tomando en consideración el informe elaborado sobre esta materia y sometido al plenario en el año 2005, así como las implicaciones que para el derecho fundamental a la protección de datos revise la lucha contra el terrorismo.

Por último, el Comité ofreció todo su apoyo para la efectiva implantación del día europeo de la protección de datos, finalmente establecido el día 28 de enero, en conmemoración de la adopción del Convenio 108.

RELACIONES BILATERALES EN EL ÁMBITO EUROPEO

Del mismo modo se mantienen en 2006 las tradicionales relaciones con la Autoridad de Protección de Datos de Portugal, con la que la AEPD se reunió en dos ocasiones a lo largo del año 2006. En la primera de las reuniones, celebrada en enero en San Lorenzo de El Escorial, y como continuación de los trabajos llevados a cabo en el anterior encuentro, se compararon las visiones de ambas autoridades respecto a la utilización de datos para estudios de investigación científica y ensayos clínicos. Además, se trabajó sobre las experiencias de ambas delegaciones en relación con los tratamientos realizados en aplicación de la Ley Sarbanes-Oxley, y contrastando los avances que los respectivos países han tenido en su administración electrónica.

En el segundo de los encuentros, celebrado en Óbidos (Portugal) en diciembre de 2006, se debatieron los flujos internacionales de datos, concluyendo ambas autoridades que es necesario encontrar formas flexibles que se adapten a la creciente circulación de información y de prestación de servicios, que han de mantener un nivel adecuado de protección de datos.

Además, durante el encuentro, ambas autoridades compartieron sus visiones respecto a la seguridad en los mercados financieros y las "líneas de integridad" para las empresas que cotizan en la Bolsa de Nueva York coincidiendo en la necesidad de notificación, fundamento jurídico, así como el necesario cumplimiento con los derechos de los trabajadores.

A lo largo de 2006 la AEPD ha participado en el proyecto Twinning Light que ha desarrollado la República Checa en Bosnia-Herzegovina.

Asimismo, 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 AEPD participó en el seminario organizado en el mes de octubre por la Dirección General de Ampliación de la Comisión Europea a través de TAIEX (Instrumento de Asistencia Técnica e Intercambios de Información) en la nueva República de Montenegro, independiente desde mayo de ese mismo año y país candidato a incorporarse a la UE.

El seminario en el que, junto con representantes de varias autoridades europeas de protección de datos participaban también representantes de la Comisión Europea, se dirigía a responsables de los Ministerios de Telecomunicaciones, Interior, Justicia y Empleo de esa nueva República y su objetivo era proporcionar información y asistencia en

materia de protección de datos de cara a una eventual incorporación de Montenegro a la Unión Europea.

II. IBEROAMERICA

LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS

La Red Iberoamericana de Protección de datos 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), que 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 el 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.

Por ello la Red se crea como un foro permanente cuyo objetivo es potenciar las iniciativas de intercambio de experiencia entre los países iberoamericanos, estableciendo canales siempre abiertos de diálogo y colaboración en materia de protección de datos. La Secretaría de la Red la ostenta la Agencia Española de Protección de Datos que proporciona el soporte organizativo a este foro de dialogo. La Red cuenta con representación de entidades de 19 países de los 22 que integran la Comunidad Iberoamericana. Entre los objetivos de la Red, destaca especialmente su labor tendente a impulsar la elaboración de los instrumentos normativos necesarios para garantizar este importante derecho fundamental en aquellos países de la Comunidad Iberoamericana en los que aún no se ha emprendido esta regulación.

En mayo de 2006, la AEPD, en colaboración con la Agencia Española de Cooperación Internacional y la Fundación Internacional y para Iberoamérica de Administración y Políticas Públicas, reunió en Santa Cruz de la Sierra, Bolivia, a representantes de 12 países miembros la Red Iberoamericana de Protección de Datos.

Durante el encuentro los participantes, que se reunieron en los cuatro grupos de trabajo creados en el IV Encuentro Iberoamericano de protección de datos, celebrado en México en 2005, sobre "Impulso Normativo y Armonización", "La Red On-line" "Instrumentos de Autorregulación" y "Tratamientos de Datos de Salud", elaboraron distintos documentos de trabajo que serán sometidos a aprobación en el próximo encuentro de la Red que se celebrará en el primer semestre de 2007.

Entre las principales conclusiones recogidas en dichos documentos destacan:

- Es necesario adoptar medidas que garanticen un nivel de protección adecuado en todos los países iberoamericanos con el objetivo de que exista una armonización normativa entre los Estados que permita el flujo de información necesario para el correcto desarrollo del mercado. En este sentido, se asumió el compromiso de elaborar una propuesta de directrices para la armonización de la regulación de la protección de datos en la comunidad Iberoamericana, y colaborar mediante el asesoramiento con los países que adopten iniciativas legislativas en este ámbito.
- La finalidad principal de la historia clínica debe ser el de facilitar la asistencia sanitaria de forma que consten en ella todos aquellos datos que permitan un conocimiento veraz y actualizado del estado de salud. La obtención, uso, archivo, custodia y transmisión de los datos de salud contenidos en ella exigen instrumentos adicionales de garantía y deben responder a principios básicos tales como el respeto a la dignidad de la persona, la autonomía de su voluntad y su intimidad, y la protección de los datos personales. No obstante, el principio básico del consentimiento de la persona puede verse limitado cuando tal limitación constituya una medida necesaria por razones de interés general reconocidas en una norma con rango de Ley. Asimismo, se concluyó que los sistemas sanitarios han de prever garantías de movilidad mediante el establecimiento de sistemas de intercambio de información de salud entre los distintos organismos, centros y servicios del sistema sanitario, que garanticen la adecuada asistencia sanitaria cuando los ciudadanos se desplacen por el territorio nacional.
- Las iniciativas de autorregulación, entendidas como complemento a un marco normativo previamente definido por el Estado, pueden ofrecer un valor añadido en la protección de datos personales. Estos mecanismos pueden añadir garantías adicionales a las contempladas en las regulaciones, contribuir a la consolidación de una cultura de protección de datos y fomentar el tratamiento correcto de la información personal en la medida en que aporten un valor añadido y tengan efectividad práctica. Es por ello que se recomienda la incorporación en los textos legales sobre protección de datos de disposiciones explícitas tendentes a utilizar mecanismos de autorregulación, la promoción de su publicidad, y el establecimiento de medidas efectivas en caso de incumplimiento de estas normas.
- Por último, la dispersión geográfica de los miembros de la Red hace preciso dotarla de mecanismos ágiles y eficaces para mantener la fluidez en este intercambio de experiencias e informaciones. Por este motivo, durante la celebración del Seminario Iberoamericano fue presentado el proyecto de la Red "on line". El objetivo principal de este proyecto es contar con un instrumento virtual de la Red Iberoamericana en el desarrollo y la divulgación de sus actividades, la difusión del derecho fundamental a la protección de datos en Iberoamérica y configurar un sistema de intercambio de información entre sus miembros.

III. ESTADOS UNIDOS

COOPERACIÓN CON LA COMISIÓN FEDERAL DE COMERCIO DE LOS ESTADOS UNIDOS

La Agencia viene desarrollando desde el año 2005 una cooperación efectiva con la Comisión Federal del Comercio (FTC) de los Estados Unidos, entidad competente para luchar contra los fraudes a los consumidores y las violaciones de las normas sobre comunicaciones comerciales electrónicas. La existencia de ámbitos comunes de actuación y la similitud de métodos y facultades para conseguir el cumplimiento de la ley hicieron posible la firma de un Acuerdo de Entendimiento entre ambos organismos.

Una aplicación esencial y práctica del mismo es la difusión de las normas de privacidad y protección de datos en los foros académicos universitarios de los respectivos países. Durante el otoño de 2006, representantes de la Agencia y de la FTC impartieron en la Facultad de Derecho de la Universidad de Georgetown (Washington DC) un seminario de derecho comparado sobre la protección de datos en ambos lados del Atlántico. Su objetivo no es solo comparar los modelos normativos europeo y americano sino también explicar a los futuros profesionales del derecho en los Estados Unidos, los métodos de trabajo que utilizan las autoridades de supervisión para hacer cumplir las normas de protección de datos y cómo pueden cooperar mutuamente.

IV. OTRAS ACTIVIDADES INTERNACIONALES

CONFERENCIAS INTERNACIONALES DE PROTECCIÓN DE DATOS

Los días 24 y 25 de abril de 2006 tuvo lugar en Budapest la Conferencia de Primavera de las Autoridades Europeas de Protección de Datos. Esta Conferencia se celebra anualmente en Europa y tiene como finalidad el análisis de todas aquellas cuestiones, legislativas o tecnológicas, que puedan afectar a la privacidad de los ciudadanos europeos con el objetivo de buscar soluciones armonizadas en dicho ámbito.

En su reunión de 2006 se abordaron temas como la tecnología de identificación por radiofrecuencia (RFID), las denominadas "líneas de integridad" puestas actualmente en marcha en numerosas empresas o la centralización de la información sanitaria y la tarjeta sanitaria electrónica. Como también viene siendo habitual en las últimas conferencias europeas, las autoridades de protección de datos debatieron sobre el tratamiento de datos de carácter personal por las fuerzas de seguridad pública, a cuyos efectos

aprobaron una declaración de aplicación al tratamiento de datos en el III Pilar. En la misma, se hizo hincapié en que la utilización de la información disponible para las fuerzas policiales de los Estados Miembros, así como el intercambio de la misma debería realizarse en el marco de unos estándares mínimos que garantizaran la protección de los datos personales de los ciudadanos. Es partiendo de esta premisa con la que se debe lograr un equilibrio entre la utilización de la información como medio valioso de las autoridades policiales y judiciales y la protección de los derechos fundamentales, y entre ellos a la protección de sus datos personales, de los ciudadanos de la Unión Europea.

En otoño se celebró en Londres la Conferencia Internacional de Protección de Datos y su organización corrió a cargo de la Comisión de Protección de Datos de Reino Unido (Information Commission Office). La Conferencia, cuyo tema central giró en torno al tema "Una sociedad bajo vigilancia", contó con la participación en torno a diferentes paneles, de representantes de las autoridades de protección de datos del ámbito internacional, parlamentarios, y representantes de medios de comunicación, universidad y de ONGs.

Resultado de esta reunión nace la "London Initiative", una iniciativa de la CNIL, la Autoridad de Protección de Datos francesa, que a través de su documento "Claves para la comunicación de la protección de datos y como incrementar su eficacia" enfatiza la importancia de la privacidad y la protección de los datos personales en los rápidos desarrollos, y la necesidad de una acción urgente para afrontar los nuevos desafíos. Mediante la adhesión a esta iniciativa, en la que la AEPD forma parte, las autoridades de protección de datos se comprometen a:

- Desarrollar actividades de comunicación.
- Adaptar sus prácticas y métodos mediante la evaluación minuciosa de su eficacia y efectividad.
- Contribuir al reconocimiento institucional de las Autoridades de Protección de Datos a nivel internacional y fomentar la participación de otras partes interesadas apropiadas, nacional e internacionalmente.

Además, los Comisarios de Privacidad y Protección de Datos presentes, aprobaron la Acreditación de 8 nuevos miembros para la Conferencia y se aprobaron dos resoluciones sobre cuestiones organizativas y sobre la protección de la privacidad y los buscadores de Internet.

Previamente, con motivo de esta reunión internacional, se celebraron dos reuniones sobre "Security breaches" y "Cooperación Internacional en materia de Enforcement" respectivamente, organizadas por sectores privados, la Cámara de Comercio Internacional y la Organización para la Cooperación y el Desarrollo Económico (OCDE).

Toda la información sobre esta Conferencia puede encontrarse en el siguiente hipervínculo:

<http://www.privacyconference2006.co.uk/>

En marzo del año 2006 tuvo lugar el I Congreso Europeo de Protección de Datos, organizado por la Agencia Española de Protección de Datos, en colaboración con la Fundación BBVA y el Consejo Superior de Cámaras de Comercio, Industria y Navegación.

El Congreso consiguió reunir por primera vez en un mismo foro a los máximos representantes de las Autoridades Europeas de Protección de Datos, expertos en la materia y cualificados representantes del ámbito político y empresarial no sólo de Europa, sino también de EE.UU. e Iberoamérica, y surgió con el objetivo de crear un foro abierto para permitir la puesta en común del conocimiento y el esfuerzo de todos los agentes implicados en la salvaguardia del derecho fundamental a la protección de datos, tanto del sector público como del sector privado.

En el Congreso, que se dividió en torno a 6 paneles, se tuvo la oportunidad de tratar temas como el desarrollo reglamentario de la Ley Orgánica de Protección de Datos debatiéndose las principales novedades del texto que entonces ya estaba siendo elaborado.

Se analizó igualmente la Directiva europea sobre protección de datos exponiéndose el trabajo desarrollado por el Grupo de Trabajo del Artículo 29 y analizando el marco jurídico de la protección de datos más allá de nuestras fronteras.

También fueron objeto de análisis las transferencias internacionales de datos basadas en las llamadas Binding Corporate Rules o Reglas Vinculantes de las Corporaciones y su aplicación en la actividad económica en el sector privado.

Asimismo, se trató la relación entre la lucha contra el fraude y la protección de datos, destacando las propuestas europeas de la lucha contra el fraude en el sector financiero y su incidencia en la privacidad y por tanto en la protección de datos personales.

Del mismo modo, se analizó la lucha contra el terrorismo y la delincuencia organizada y su conexión con la protección de datos, examinando los instrumentos jurídicos para la lucha contra el terrorismo y la delincuencia y las novedades introducidas por la normativa de retención de datos de tráfico.

Por último, se debatió sobre la tensión entre la transparencia en las actividades públicas, la protección de datos y el rápido desarrollo de las nuevas tecnologías de la información.

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

El "London Action Plan" es un foro de debate que reúne a organizaciones tanto públicas como privadas de 27 países, responsables del cumplimiento de las leyes que luchan contra el Spam. Entre ellas se encuentra una amplia representación de agencias de protección de datos, agencias de telecomunicaciones y de protección de los derechos de los consumidores. Su objetivo es una cooperación para luchar contra el spam a nivel internacional, para tratar problemas tales como el fraude on-line, los engaños, el "Phising" y la difusión de virus.

Asimismo, se colabora también con otras organizaciones internacionales, tales como la Organización para la Cooperación Económica y el Desarrollo (OECD), la Unión Internacional de Telecomunicaciones (ITU), la Unión Europea (UE), la Red Internacional para el cumplimiento de las leyes de Protección al Consumidor (ICPEN), y la Cooperación Económica Asia-Pacífico (APEC).

La AEPD firmó el acuerdo del London Action Plan en octubre de 2004 y es miembro de este grupo de trabajo a nivel mundial con vistas a la colaboración en la lucha contra el Spam. Durante el año 2006 se realizaron trabajos de estudio en temas concretos, como la pornografía infantil en Internet y el futuro de la base de datos de WHOIS, que identifica la gestión de las páginas de Internet y ayuda a la persecución del fraude, a nivel mundial.

CASE HANDLING WORKSHOP

Este Grupo de Trabajo -denominado de tratamiento de quejas- se creó en el año 1999 en Helsinki en el seno de la Conferencia de Primavera de Autoridades Europeas de Protección de Datos, con el fin de dar cumplimiento a lo establecido en el Artículo 28(2) de la Directiva 95/46/CE. Su finalidad principal es comparar los procedimientos en el tratamiento de reclamaciones en las distintas autoridades de protección de datos y prestarse ayuda en procedimientos que revisten una especial sensibilidad o dificultad.

El Grupo de Trabajo de Tratamiento de Quejas se reúne semestralmente, celebrándose la decimotercera reunión en el mes de marzo en Madrid.

Los temas sobre los que giró el encuentro, entre otros, estuvieron relacionados la Administración electrónica, y la vigilancia de los trabajadores. La AEPD participó en dos sesiones con la presentación de las garantías que en materia de protección de datos supone el nuevo Documento Nacional de Identidad electrónico y con la presentación de algunos de los casos más relevantes que en materia de videovigilancia en el entorno laboral se han llevado.

La decimocuarta reunión, se celebró en Atenas, centrándose el intercambio de ideas sobre la videovigilancia, así como en sesiones paralelas en las que se compartieron experiencias respecto a los datos bancarios y financieros en las transferencia de los datos personales de los clientes de los bancos a otras instituciones financieras en caso de transacciones o contratos incompletos o la recogida y almacenamiento de este tipo de datos. Por otro lado, también se tuvo la oportunidad de compartir opiniones y prácticas en las competencias para aplicar las leyes de protección de datos y en las relaciones de las autoridades de protección de datos con los medios de comunicación.

GRUPO DE TRABAJO INTERNACIONAL DE PROTECCIÓN DE DATOS EN TELECOMUNICACIONES (IWGPDPT)

El Grupo de Trabajo Internacional de Protección de Datos en Telecomunicaciones, creado por la Autoridad de Protección de Datos y de Acceso a la Información Pública de Berlín, celebró durante el año 2006 sus reuniones número 39 y 40, en Washington y Berlín respectivamente. La AEPD participa en este grupo desde sus inicios.

En su primera reunión del año 2006 este Grupo de trabajo se centró en contenidos como la informática de confianza, los problemas relativos al fenómeno del marketing transfronterizo, con las cada vez más débiles fronteras de los países frente a la invasión de publicidad no deseada, así como la gestión segura de la información que se aloja en servidores.

Finalmente se presentaron aplicaciones prácticas de tecnologías de RFID, y las nanotecnologías.

Se adoptó un documento de trabajo sobre la disponibilidad de las historias clínicas electrónicas (Working Paper on Online Availability of Electronic Health Records cuyo texto puede ser consultado en:

(http://www.datenschutz-berlin.de/doc/int/iwgdpt/WP_HealthRecords_en.pdf)

En su segunda reunión se trataron temas relativos a los problemas derivados del uso de servicios web, identificadores por radiofrecuencia (RFID) y las tecnologías de análisis de voz. Se procedió a la aprobación de los siguientes documentos:

- Working Paper on Trusted Computing, Associated Digital Rights Management Technologies, and Privacy - Some issues for governments and software developers
- Working Paper on Privacy and Security in Internet Telephony (VoIP)

