AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

MEMORIA 2010

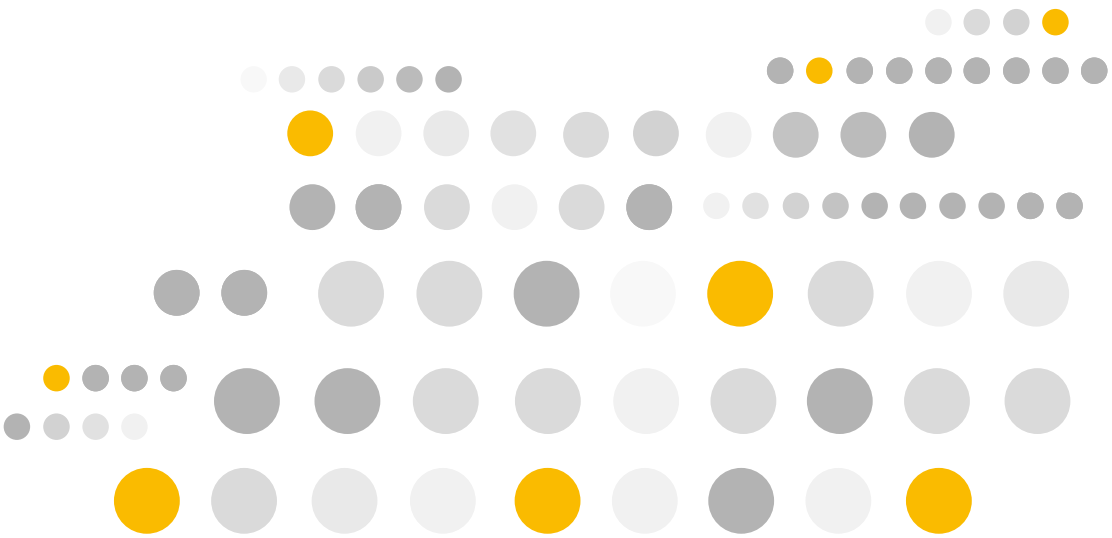
Un año más constituye una gran satisfacción la presentación de la memoria anual de la Agencia Española de Protección de Datos y, mediante ella, trasladar a la sociedad la forma en la que se va conformando la tutela del derecho fundamental a la protección de datos personales.

Cómo los lectores podrán apreciar la Memoria 2010, al igual que en los años precedentes, incluye la información más destacada del ejercicio buscando otorgar una visión global de la situación del derecho fundamental a la protección de datos en España, las tensiones a que hoy está sometido, así como informar del trabajo de esta institución en el desarrollo de las funciones que tiene encomendadas.

La principal prioridad de la Agencia son los derechos de los ciudadanos y, por ello, en 2010 la Agencia Española de Protección de Datos ha continuado trabajando intensamente en el desarrollo de distintas iniciativas para impulsar su conocimiento y garantizar su ejercicio efectivo; así como en lograr la efectiva implantación de esta normativa, mediante la difusión y simplificación del cumplimiento de la Ley. Como se desprende de la información recogida a lo largo de las próximas páginas, se vuelven a constatar los avances obtenidos de dichas iniciativas. Así, lo ponen de relieve la consolidación de los incrementos de las funciones que tiene encomendadas la AEPD, tal como se pone de manifiesto en los indicadores de actividad en las áreas de Atención al Ciudadano ó Inspección y, también, indicadores como el incremento de ficheros inscritos en el RGPD y la disminución de la cuantía de las sanciones económicas -lo que refleja un grado cada vez mayor de adecuación por parte de estas empresas e instituciones-.

Pero, sin duda, nuestra misión presenta hoy una mayor complejidad ante la emergencia de nuevos desafíos. En esta edición se puede apreciar el peso específico y la relevancia adquirida por el reto que para la privacidad supone el desarrollo tecnológico y, en particular, de Internet. En concreto, se pone de relieve como cuestiones que se vislumbraban en años anteriores como el denominado "derecho al olvido" en Internet, adquieren en la actualidad importantes cotas de preocupación social. Esta cuestión se ha configurado como un derecho emergente cada vez mas reclamado por los ciudadanos, y uno de los principales desafíos a los que nos enfrentamos en la actualidad al objeto de conciliar los derechos y libertades esenciales en cualquier sociedad democrática.

La necesidad de dar respuesta a los retos que plantean las nuevas tecnologías y el mundo globalizado también ha sido uno de los ejes y constantes en la agenda internacional. Bajo el epígrafe *"actualizar el marco normativo de protección de datos: una necesidad compartida"* se destacan algunas referencias a las distintas iniciativas internacionales relativas a procesos de actualización y adaptación de los instrumentos normativos del mundo interconectado y globalizado. Mención especial merece, en este sentido, la Comunicación de la Comisión



«En esta edición se puede apreciar el peso específico y la relevancia adquirida por el reto que para la privacidad supone el desarrollo tecnológico y, en particular, de Internet»

Europea, de 4 de noviembre, en la que se pone de manifiesto la necesidad de actualizar las normas actuales a la realidad cambiante, y se fijan las prioridades y líneas maestras del futuro marco legal europeo.

El apartado la *"Agencia en cifras"* proporciona el resumen de datos estadísticos correspondiente al año 2010 mediante información gráfica y estadística de gran utilidad para valorar el alcance cuantitativo de las actividades desarrollada por la Agencia. Nuevamente, en 2010, la AEPD vuelve dirigir *"Recomendaciones"* con el fin de se promuevan y pongan en marcha iniciativas en ámbitos específicos, para promover la efectiva garantía del derecho fundamental a la protección de datos.

Esta memoria quiere constituir un documento de fácil consulta y utilización intentando evitar referencias demasiado extensas. No obstante puede encontrase una información más exhaustiva en la página Web de la AEPD (www.agpd.es), donde se encuentran recopiladas normativa aplicable, resoluciones dictadas por la Agencia, informes jurídicos, consultas, sentencias y diverso material complementario.

Espero sinceramente que esta nueva edición de la Memoria contribuya una vez más a poner de manifiesto el valor del intenso trabajo desarrollado por los profesionales que prestan servicio en esta institución, que día a día dedican sus mejores esfuerzos en favor de la labor de la Agencia, y permita apreciar como se consolida la efectiva salvaguarda del derecho fundamental a la protección de datos de carácter personal.

Artemi Rallo Lombarte
Director de la Agencia Española de Protección de Datos

«La principal prioridad de la Agencia son los derechos de los ciudadanos y, por ello, en 2010 la Agencia Española de Protección de Datos ha continuado trabajando intensamente en el desarrollo de distintas iniciativas para impulsar su conocimiento y garantizar su ejercicio efectivo»

EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL: SITUACIÓN ACTUAL Y PERSPECTIVAS DE FUTURO 7

1. CIUDADANOS MÁS INFORMADOS Y CONCIENCIADOS SOBRE SUS DERECHOS 8

A. EL "DERECHO AL OLVIDO" EN INTERNET: UNA DEMANDA EMERGENTE 8
B. INFORMAR A LOS CIUDADANOS: PROMOVER SUS DERECHOS 8

2. VELAR POR EL CUMPLIMIENTO DE LA LEY 11

A. UNA APUESTA POR FACILITAR EL CUMPLIMIENTO DE LA LOPD 11
B. LA SEGURIDAD JURÍDICA COMO OBJETIVO PRIMORDIAL 15
C. UNA DEMANDA CRECIENTE DE GARANTÍAS: UNA RESPUESTA ACTIVA DE LA AGENCIA 22

3. RETOS PARA LA PRIVACIDAD. LAS GRANDES CUESTIONES 26

A. INTERNET. UN PASO ADELANTE EN LA PROTECCIÓN DE LOS USUARIOS 26
B. ¿ESTÁ SEGURA TU HISTORIA CLÍNICA? 28
C. EL INTERNET DE LAS COSAS: SEGURIDAD Y PRIVACIDAD EN LA TECNOLOGÍA RFID 29
D. LOS FLUJOS INTERNACIONALES DE DATOS. FLEXIBILIDAD Y GLOBALIZACIÓN 31

4. ACTUALIZAR EL MARCO NORMATIVO DE PROTECCIÓN DE DATOS: UNA NECESIDAD COMPARTIDA 33

A. ESTÁNDARES INTERNACIONALES PARA LA PROTECCIÓN DE LA PRIVACIDAD EN RELACIÓN CON EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL 33
B. DIRECTRICES DE PRIVACIDAD Y FLUJOS TRANSFRONTERIZOS DE DATOS DE LA ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICO (OECD) 33
C. RESOLUCIÓN SOBRE LA PROTECCIÓN DE DATOS Y LA PRIVACIDAD EN EL TERCER MILENIO 34
D. NUEVOS HORIZONTES PARA LA PROTECCIÓN DE DATOS EN ESTADOS UNIDOS 34
E. LA DIRECTIVA EUROPEA DE PROTECCIÓN DE DATOS 35

5. LAS AUTORIDADES EUROPEAS DE PROTECCION DE DATOS ANTE LOS NUEVOS RETOS 36

A. DICTAMEN 8/2010 SOBRE LEY APLICABLE (WP 179) 36
B. DICTAMEN 3/2010 SOBRE EL PRINCIPIO DE RESPONSABILIDAD ("ACCOUNTABILITY") (WP 173) 36
C. DICTAMEN 1/2010 SOBRE LOS CONCEPTOS DE "RESPONSABLE DEL TRATAMIENTO" Y "ENCARGADO DEL TRATAMIENTO" (WP 169) 36
D. INFORME 1/2010 SOBRE LA SEGUNDA INVESTIGACIÓN CONJUNTA: CUMPLIMIENTO A NIVEL NACIONAL DE LOS PROVEEDORES DE TELECOMUNICACIONES Y PROVEEDORES DE SERVICIOS DE INTERNET EN RELACIÓN CON LAS OBLIGACIONES REQUERIDAS POR LA LEGISLACIÓN DE CONSERVACIÓN DE DATOS (WP 172) 37
E. ACTUACIONES EN EL ÁREA DE COOPERACIÓN POLICIAL Y JUDICIAL 37
F. AVANCES EN OTROS FOROS INTERNACIONALES 39
G. LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS: LA CONSOLIDACIÓN DE UN PROYECTO 39

6. COOPERACIÓN CON LAS AGENCIAS AUTONÓMICAS DE PROTECCIÓN DE DATOS 41

RECOMENDACIONES 43

RECOMENDACIONES 45

RECOMENDACIONES NORMATIVAS 45
RECOMENDACIONES EJECUTIVAS 45

LA AGENCIA EN CIFRAS 47

1. INSPECCIÓN 48

2. GABINETE JURÍDICO 60

3. ATENCIÓN AL CIUDADANO 69

4. REGISTRO GENERAL DE PROTECCIÓN DE DATOS 71

5. PRESENCIA INTERNACIONAL DE LA AEPD 88

6. SECRETARÍA GENERAL 94

ANNUAL REPORT 97

EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL: SITUACIÓN ACTUAL Y PERSPECTIVAS DE FUTURO

< ÍNDICE >

1. CIUDADANOS MÁS INFORMADOS Y CONCIENCIADOS SOBRE SUS DERECHOS

A. EL "DERECHO AL OLVIDO" EN INTERNET: UNA DEMANDA EMERGENTE

El "derecho al olvido" en Internet se ha erigido en uno de los más intensos temas de debate en el entorno de los nuevos servicios de Internet.

Frente a quienes niegan la posibilidad de excluir el acceso a la información personal en la Red, los ciudadanos reclaman cada vez con mayor intensidad la posibilidad de ejercer un control sobre sus datos personales incluido el derecho a no figurar en ella.

El incremento de las consultas sobre cómo desaparecer de Internet y sobre el ejercicio de los derechos de cancelación y oposición acreditan la intensidad de esta demanda.

El volumen más importante de consultas al Servicio de Atención al Ciudadano se centra en cómo ejercer los derechos de acceso, rectificación, cancelación y oposición (28,81%).

Dentro de ellas las relativas a los derechos de cancelación y oposición -que constituyen las dos modalidades de ejercer el derecho al olvido- ascienden al 66,15% del total. En particular, las consultas sobre el derecho de oposición se han multiplicado pasando de suponer sólo el 8, 66% del total en 2009 al 25,51% en 2010.

Las mismas conclusiones se constatan en el ejercicio de derechos ante los responsables de motores de búsqueda en Internet ascendiendo a casi un centenar (98) las resoluciones dictadas sobre la tutela de estos derechos. El 87% afectan al motor de búsqueda de Google y el resto a Yahoo!, Lycos, Altavista, Bing y Terra. El 75,5% de las resoluciones han estimado las reclamaciones de los ciudadanos.

El origen de estas reclamaciones se encuentra en la publicación de datos personales en boletines y diarios oficiales, medios de comunicaciones digitales, sentencias y otros sitios web.

De este modo la AEPD ha dado respuesta a las demandas de los ciudadanos en servicios prestados por empresas multinacionales por considerar que para ello utilizan medios en territorio español y se dirigen específicamente a usuarios radicados en España. Parte de las resoluciones han sido recurridas ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional estando pendiente de dictarse las primeras sentencias que, sin duda, constituirán un novedoso precedente sobre la protección de datos en Internet.

El "derecho al olvido" se ha incorporado también a la agenda de la Comisión Europea, que en su Comunicación sobre "un enfoque global de la protección de datos personales en la Unión Europea" incorpora la necesidad de analizar los medios que permitan "clarificar el *derecho a ser olvidado*, es decir, el derecho de las personas a que sus datos no se traten y se supriman cuando dejen de ser necesarios con fines legítimos" (por ejemplo, en el caso en que la persona retire su consentimiento al tratamiento de datos o en el que haya expirado el plazo de conservación de los datos).

B. INFORMAR A LOS CIUDADANOS: PROMOVER SUS DERECHOS

Los medios de comunicación se han consolidado como el instrumento más eficaz para facilitar el conocimiento de los ciudadanos sobre la protección de sus datos personales. Lo que impone a la AEPD un papel activo en orden a atender las demandas de información y la presencia directa en los medios.

Estas nuevas exigencias se han traducido en la elaboración de 67 notas de prensa y convocatorias enviadas a medios de comunicación, 65 notas de la agenda informativa de la web de la Agencia y en torno a 700 entrevistas y solicitudes de información de medios de comunicación.

Los principales temas que han suscitado la atención de los medios de comunicación están vinculados a los riesgos en Internet, destacando los siguientes:

- El "derecho al olvido" en Internet.
- La privacidad en las redes sociales con una especial incidencia sobre los riesgos que afectan a los menores.
- La utilización de "cookies" y dispositivos similares que permiten rastrear a los usuarios cuando navegan en Internet.
- El almacenamiento de información personal por los prestadores de servicios de Internet.
- La captación de datos de redes inalámbricas (WI-FI) abiertas con ocasión de la captación de imágenes para el servicio Street View de Google.

Otros temas destacados por los medios de comunicación han sido:

- La videovigilancia.
- Las comunicaciones comerciales por el canal telefónico.
- El informe sobre el cumplimiento de la LOPD en hospitales.
- El tratamiento de datos en ficheros de morosos.

La Agencia ha reconocido el esfuerzo de los medios mediante la concesión de los Premios de Comunicación y Difusión de Protección de Datos al área de sociedad de los servicios informativos de Radio Televisión Española, los reportajes del programa REC de Cuatro y a periodistas de la Agencia EFE y el diario El País.

El aumento de informaciones sobre protección de datos en los medios de comunicación se ha traducido en un incremento de las consultas al Servicio de Atención al Ciudadano que han superado la cifra de 100.000, (104.826) con un crecimiento del 8,2%.

El canal telefónico se consolida como el principal instrumento para contactar con la Agencia siendo utilizado en el 81,3% de los casos, mientras que la atención presencial y por escrito se mantienen estables. En la atención por escrito casi el 90% (87,9%) de las consultas se canalizaron a través del buzón electrónico **ciudadano@agpd.es**, lo que indica la eficacia de los medios electrónicos para la comunicación con los ciudadanos. El mayor crecimiento se ha producido en las consultas sobre la posibilidad de hacer desaparecer información personal de Internet, especialmente en relación con los resultados de las búsquedas a través de Google.

La videovigilancia se consolida como una inquietud habitual de los ciudadanos centrada fundamentalmente en la instalación de cámaras en comunidades de propietarios, portales o garajes.

En el entorno de crisis económica se han multiplicado las consultas sobre ficheros de morosos, destacando el aumento de preguntas relativas al cobro de deudas por terceros distintos del acreedor, tales como despachos de abogados o empresas especializadas en recobro.

Las encuestas sobre el nivel de satisfacción del Servicio de Atención al Ciudadano arrojan como principales conclusiones las siguientes:

- Más de la mitad de los encuestados manifiesta tener conocimiento de la información que suministra la Agencia antes de realizar la consulta.
- En el canal telefónico, que constituye el principal medio de comunicación con los ciudadanos, el 98,42% de los encuestados se mostraron satisfechos con la información recibida llegando casi al 100% (99,61%) la valoración de los conocimientos de quieres les atendieron.
- El nivel de satisfacción sobre el trato y la atención recibida es elevada (89,60% en la atención presencial y 99,87% en el canal telefónico).

Los menores constituyen uno de los colectivos más sensibles respecto del tratamiento de sus datos personales tanto por los riesgos a que están expuestos como por el déficit de información sobre cómo abordarlos. La protección de los menores implica a un amplio abanico de agentes tales como los prestadores de servicios en Internet, los padres o tutores, los poderes públicos, los educadores y los propios menores.

La deficiente formación en materia de privacidad y protección de datos en los programas de estudio y en los currículos académicos de los formadores, unida al limitado control parental del uso que los menores hacen de Internet, acentúa las situaciones de riesgo.

Con motivo del "Día Internacional de la Internet Segura" la AEPD ha reiterado públicamente a los agentes implicados la necesidad de redoblar esfuerzos para hacer frente a los riesgos de los menores en Internet.

Asimismo la AEPD ha intensificado la oferta de información dirigida a la protección de los menores creando una sección específica en la web institucional con contenidos divulgativos actualizados que incluye guías prácticas, recomendaciones, videos, estudios y conexiones a otras páginas de interés.

2. VELAR POR EL CUMPLIMIENTO DE LA LEY

A. UNA APUESTA POR FACILITAR EL CUMPLIMIENTO DE LA LOPD

En 2010, y con el objeto de facilitar a los responsables de ficheros y a los encargados de tratamiento el cumplimiento de la LOPD y de su Reglamento de desarrollo, se implantó en la página web de la Agencia Española de Protección de Datos (www.agpd.es) la herramienta de autoevaluación EVALUA. Esta utilidad permite comprobar tanto el cumplimiento de la Ley Orgánica 15/1999 como evaluar específicamente las medidas de seguridad establecidas en su Reglamento de desarrollo, permitiendo obtener un informe con las deficiencias detectadas para, en su caso, adoptar las medidas correctoras correspondientes. Al finalizar 2010, el número de accesos a esta herramienta ha ascendido a 20.294.

La Agencia ha continuado su política informativa a expertos y sujetos obligados por la LOPD con la celebración de la III Sesión Anual Abierta de la AEPD.

La Sesión Anual, con asistencia de unos 800 participantes, abordó la incidencia de la administración electrónica en la protección de datos personales, la repercusión de las sentencias dictadas por el Tribunal Supremo en relación con el Reglamento de desarrollo de la LOPD, así como la información sobre las principales novedades del último año en el ámbito nacional e internacional. El desarrollo de la III Sesión Anual se encuentra disponible en el enlace:

www.agpd.es/portalwebAGPD/jornadas/3_sesion_abierta_2010

Asimismo, se ha ampliado el catalogo de guías prácticas para la difusión de la LOPD con la publicación de la "Guía sobre seguridad y privacidad de la tecnología RFID", en colaboración con el Instituto Nacional de Tecnologías de la Comunicación (INTECO), y la reedición de la "Guía de Seguridad".

En ella se recopila un cuadro resumen de las medidas de seguridad recogidas en el RLOPD, y se incluye un modelo de "Documento de Seguridad", que sirve de guía y facilita el desarrollo y cumplimiento de la normativa sobre protección de datos. Asimismo, se incluye una relación de comprobaciones con el objeto de facilitar la realización de la auditoría de seguridad. Aprovechando la publicación de esta nueva edición, la AEPD ha puesto a disposición de los responsables en formato Word el documento modelo del Documento de Seguridad incluido en la Guía. Este documento puede ser descargado desde la página web de la AEPD, y editado y personalizado por los responsables de ficheros de datos personales de acuerdo con sus circunstancias particulares.

El tratamiento de datos personales en la Administración de Justicia ofrece una especial sensibilidad tanto por la naturaleza de las informaciones a que afecta como por la propia función Constitucional de los juzgados y tribunales. Conscientes de esta sensibilidad el Consejo General del Poder Judicial y la AEPD suscribieron un Convenio de colaboración.

El Convenio contempla un protocolo para el desarrollo de actuaciones inspectoras sobre protección de datos en órganos judiciales, así como el desarrollo de iniciativas que impulsen la aplicación efectiva de la normativa de protección de datos en el conjunto de la Administración de Justicia. El Convenio contempla la posibilidad de promover la participación en dichas iniciativas del Ministerio de Justicia, las Comunidades Autónomas u otras entidades competentes para la consecución de los objetivos del Convenio.

En cuanto a las consultas de mayor complejidad dirigidas a facilitar la aplicación de la LOPD a los responsables de tratamientos públicos y privados, se atendieron un total de 527, de las cuales 298 (57%) fueron planteadas por las Administraciones Públicas y 229 (43%) por el sector privado.

Se produce así una reducción en el número de consultas planteadas respecto a las formuladas en años anteriores y, en particular, a los años 2008 a 2009. Ello puede ser debido a la mitigación del efecto producido como consecuencia de la entrada en vigor del Reglamento de desarrollo de la LOPD, que hizo incrementarse en gran medida el número de consultas durante el período inmediatamente posterior a su aprobación. Del mismo modo, cabe apreciar que en este año se ha producido una mayor singularidad en el contenido de las consultas planteadas, así como una reducción de las dudas de carácter general que habían podido suscitarse tras la entrada en vigor del Reglamento y que fueron resueltas en los informes emitidos a consultas planteadas en los dos ejercicios anteriores.

Igualmente, se aprecia, en cuanto al reparto de las consultas de los sectores público y privado, un cambio de tendencia ya apuntado en 2009, dado que frente a la modificación producida en 2008, en que aumentaron considerablemente las consultas referidas al sector privado, se ha retomado la pauta habitual de similitud en el número de las mismas, con ligera preponderancia de las procedentes del sector público (en este ejercicio el 57% del total).

En cuanto a las materias objeto de consulta destacan las siguientes conclusiones:

- El notabilísimo incremento (117%, que se une al del 142% producido en 2009) de las consultas relacionadas con la delimitación de los conceptos de ficheros de titularidad pública y privada y los requisitos exigibles a estos últimos.

- El incremento de las cuestiones relacionadas con el ejercicio de los derechos de rectificación y cancelación (que prácticamente se han triplicado en 2010), así como las referidas a datos especialmente protegidos (que se han duplicado, aumentando en un 56% las referidas a datos relacionados con la salud).

- La mayor relevancia en este ejercicio de las consultas relacionadas con el cumplimiento de los principios de calidad de datos, y en particular de los informes que se centran en el análisis del cumplimiento del principio de proporcionalidad, produciéndose un incremento del 90%.

- El mantenimiento de un número relevante, que incluso se incrementa en un 45%, de las cuestiones relacionadas con las medidas de seguridad, incrementándose igualmente, aunque de forma más ligera, las relacionadas con el ámbito de aplicación de la LOPD.

- La disminución cuantitativa de cuestiones que resultaron especialmente reiteradas en el año 2008, pese a mantener un importante volumen en términos comparativos con las restantes. Así sucede en relación con las consultas relativas a las cesiones de datos, transferencias internacionales y régimen del encargado del tratamiento.

- El incremento de las cuestiones relacionadas con la aplicación de la Ley 11/2007, de acceso electrónico por los ciudadanos a las Administraciones Públicas, si bien las cifras totales aún no representan un volumen significativo respecto del total de consultas planteadas.

- Una disminución sensible, de un 25% de las cuestiones relacionadas con el tratamiento de datos con fines de videovigilancia, así como las relacionadas con el sector de las comunicaciones electrónicas, que prácticamente se reducen a la mitad.

Atendiendo a la distribución sectorial de las consultas del sector privado, las principales conclusiones son:

- El descenso en más de un 40% (que se une al del 65% ya producido en 2009) de las consultas procedentes de entidades dedicadas a la asesoría y consultoría, dado que, transcurridos más de dos años desde la entrada en vigor del reglamento, la Agencia ha vuelto a mantener el criterio general de atender únicamente las consultas relacionadas con sus ficheros y tratamientos y no con las de sus clientes, que deberán formularse por éstos últimos.

- La relevancia adquirida en este ejercicio por las consultas procedentes de asociaciones no profesionales y fundaciones, así como de partidos políticos y sindicatos, representando ambos grupos en torno al 10% de las consultas formuladas.

- El mantenimiento de la importancia de las consultas procedentes de asociaciones empresariales y profesionales y de los sectores financiero, farmacéutico y de transporte.

- La disminución del volumen de consultas procedentes de los sectores de las telecomunicaciones y educativo, así como de las formuladas por particulares, que habían sufrido un notable incremento en 2009.

En cuanto a las cuestiones concretas que han sido analizadas y sus conclusiones cabe hacer referencia, por su interés, a las siguientes:

- Los requisitos legalmente exigibles para la difusión pública en Internet de datos personales referidos a las víctimas de la Guerra Civil y represaliados de franquismo.

- Las consecuencias que pueden derivarse como consecuencia de la creación, a través de un acuerdo contractual, del sistema institucional de protección del que forman parte varias cajas de ahorro en relación con todos los tratamientos llevados a cabo por las mismas. En una segunda consulta se plantearon las implicaciones que la constitución del sistema podía tener en cuanto al cumplimiento de las obligaciones en materia de prevención y la gestión del cumplimiento de dichas obligaciones por parte de la entidad bancaria cabecera del sistema.

- Las referidas a la naturaleza de los ficheros de los Consorcios y la aplicación a los mismos de las normas reguladoras de los ficheros de titularidad pública o privada.

- Los requisitos para que resulte conforme a la LOPD la publicación en Internet de las sanciones impuestas en cumplimiento de la Ley Orgánica 7/2006, de 22 de noviembre, de Protección de la salud y lucha contra el dopaje en el deporte.

- La modificación del régimen de legitimación para el tratamiento de datos con fines de videovigilancia que se derivan de la entrada en vigor de la Ley 25/2009, de 27 de diciembre, de modificación de diversas leyes para su adaptación a la Ley sobre el libre acceso a las actividades de servicios, que modifica el criterio hasta entonces mantenido por la Agencia en relación con el tratamiento de las imágenes a través de sistemas de videovigilancia por razones de seguridad, que exigía la instalación de las cámaras por empresas de seguridad privada.

- Las relativas al mantenimiento de cámaras de videovigilancia, incluso cuando se produce la grabación de parte de la vía pública, en el ámbito de actividades o sectores estratégicos.

- Diversas cuestiones relacionadas con la aplicación de la Ley Orgánica 2/2010, de 3 de marzo, de salud sexual y reproductiva y de la interrupción voluntaria del embarazo, en particular, en lo relativo a la creación de registros de objetores de conciencia y al acceso a los datos de las embarazadas por parte de los servicios de inspección sanitaria.

- Las relacionadas con la delimitación del ámbito de aplicación territorial de la Ley Orgánica 15/1999 y, en su caso, con la existencia o inexistencia de transferencias internacionales de datos.

- La resolución de cuestiones relacionadas con los ficheros mantenidos por los sujetos obligados en el marco de las exigencias contenidas en la legislación de blanqueo de capitales y de la financiación del terrorismo.

- Diversas cuestiones relativas a la procedencia o improcedencia de la cesión o comunicación de datos a órganos estatales o autonómicos competentes para el ejercicio de las funciones inherentes a la función estadística pública.

- La improcedencia, de que se comuniquen a las representaciones sindicales los datos referidos a la productividad o gratificaciones extraordinarias del personal funcionario.

- Los requisitos para que pueda entenderse cumplido el deber de información al afectado en los supuestos en que resulta aplicable la excepción a la cesión establecida en el artículo 19 del Reglamento de desarrollo de la LOPD (operaciones de fusión, escisión, transmisión de activos o pasivos u operaciones mercantiles de análoga naturaleza), teniendo en cuenta la doctrina de la Audiencia Nacional según la cual en caso de incumplirse el deber de información sí existirá cesión de datos.

- La conformidad con lo dispuesto en la Ley Orgánica 15/1999 de la publicación en medios de comunicación del contenido íntegro de las Sentencias siempre que se den los requisitos exigidos por el Tribunal Constitucional para que pueda considerarse prevalente el derecho a la información sobre los derechos al honor, a la intimidad y a la propia imagen.

- Las cuestiones relacionadas con la aplicación de las normas reguladoras del nivel de medidas de seguridad exigibles en relación con determinados tratamientos de datos y, en particular, con la aplicabilidad de las excepciones a la exigibilidad del nivel alto de seguridad.

- Diversas cuestiones relacionadas con el tratamiento de datos en historias clínicas, y en particular las relacionadas con el acceso a los datos de menores de edad y los plazos de conservación de la información.

- Las exigencias legales de consulta de los ficheros de exclusión publicitaria o "listas Robinson".

- Las relativas a los tratamientos llevados a cabo por los servicios de prevención en el marco de la Ley de Prevención de riesgos laborales, el acceso a datos de salud por el empresario y el tratamiento y comunicación de datos por las mutuas de accidentes de trabajo.

- Diversas cuestiones relacionadas con el cumplimiento de lo dispuesto en la Ley 11/2007, de 22 de junio, de Acceso electrónico de los ciudadanos a los Servicios Públicos y a la posibilidad de verificación de los datos aportados por los interesados y obrantes en poder de la misma u otra Administración Pública, teniendo en particular en cuenta la anulación por la Sentencia del Tribunal Supremo de 15 de julio de 2010 del artículo11 del Reglamento de desarrollo de la Ley Orgánica 15/1999.

La inscripción de ficheros en el Registro General de Protección de Datos (RGPD) es uno de los indicadores significativos para conocer el nivel de conocimiento y cumplimiento de la LOPD.

En 2010 se inscribieron cerca de medio millón de nuevos ficheros en el RGPD, cifra que representa un incremento de un 31% respecto al volumen de ficheros inscritos el año anterior. Este incremento ha permitido superar la cifra de 2 millones de ficheros inscritos en el RGPD, cerrando el año con 2,1 millones de ficheros activos. El fuerte impulso registrado en esta actividad en los últimos años se refleja en el hecho de que la inscripción del segundo millón de ficheros se ha realizado en tan solo tres años, frente a los 13 que fueron necesarios para alcanzar el primer millón de ficheros. Es de destacar asimismo el incremento en el uso de la firma electrónica en las notificaciones de ficheros, pasando a ser un 26% de las realizadas a través de Internet, frente al 22% del año anterior.

En términos absolutos, los ficheros notificados en 2010 tienen entre sus principales finalidades declaradas las que se refieren a la gestión de clientes, contable, fiscal y administrativa, junto con la gestión de recursos humanos y la gestión de nóminas. También la publicidad y prospección comercial figura como una de las finalidades a las que mayoritariamente se destina el tratamiento de datos personales en el sector privado.

Aunque con menor incidencia en términos absolutos, merecen destacarse las solicitudes que han experimentado un incremento relativo con respecto a años anteriores, tales como los ficheros relacionados con las actividades políticas, sindicales y religiosas (56%) correspondientes a distintas organizaciones sindicales y políticas, obispados y arzobispados, parroquias, así como otras entidades religiosas.

Asimismo destaca el incremento en la notificación de ficheros relacionados con el comercio y servicios electrónicos de diversa índole (63%) entre los que se incluyen los ficheros relacionados con la gestión de los usuarios que participan en las distintas redes sociales que han pasado de 67 ficheros en 2009, a los 174 ficheros inscritos al finalizar 2010. Finalmente las inscripciones en las que se ha señalado la finalidad de prevención de riesgos laborales han tenido un incremento también importante, cerrándose el año con un 48% más de ficheros en los que se ha declarado esta finalidad.

En el ámbito de las Administraciones públicas, durante el año 2010, se ha llegado a la cifra de 108.289 ficheros inscritos en el RGPD; en concreto se han inscrito un total de 14.497 ficheros.

Respecto a los ficheros de las Comunidades Autónomas destacan las de Andalucía, Cataluña, Valencia y La Rioja con unos incrementos del 248%, 464,9%, 225% y 366,6%.

En el ámbito de la Administración Local, en 2010 se ha producido la inscripción de 9.130 nuevos ficheros, con lo que al finalizar 2010 un 57,9% de municipios han inscrito ficheros, cifras que en términos de población corresponden al 96,3% de habitantes.

Por último, otras personas jurídico-públicas, como los Colegios Profesionales o las Universidades siguen completando sus procesos de inscripción, incrementándose el número de inscripciones en ambos colectivos un 113% y un 122% respectivamente.

B. LA SEGURIDAD JURÍDICA COMO OBJETIVO PRIMORDIAL

La AEPD ha continuado trabajando en el objetivo de lograr mayor seguridad jurídica a través de los informes preceptivos sobre disposiciones de carácter general, dirigidos a mejorar la sistemática del ordenamiento jurídico integrando una norma de carácter transversal con las regulaciones sectoriales.

De este modo fueron informadas 97 disposiciones de carácter general, entre las que cabe hacer referencia a las siguientes:

- El Anteproyecto de Ley de Economía Sostenible.
- El Anteproyecto de Ley del Registro Civil.
- El Anteproyecto de Ley de Contratos de Crédito al Consumo.
- El Anteproyecto de regulación del Juego.
- En el ámbito sanitario, los proyectos de Reales Decretos y Orden Ministerial por los que se establecen se establecen los criterios básicos sobre la organización de recursos para desarrollar la actividad sanitaria de los servicios de prevención, los requisitos básicos de autorización y funcionamiento de biobancos con fines de investigación biomédica y del tratamiento de las muestras biológicas de origen humano, y se establece el funcionamiento y organización del registro nacional de biobancos para investigación biomédica y la creación de la Historia clínica electrónica única en el ámbito de MUFACE, a través del informe emitido al Proyecto de Orden de creación del correspondiente fichero.
- En relación con la Administración de Justicia los proyectos de Real Decreto y Orden Ministerial por los que se modifica el Real Decreto 95/2009, de 6 de febrero por el que se regula el Sistema de registros administrativos de apoyo a la Administración de Justicia y se determinan los requisitos y condiciones para tramitar por vía telemática los certificados de antecedentes penales.
- El Proyecto de Real Decreto por el que se modifica el Real Decreto 190/1996, de 9 de febrero, por el que se aprueba el reglamento Penitenciario.
- El Proyecto de Real Decreto sobre expediciones de títulos universitarios oficiales.
- El Proyecto de Orden por la que se regulan la consulta, la solicitud y la expedición de certificados de inscripción en el fichero nacional Padrón de españoles residentes en el extranjero.
- El Proyecto de Orden por la que se regula el procedimiento de reconocimiento, control y seguimiento de las situaciones de incapacidad temporal, riesgo durante el embarazo y riesgo durante la lactancia natural en el Régimen Especial de la Seguridad Social de los Funcionarios Civiles del Estado.
- El Proyecto de Orden de creación del fichero de datos del Sistema de Información e Visados Nacional (VIS-Nacional) y de la Autoridad Nacional del Sistema de Información de Visados (VIS).
- Por último, fueron informadas diversas disposiciones de creación de ficheros de los Ministerios de Defensa, Asuntos Exteriores, Cultura, Fomento, Interior, Medio Ambiente y Medio Rural y Marino, Economía y Hacienda, Sanidad, Política Social e Igualdad, Justicia, Educación Política territorial y Administraciones Públicas y Presidencia así como de los creados por diversas Consejerías de varias Comunidades Autónomas.

Por otra parte, el análisis del grado de seguridad jurídica en la aplicación de la LOPD obliga a contemplar en qué medida las Resoluciones de la AEPD son ratificadas o revocadas por los Tribunales.

Durante el año 2010 se han dictado, respectivamente, por la Sala de lo contencioso-administrativo de la Audiencia Nacional y por la del Tribunal Supremo 230 y 29 Sentencias.

En cuanto a las Sentencias de la Audiencia Nacional:

- 158 fueron desestimatorias de los recursos formulados contra resoluciones de la Agencia (que quedaron plenamente confirmadas) (69%).
- 16 estimaron parcialmente los recursos (7%).
- 49 estimaron íntegramente las pretensiones anulatorias de las resoluciones de la Agencia (21% frente al 25% del año anterior).
- 7 inadmitieron los recursos interpuestos contra resoluciones de la Agencia (3%).

En relación con los sectores de actividad a los que afectan las sentencias dictadas se mantiene en parte la tendencia sostenida en ejercicios anteriores, siendo cada vez más importante el peso de los sectores financiero y de telecomunicaciones, que prácticamente representan la mitad de las sentencias dictadas en el ejercicio. En el primero de los casos se mantiene el número de recursos respecto de 2009; en el segundo, se produce un incremento del 29%.

También se constata un notable incremento del 50% de los recursos interpuestos por particulares contra resoluciones de archivo dictadas por la Agencia, que suponen un 15% de los resueltos en este año.

Al propio tiempo, disminuye la relevancia de sectores como agua y energía, así como los recursos interpuestos por sindicatos o asociaciones empresariales o profesionales. Igualmente es poco relevante el número de recursos interpuestos por entidades gestoras de ficheros de solvencia patrimonial y crédito (que aún habiéndose duplicado respecto del pasado ejercicio únicamente representan el 2,5% del total).

Por último, en 2010 han desaparecido prácticamente los recursos relacionados con las solicitudes de cancelación de los datos en los Libros de Bautismo de la Iglesia Católica, habiéndose dictado en este ejercicio 2 sentencias frente a las 99 dictadas en 2009.

En cuanto a las materias, son significativas las referidas a la inclusión de datos inexactos en ficheros de solvencia patrimonial y crédito o con la contratación de servicios.

También es preciso indicar que en un buen número de sentencias estimatorias, la decisión final del recurso se ha fundado en la ampliación, mediante la prueba practicada en el ámbito del recurso, de la llevada a cabo por la Agencia. En este sentido, conviene precisar que la mayor parte de los criterios estimatorios de la Audiencia Nacional se han fundado en una distinta interpretación de la prueba obrante en autos y no en discrepancias con las resoluciones recurridas en lo que a la aplicación de las normas sustantivas de protección de datos se refiere.

De las sentencias de la Audiencia Nacional cabe desatacar las siguientes:

- La SAN de 11 de enero de 2010, que considera que no existe cesión ilegal de datos como consecuencia de la aportación en juicio por el empresario de los datos resultantes de las pruebas realizadas en acciones de vigilancia de la salud de los trabajadores al prevalecer el derecho a la tutela judicial efectiva.
- La SAN de 22 de enero de 2010, que pone de manifiesto que el mero hecho de que una entidad facilite verbalmente a otras mercantiles informaciones y juicios sobre una persona con la finalidad de que no fuera contratada por las mismas no se encuentra sujeta a la LOPD.
- La SAN de 10 de febrero de 2010, que considera vulnerado el deber de secreto como consecuencia de la publicación en un diario oficial de una resolución dictada en expediente disciplinario contra un funcionario, en que se reproduce íntegramente la propuesta de resolución, haciéndose constar los datos que motivan la sanción impuesta, procedentes de una causa penal dirigida contra ese funcionario, con indicación literal de la sentencia condenatoria penal del denunciante, dando a conocer un delito y la pena impuesta, al entenderse que estos datos resultan excesivos para la finalidad pretendida con la publicación.

- La SAN de 10 de febrero de 2010, que considera que el derecho de acceso únicamente puede ir referido a datos que estén siendo tratados en el momento de ejercerse, pero no abarca datos respecto de los que hubiese cesado el citado tratamiento, en términos que en la actualidad recoge el artículo 27 del RLOPD.

- La SAN de 23 de febrero de 2010, que considera que prevalece el derecho a la libertad de información en los supuestos de publicación en periódicos digitales de datos referidos al gerente de una empresa pública, relacionados con sus retribuciones y contratos celebrados por la empresa a favor de dicho gerente y su cónyuge.

- La SAN de 4 de marzo de 2010, que considera que no prevalece el derecho a la libertad sindical sobre el derecho a la protección de datos en los supuestos de remisión de publicidad electoral por un sindicato a la dirección particular del trabajador.

- La SAN de 18 de marzo de 2010, que considera lícito el acceso a datos contenidos en la historia clínica de un paciente, que a su vez era facultativo, por parte de los órganos de inspección sanitaria, a fin de determinar su habilitación profesional. En relación con la historia clínica puede también consultarse la SAN de 25 de marzo de 2010.

- La SAN de 25 de marzo de 2010, que confirma la sanción impuesta por la Agencia a una entidad que procedió al tratamiento de datos de un menor de 13 de años de edad en el ámbito de una contratación que no podía haberse llevado a cabo, confirmando la Sala el criterio establecido en el artículo 13 del RLOPD (no aplicable al caso dada la fecha en que se produjeron los hechos). Igualmente se imputa a la recurrente no haber comprobado la concurrencia de este requisito. En el mismo sentido, la SAN de 14 de enero de 2010 confirma la sanción impuesta a la Agencia en relación con un contrato en que la fecha de nacimiento del menor aparecía en blanco.

- Las SSAN de 8 de abril y 22 de julio de 2010, que ponen de relieve que aunque de los artículos 122 y siguientes del RLOPD se desprende la posibilidad de llevar a cabo las denominadas actuaciones previas con anterioridad a la iniciación del procedimiento sancionador con el objeto de determinar si concurren circunstancias que justifiquen tal iniciación, puede haber sin embargo determinados supuestos en los que, a tenor de las circunstancias concurrentes, y desprendiéndose del somero análisis del relato de hechos de la denuncia que los mismos en ningún caso son susceptibles de vulnerar la LOPD, que ni siquiera sea necesario, ni haya justificación ninguna, para iniciar dichas actuaciones previas o de inspección. No obstante, la SAN de 26 de noviembre de 2010 considera necesaria la realización de dichas actuaciones cuando de los hechos denunciados pudiera derivarse la existencia de una infracción.

- Las SSAN de 8 de abril y 25 de noviembre de 2010, que confirman la sanción impuesta por la AEPD como consecuencia de una insuficiente implantación de las medidas de seguridad exigibles, a pesar de haberse acreditado la existencia de un supuesto acceso indebido a los sistemas informáticos del responsable, realizado por expertos en la materia que saltando las medidas de seguridad lograron acceder a algunos datos. En relación con una conducta similar, sin embargo, la SAN de 25 de febrero de 2010 considera que no existe vulneración del deber de seguridad, pero sí del deber de secreto, al no adoptarse medidas posteriores al ataque informático para evitar la difusión de los datos.

- La SAN de 15 de abril de 2010, que sanciona a una empresa de telecomunicaciones por el hecho de no haber comunicado a una empresa de recobros por ella contratada el hecho de que la deuda objeto de recobro era inexistente, al haber sido anulada por resolución de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.

- La SAN de 30 de abril de 2010 resulta igualmente interesante, por cuanto analiza los requisitos necesarios para la procedencia de la adopción de la medida de inmovilización del fichero, prevista en el artículo 49 de la LOPD, confirmando en ese caso la resolución adoptada por la Agencia.

- La SAN de 20 de mayo de 2010, que aclara que el hecho de que determinados datos hayan sido obtenidos por una agencia de detectives privados podría amparar el tratamiento de los mismos realizado por aquélla, pero en ningún caso legitima la cesión de dichos datos a una empresa para que la ésta se ponga en contacto con los interesados.

- La SAN de 20 de mayo de 2010, que recuerda que para el ejercicio de los derechos consagrados en la LOPD a través de representante no puede considerarse suficiente la aportación de un poder genérico, sino que será necesario que el representante disponga de un apoderamiento que habrá de ser escrito, individual y otorgado en términos estrictos.

- La SAN de 22 de julio de 2010, que considera que no se ha producido una vulneración del principio de proporcionalidad como consecuencia del hecho de que una entidad facilitase a un órgano jurisdiccional, a su requerimiento, una información que excedía de la que el mismo pretendía solicitar, dados los términos poco claros de la resolución por la que dicha información era solicitada.

- La SAN de 22 de julio de 2010, que considera lícito el tratamiento llevado a cabo por un encargado del tratamiento, en este caso una empresa de recobros, consistente en la actualización del dato del domicilio del denunciante, que este no había actualizado a la entidad acreedora durante la vigencia de su relación contractual con la misma.

- La SAN de 10 de septiembre de 2010, que considera que en los supuestos de cesión de créditos en que el interesado no ha sido informado de la cesión existirá una cesión de datos que será ilícita si no se cuenta con el consentimiento del interesado. Al propio tiempo, la sentencia considera que el plazo máximo de doce meses de duración de las actuaciones inspectoras establecido en el artículo 122.4 del RLOPD no es aplicable a los procedimientos inspectores iniciados con anterioridad a su entrada en vigor. En este mismo sentido, la SAN de 23 de julio de 2010 considera que existe cesión de datos cuando no puede probarse la existencia del crédito cedido.

En relación con las cesiones de crédito son también de interés las SSAN de 17 de diciembre de 2010, y la de 23 de diciembre que considera que la AEPD no es competente para valorar la existencia de la deuda cuando la misma puede derivarse de la interpretación de las cláusulas de un contrato.

- La SAN de 10 de octubre de 2010, que considera que no existiría prejudicialidad penal en los casos en que se haya producido una suplantación de personalidad que no fue debidamente controlada por el responsable, dado que en la vía penal los hechos serían constitutivos de estafa, siendo el bien jurídico protegido distinto al derivado de un tratamiento ilícito de los datos.

- En el ámbito del tratamiento de datos vinculado a la celebración de un contrato, la SAN de 18 de febrero de 2010 confirma la sanción impuesta por la Agencia en un supuesto en que la empresa se amparaba en una supuesta contratación telefónica de un servicio, resultando ser distinta la persona contactada de aquélla a la que se facturaba el servicio y la presentación por ésta de diversas reclamaciones ante la empresa y ante una OMIC. En este mismo ámbito, la SAN de 6 de mayo de 2010 considera inexistente el contrato que supuestamente da cobertura al tratamiento cuando el interesado rechazó el equipo en el momento en que el mismo fue suministrado y formuló una queja ante el organismo regulador (criterio igualmente sostenido por la SAN de 3 de junio de 2010). Por último, la SAN de 10 de junio de 2010 considera inexistente el contrato al no constar firma del interesado y haberse rechazado todos los recibos presentados al pago.

- Por contra, la SAN de 29 de abril de 2010 aprecia indicios de la existencia de un contrato que legitima el tratamiento en el ámbito de la telefonía móvil al haberse producido llamadas entre el titular contratante y sus familiares, siendo el número de referencia facilitado por el contratante en el momento de la contratación aquél respecto del que constan dichas llamadas. Asimismo, la SAN de 24 de junio de 2010 aprecia la existencia de contrato al considerarse indicios suficientes la similitud de firmas entre la plasmada en él y la del DNI del interesado, el hecho de que la recurrente disponga de los datos bancarios de aquélla y que el número de teléfono facilitado pertenece realmente al afectado (en el mismo sentido puede consultarse la SAN de 28 de octubre de 2010). Por último, las SSAN de 15 de julio y 17 de noviembre 2010 valoran el indicio de la realización de determinados pagos correspondientes al servicio.

- En relación con el requerimiento previo de pago para la inclusión de los datos en ficheros de solvencia patrimonial y crédito la SAN de 17 de septiembre de 2010 (referida a hecho anteriores a la entrada en vigor del RLOPD) recuerda que la omisión de este requisito es susceptible de sanción por parte de la Agencia, dado el carácter normativo de la Instrucción 1/1995 reconocido por el Tribunal Supremo. Por su parte, la SAN de 23 de julio de 2010 considera que es posible la existencia de un solo requerimiento en una deuda de pago fraccionado, aun cuando su cuantía se incremente posteriormente en el fichero y la de 23 de febrero de 2010 considera válido el requerimiento efectuado por una empresa de recobro casi un año antes de la inclusión del dato en el fichero de solvencia. A su vez la SAN de 29 de abril de 2010 considera que el requerimiento podría verificarse de forma telefónica siempre que pueda acreditarse su existencia. Finalmente, la SAN de 16 de mayo de 2010 considera obligatorio el cumplimiento de este requisito, no pudiendo aceptarse la renuncia al mismo mediante un consentimiento solicitado del deudor a través del procedimiento establecido en el artículo 14 del RLOPD.

- En cuanto a la necesidad de que la deuda incluida en los ficheros de solvencia sea cierta, vencida, exigible e impagada, la SAN de 23 de septiembre de 2009 no considera que concurren dichos requisitos en el supuesto de la cuantía derivada de la aplicación de una cláusula penal que es objeto de litigio en el momento de la inclusión. Del mismo modo, la SAN considera que no procede el mantenimiento en el fichero de la parte no satisfecha de la deuda cuando fue aceptado el pago con la consiguiente reducción en un convenio de quita. Asimismo, no procede incorporar la deuda correspondiente al abono de un servicio cuya tarifa fue incrementada unilateralmente por el prestador sin conocimiento del interesado, tal y como indica la SAN de 25 de marzo de 2010.

- Por otra parte, son numerosas las sentencias en que, frente a la alegación de la recurrente acerca de la existencia de un uso fraudulento o abusivo por parte de la EPD del trámite de diligencias previas, la Audiencia Nacional ha puesto de manifiesto la improcedencia de dicha alegación atendiendo al incremento de la carga de trabajo producida en la Agencia, siguiendo el criterio ya establecido en la SAN de 19 de noviembre de 2008. Criterio que ha sido ratificado por la STS de 8 de septiembre de 2010.

- En relación con la divulgación de datos mediante la utilización de programas de intercambio de archivos P2P, la SAN de 11 de febrero de 2010, referida a un supuesto en que el fichero compartido contenía datos de salud procedentes de un centro sanitario, recuerda que al responsable del tratamiento de datos de salud debe exigírsele una diligencia específica para asegurar que dicho tratamiento cumple con los principios y garantías exigidos en la LOPD. Además, señala que el hecho de que el intercambio se haya producido desde el ordenador de un trabajador que instaló el programa no exonera al centro sanitario, que debió implantar las medidas de seguridad adecuadas para evitar el hecho. En el mismo sentido se pronuncia la SAN de 15 de julio de 2010, referida a un sindicato.

- En relación con el deber de secreto, la SAN de 8 de abril de 2010 considera que el mismo no aparece vulnerado por el hecho de que un cónyuge haya tenido acceso a los extractos de las cuentas corrientes del otro compartiendo ambos el domicilio. Del mismo modo, no se entiende vulnerado este deber en caso de publicación de tablones de una lista de morosos de una comunidad de propietarios habiéndose intentado antes su comunicación en el domicilio, según la SAN de 3 de junio de 2010 o por la publicación de datos de condenas en boletines oficiales, conforme a la SAN de 10 de febrero de 2010. Asimismo, la SAN de 24 de septiembre de 2010 considera que la revelación efectuada por un concejal no puede implicar una sanción a un Ayuntamiento por vulneración de dicho deber. Por el contrario, sí existe vulneración cuando se remite información a una persona distinta de la interesada, pero con similar nombre (SAN de 4 de marzo de 2010) o cuando se divulga a todo el personal de una entidad una sentencia sin haber anonimizado el dato del trabajador involucrado (SAN de 11 de marzo de 2010).

- En materia de videovigilancia, la SAN de 20 de mayo de 2010 entiende vulnerada la LOPD dado que la cámara instalada grababa zonas comunes de una comunidad de propietarios, por lo que se excedía la excepción doméstica, no contándose con la autorización de la Junta. Del mismo modo, otra sentencia de la misma fecha recuerda que no cabe amparar la inaplicación de la LOPD en una deficiente calidad de las imágenes, añadiendo la SAN de 27 de mayo de 2010 que en caso de difusión de las imágenes a través de Internet será necesaria la existencia de una legitimación específica para tal difusión. Por su parte, la SAN de 17 de junio de 2010 recuerda que en este caso se trataría de una infracción "permanente"; que subsistiría en tanto existiese el tratamiento y que el mismo se encuentra sujeto a la LOPD aun cuando no se proceda a la grabación de las imágenes.

Por su parte, el Tribunal Supremo, dictó un total de 29 sentencias referidas a recursos de casación o de casación para unificación de doctrina interpuestos frente a sentencias dictadas en procesos en los que era parte la Agencia.

Al propio tiempo, y aún no tratándose de recursos relacionados con actos dictados por la AEPD, resultan especialmente relevantes tres sentencias de 15 de julio de 2010 por las que se resolvían los recursos planteados contra el Reglamento de desarrollo de la LOPD, así como dos Autos de planteamiento de cuestión prejudicial, de la misma fecha, relacionados con el artículo 10.2 b) del mencionado Reglamento.

En relación con estos recursos, las sentencias:

- Estimaron el recurso, anulando los artículos 11, 18, parte del 38.1 a), 38.2 y 123 del Reglamento.

- Desestimaron el recurso, confirmando la legalidad de los artículos 5.1 q), 8.5, 12, 13.4, 15, 20.1, 21.2 a), 23.2 a), 24.3, 38.1 b), 38.3, 39, 40, 41, 42.2, 44.3, 45.1 b), 46, 47, 69, 70, 83 y la disposición adicional única del Reglamento.

En ellas el Tribunal Supremo avala ampliamente el Reglamento al anular sólo 5 de los 158 artículos que lo integran, incrementando la seguridad jurídica en el sistema español de protección de datos.

Hecha esta referencia, y centrándonos en las sentencias referidas a procesos en que era parte la AEPD, el Tribunal Supremo:

- Declaró en 13 sentencias no haber lugar a los recursos interpuestos contra sentencias que confirmaban las resoluciones de la Agencia, que quedaron así confirmadas.

- Declaró en 12 sentencias haber lugar a los recursos interpuestos contra sentencias que confirmaban las resoluciones de la Agencia, que quedaron así anuladas. De estas 12 sentencias 6 estiman los recursos de casación interpuestos por los Obispados contra las SSAN por las que se desestimaban los recursos relativos a la cancelación de los datos de los libros de Bautismo de la Iglesia Católica.

- Declaró en dos supuestos no haber lugar al recurso interpuesto por la representación procesal de la Agencia contra sentencias que estimaban los recursos interpuestos contra la resolución de esta Agencia.

- Acordó en dos supuestos la inadmisión del recurso.

En consecuencia, y al margen de las cuestiones relacionadas con la cancelación de los libros de Bautismo, el Alto Tribunal vino a ratificar los criterios de la Agencia en 15 de las 23 ocasiones en que la cuestión fue sometida a su parecer.

Dicho lo anterior, debe hacerse referencia a las siguientes sentencias:

- Las SSTS de 26 de enero, 2 de julio y 22 de octubre de 2010, referidas a supuestos idénticos de tutela del derecho de acceso ejercidos por un mismo interesado ante un mismo responsable, en las que se indica que no es necesaria la atención de plazos y términos formales para atender este derecho en caso de que el responsable del tratamiento haya puesto a disposición del afectado un procedimiento que permite el acceso permanente online a sus datos personales.

- La STS de 16 de marzo de 2010 se refiere a un supuesto de cesión de datos, considerando que la infracción del artículo 11 de la LOPD no puede considerarse como infracción continuada, sino que se produce en el momento de la revelación del dato, momento a partir del cual computan los plazos de prescripción establecidos en la LOPD.

- La STS de 17 de marzo de 2010 menciona un supuesto de recogida por una empresa de datos referidos a subastas judiciales con la finalidad de elaborar un fichero posteriormente comercializado por esta empresa, recordando el Tribunal, frente a la alegación de la recurrente, la doctrina sobre la publicidad de las actuaciones judiciales y la legitimación para el tratamiento de los datos relacionados con esa actuaciones, que queda limitada a quienes fueron parte en el proceso, no siendo esa publicidad absoluta, sino restringida a aquéllas.

- La STS de 19 de mayo de 2010, referida a un supuesto en que, no atendido su derecho de acceso, el interesado instó de la AEPD la apertura de un procedimiento sancionador, sin iniciar el procedimiento de tutela de derechos previsto en el artículo 18 de la LOPD, considerando la Sala que dicha opción es posible y que puede denunciarse la denegación del acceso sin solicitar la tutela previa de la Agencia.

- La STS de 2 de junio de 2010 ratifica la doctrina actualmente existente en relación con la vulneración del deber de secreto en el caso de documentación aparecida en la vía pública, considerando que la infracción es imputable al recurrente con independencia de que la documentación fuera abandonada por un tercero que posteriormente se demostró que trabajaba como administrativo para aquélla.

- Las SSTS de 22 de julio y 5 de octubre de 2010 recalcan la necesidad de que la contratación de servicios de un encargado del tratamiento conste en un contrato que deberá formularse por escrito o por otro medio que pueda acreditar su contenido, al encontrarse el mismo tasado por el artículo 12.2 de la LOPD, lo que no sucedía en el caso analizado.

- La STS de 29 de junio de 2010 considera que no puede encuadrarse en la relación responsable- encargado el supuesto en que una entidad bancaria y una inmobiliaria firmaron un acuerdo en virtud del cual la segunda facilitaba a la primera los datos de los adquirentes de viviendas para que la entidad bancaria pudiera ofrecer a los mismos una oferta de financiación.

- La STS de 17 de septiembre de 2010 analiza un supuesto en que una entidad contrató los servicios de un "listbroker" para la realización de una campaña publicitaria, empleando éste los datos de clientes de otra entidad. La sentencia considera que existe una cesión a la beneficiaria de la publicidad, aun cuando la misma no accedió materialmente a los datos. Del mismo modo, se considera que la cláusula informativa contenida en la revista de la recurrente para la cesión de sus datos adolecía de tal imprecisión que impedía poder considerar prestado el consentimiento por sus clientes.

- La STS de 5 de octubre de 2010 se refiere a un supuesto de sanción como consecuencia de la recogida de datos de forma engañosa o fraudulenta, indicando que para que sea posible la imputación de la infracción del artículo 44.4 a) de la LOPD será necesario motivar y acreditar la efectiva existencia de engaño o fraude en la conducta del infractor.

- La STS de 8 de octubre de 2010 considera que la excepción al consentimiento para la cesión de los datos basada en la existencia de una relación jurídica (artículo 11.2 c) de la LOPD) debe ser objeto de interpretación restrictiva, al emplearse el adverbio "necesariamente", sinónimo de "inevitablemente", "irremediablemente" o "indefectiblemente", lo que exige un carácter forzoso en la cesión.

- La STS de 16 de diciembre de 2010 finalmente confirma el criterio de la Audiencia Nacional por el que se ordenaba a la AEPD la tramitación de actuaciones de investigación en relación con la difusión a través de un medio televisivo de imágenes del recurrente en primera instancia que habían sido modificadas digitalmente.

C. UNA DEMANDA CRECIENTE DE GARANTÍAS: UNA RESPUESTA ACTIVA DE LA AGENCIA

Durante 2010 la actividad desarrollada por la Agencia al objeto de reparar y evitar vulneraciones a la privacidad ha sido constante y ha respondido con prontitud no sólo atendiendo a las reclamaciones presentadas por los afectados sino también actuando de oficio en los ámbitos en los que se consideraba que era necesario evitar cualquier tipo de riesgo o infracción.

En la vertiente reactiva debe subrayarse que no sólo se ha consolidado el incremento del 75% en el número de denuncias que se produjo en 2009 respecto a 2008 sino que se ha producido un crecimiento adicional de un 4% alcanzando la cifra de 4.300.

Por el contrario es de destacar el decremento en casi un 13% en las solicitudes de las tutelas relativas al ejercicio de los Derechos de acceso, rectificación, cancelación y oposición. La razón principal de esta disminución debe encontrarse en la práctica desaparición de solicitudes de tutela frente a la negativa de cancelación de partidas de bautismo por la iglesia católica tras haber recaído en septiembre de 2009 una Sentencia del Tribunal Supremo que no consideraba aplicable la LOPD al no estar organizados los libros de bautismo como un fichero. Como consecuencia, en 2010 únicamente se presentaron 3 reclamaciones frente a las 393 solicitadas en 2009.

Entre las solicitudes de tutelas destacan, junto con las de Internet que se incrementan respecto al año anterior en mas de un 56%, las referidas al derecho de cancelación alegando una indebida inclusión en ficheros de morosos (17% de total).

Telecomunicaciones y videovigilancia son los sectores sobre los que se ha planteado un mayor número de denuncias con un incremento porcentual cercano al 29% y al 14% respectivamente. Otros sectores en los que se han incrementado las denuncias son los servicios de Internet y publicidad y prospección comercial (excepto spam), fuerzas y cuerpos de seguridad y empresas de suministro (gas, electricidad y agua). Debe destacarse que, aunque sigue representando un porcentaje bajo, se ha doblado el número de denuncias referidas a la actuación de los sindicatos en el uso de datos de carácter personal (48). Y junto a ello, el fenómeno de las redes sociales con una tendencia creciente de denuncias y tutelas por presuntas vulneraciones de la privacidad en redes sociales (40 en 2010 frente a 32 en 2009).

Por contra se han producido disminuciones sustanciales en el sector de comunicaciones comerciales por spam o faxes (en dos tercios) y en las denuncias presentadas por el uso de datos en comercios, transporte y hostelería y enseñanza lo que implica una progresiva concienciación de esos sectores en relación a sus obligaciones en el tratamiento de datos de carácter personal.

Sobre las comunicaciones comerciales no solicitadas cabe destacar que, según los datos facilitados por la Asociación Española de la Economía Digital, (adigital), a 31 de diciembre de 2010 los usuarios inscritos en el servicio de Lista Robinson de exclusión publicitaria ascendían a 380.288, siendo el canal con mayor número de usuarios inscritos el telefónico con un 34% del total.

El incremento de las denuncias presentadas en 2010 del 4% debe ser puesto en correlación con un incremento del 8% en el número de procedimientos sancionadores.

Destaca la videovigilancia como sector en el que han recaído mayor número de resoluciones sancionadoras. En el sector de las empresas de telecomunicaciones, aún siendo el sector en el que se han recibido un mayor número de denuncias, se han impuesto un número menor de sanciones situándose en segundo lugar en número de procedimientos sancionadores.

Las razones de esta desproporción se encuentran en el desconocimiento en que con frecuencia incurren los denunciantes sobre las competencias de la AEPD que derivan en que no prosperen las reclamaciones al referirse a cuestiones como facturación o consumo, deficiencias en la prestación del servicio, interpretación sobre cláusulas contractuales o envío de mensajes de tarificación adicional Premium que deberían presentarse a otras instancias.

Junto a ello entre las razones que explican el incremento del 13,16% en las resoluciones de archivo y las denuncias inadmitidas se encuentran las siguientes:

- Inaplicabilidad de la LOPD por estar excluido de su ámbito territorial de aplicación.
- Tratarse de un supuesto de cesión de deuda sobre la que ya ha recaído sanción.
- Inaplicación de la LOPD por ser el denunciante o el afectado una persona jurídica.
- Tratamiento de datos relativos a fallecidos no amparados por la LOPD.
- Falta de indicios mínimos para abrir una investigación que invertiría el principio *in dubio pro reo.*
- Prevalencia del derecho a la libertad de expresión en medios de comunicación.
- Prevalencia del derecho a la tutela judicial efectiva como habilitante para el tratamiento de datos.
- Resultar procedente instar previamente la cancelación o rectificación al tratarse de una opción contemplada en el ordenamiento y no haberse producido daños.

Las resoluciones de declaración de infracción de administraciones Públicas han disminuido un 14% destacando entre ellas las siguientes:

- Comunicación de datos personales del Ayuntamiento a una asociación.
- Exposición al público de listado de propietarios de nichos del cementerio, incluyendo NIF y teléfonos.
- Cámaras en distintas calles del pueblo instaladas por el Ayuntamiento.
- Publicación en prensa de datos de salud.
- Instalación cámaras en los aseos femeninos.
- Publicación en BOE de datos referidos a notificación de sanción pagada meses antes.
- Publicación en el Boletín de un Ayuntamiento de nombre, apellidos, puesto de trabajo y sueldo de los empleados.
- Divulgación de direcciones de correo electrónico de solicitantes de partidas de nacimiento por parte de los Registros Civiles de Barcelona y de Madrid.
- Publicación en un diario de fotografía de ficha policial.
- Envío de documentación clínica perteneciente a otra paciente.

Destaca la ausencia de declaraciones de infracción en 2010 a Administraciones Públicas que fueron infractoras el año anterior como las siguientes: organizaciones colegiales (7 en 2009), órganos judiciales (6 en 2009) Parlamentos regionales (2 en 2009) notarios o entidades como el Banco de España (1 respectivamente a cada una en 2009).

Cuestión relevante es la disminución interanual en el 30% en la cuantía económica de las sanciones impuestas. Más llamativa resulta tal circunstancia puesta en relación con el incremento de un 8% en los procedimientos sancionadores. La razón principal de este desfase se encuentra en la relevancia de videovigilancia como primer sector en número de resoluciones sancionadoras en el que las infracciones se incardinan frecuentemente en las tipificadas como leves (falta de inscripción de ficheros, deficiencias en el cartel informador...) y en el hecho de que habitualmente son sancionadas personas físicas y pequeñas y medianas empresas sobre los que pueden concurrir los criterios de atenuación previstos en la ley. Asimismo ha incidido el hecho de una mayor acumulación de denuncias en un único procedimiento sancionador.

De las resoluciones sancionadoras se sigue imponiendo el porcentaje mayoritario en aplicación de la LOPD (92,5%) pero destaca un importante incremento (27%) en las impuestas en el marco de la LSSI, ley aplicable a las infracciones por comunicaciones comerciales electrónicas (spam) sin consentimiento o sin posibilidad de oposición a las mismas. Llama la atención el hecho de que aunque el número de denuncias ha bajado respecto de 2009, en 2010 se ha logrado acreditar la infracción en más casos. Por el contrario se produce un descenso sustancial (▽ 80%) en las sanciones impuestas en el marco de la Ley General de Telecomunicaciones por el envío de faxes comerciales sin habilitación normativa sobre las también se ha producido un importante descenso en la presentación de denuncias.

Las sanciones que representan un incremento mayor son las calificadas como leves (Δ 62´5%) disminuyendo sustancialmente las calificadas como muy graves (▽ 45,5%) y graves (▽14%).

El número de casos en que se apreció una disminución cualificada de la responsabilidad de los infractores fue del 31,64% del total de las resoluciones sancionadoras. Los criterios aplicados para apreciar esta circunstancia fueron los siguientes:

- Cuando la entidad imputada haya absorbido o se haya fusionado con la entidad responsable que originó la infracción y no haya transcurrido un periodo prolongado.
- Cuando la entidad imputada disponga de un protocolo de actuación adecuado en la recogida de datos y tal protocolo haya, excepcionalmente, fallado.
- Cuando la entidad imputada haya regularizado la situación denunciada de forma diligente en un tiempo prudencial desde el conocimiento de los hechos.
- Cuando los hechos denunciados deriven de un error de difícil detección no producido por una actuación negligente ni la errónea aplicación de una norma.
- Cuando los hechos denunciados deriven de la falta de diligencia en la conducta del afectado o sea corresponsable de la infracción imputada a la entidad.
- Cuando quede acreditada la confianza legítima y no quepa la exoneración al obedecer la infracción a un requerimiento de la Administración.
- Cuando se trata de una persona física o pequeña o mediana empresa y la infracción se deba a cuestiones de cualificación técnica.
- Cuando el denunciado haya reconocido espontáneamente la culpa al principio del procedimiento.

De los datos que se han expuesto cabe concluir la consolidación y crecimiento del incremento del 75 % en el número de denuncias que se produjo en 2009, así como una tendencia también creciente en la presentación de solicitudes de tutelas por derechos ARCO -excluidas las solicitudes de cancelación de partidas de bautismo- y una mejora del cumplimiento de la LOPD al incrementarse los expedientes archivados, reducirse las infracciones muy graves y disminuir la culpabilidad cuando se comete una infracción.

Pero no únicamente han actuado los servicios de inspección de la Agencia ante problemas específicos que afectan a un particular sino que también lo han hecho -bien a instancia de parte o a iniciativa del Director- para investigar problemas generales detectados en diferentes ámbitos:

a) Cesión de datos a empresas

La LOPD contempla supuestos y requisitos para que se produzca la comunicación, cesión o acceso por cuenta de terceros a datos de una empresa. Su concordancia con la ley ha sido analizada en varias inspecciones sectoriales como son:

- Venta de deuda por operadores de telecomunicaciones y entidades financieras cuya licitud está condicionada a que haya facturas pendientes de pago ó deriven de un contrato suscrito por una tercera persona.
- Análisis de cláusulas contractuales del recobro de deudas en operadores de telecomunicaciones. La presentación de servicios de recobro por cuenta de terceros está amparada por la ley si contractualmente se prevé la adopción de garantías suficientes.

b) Inspección al Sistema de información Schengen en España

El sistema permite a los países miembros incluir información y disponer de acceso a las descripciones de personas introducidas por otros países con ocasión de controles de la policía, en las fronteras o aduanas. Se ha analizado la calidad de la información que se incluye en la parte nacional del Sistema, los procedimientos de inclusión de señalamientos y la aplicación de las restricciones temporales y de forma definidas.

c) Análisis de cláusulas contractuales de los operadores de telecomunicaciones

Se ha iniciado un proceso de análisis general de las cláusulas contractuales utilizadas por las empresas de telecomunicaciones no solo para que los clientes se encuentren debidamente informados del destino de los datos aportados sino para que el eventual uso de los mismos con otras finalidades cuente con el debido consentimiento de los ciudadanos previsto en la normativa entre cuyos requisitos se encuentra la posibilidad de manifestar la negativa al uso de los datos para otros fines no relacionados directamente con la relación contractual.

d) Legalidad de grandes bases de datos

Se ha analizado el grado de concordancia con la legalidad de una gran base de datos que contenía el domicilio de 36 millones de españoles sin que aparentemente su origen conforme a la LOPD.

e) Investigación sobre el criterio de acceso en base a "interés legítimo"

El registro de la propiedad, el registro de vehículos y el catastro son tres bases de datos públicas que contienen información sobre millones de ciudadanos.

En los tres casos el acceso por parte de un tercero a la información contenida se somete al interés del consultante.

En 2010 se han presentado reclamaciones referentes al sistema de control o justificación del citado interés legítimo que ha derivado en actuaciones de inspección que eventualmente han culminado en procedimientos de infracción y han requerido un análisis integral sobre los mecanismos de evaluación del citado interés legítimo.

Finalmente debe resaltarse el cumplimiento generalizado de las previsiones temporales del Reglamento aplicable desde abril de 2008 que limitaba el plazo de actuaciones previas a un máximo de doce meses debiendo haberse resuelto y notificado antes de esa fecha el archivo del expediente o el acuerdo de inicio de un procedimiento sancionador, resoluciones que frecuentemente se han adoptado en periodos sustancialmente menores.

3. RETOS PARA LA PRIVACIDAD. LAS GRANDES CUESTIONES

A. INTERNET. UN PASO ADELANTE EN LA PROTECCIÓN DE LOS USUARIOS

Internet ha posibilitado el desarrollo de servicios que son utilizados masivamente por millones de usuarios. Los prestadores de estos servicios inciden en la privacidad de los usuarios a través de dos elementos: La fijación unilateral de las condiciones de uso y privacidad y el propio modelo de negocio que los sustenta.

La fijación unilateral de las condiciones de uso y privacidad afecta a la información que reciben los usuarios -deficiente en cuanto a su claridad y accesibilidad- a las finalidades del tratamiento de los datos y a sus plazos de conservación.

Con la circunstancia adicional de que dichas políticas se modifican periódicamente siendo también esta modificación una decisión unilateral de quienes ofrecen los servicios. A lo que se añade una omisión: la insuficiente aplicación del principio de "privacy by design" en el desarrollo de nuevos servicios.

El modelo de negocio repercute en la privacidad por ser, en términos generales, servicios gratuitos que se financian con ingresos publicitarios.

Lo que ha generado estrategias cada vez más desarrolladas para conocer los hábitos de los usuarios, elaborar perfiles de ellos y personalizar la publicidad que se les ofrece.

En este entorno la AEPD ha venido manteniendo relaciones periódicas con los principales prestadores de servicios en Internet con el fin de intercambiar información y sugerencias que incrementan las garantías de los usuarios.

Pero esta política no puede excluir una reacción adecuada cuando se traspasan las líneas rojas del respeto a la privacidad o los ciudadanos reclaman los derechos y garantías que la ley les reconoce.

En el año 2010 han proliferado ambas situaciones.

En el mes de abril la AEPD junto con nueve Autoridades de diversas áreas geográficas dirigieron una carta conjunta a Google Inc. manifestando su preocupación por el olvido de la protección de datos en el despliegue de nuevas aplicaciones tecnológicas.

En particular, destacaban las amenazas para la privacidad de la red social Google Buzz en la que se asignaron automáticamente y sin información previa a los usuarios una red de "seguidores" entre las personas con las que habitualmente mantenían correspondencia electrónica a través de email.

La reacción de las autoridades recuerda que no se trataba de un caso aislado, instando a incorporar los principios fundamentales de la privacidad en el diseño de sus nuevos servicios en línea. Y representa un precedente sobre la necesidad de adoptar iniciativas coordinadas por las Autoridades de protección de datos y de la privacidad ante servicios globales.

En el mes de mayo las Autoridades europeas de protección de datos comunicaron a los responsables de Facebook su rechazo a la modificación unilateral llevada a cabo en la configuración de la política de privacidad. La modificación ampliaba el acceso a los datos de un usuario por parte de terceros incluso aunque hubieran elegido una política de privacidad más restringida.

Las citadas autoridades se dirigieron, además, a los responsables de otras redes sociales insistiendo en que el acceso a los perfiles informativos y los contactos de cada usuario deben limitarse a los que selecciona y que otros accesos más amplios deben ser una opción explicita del usuario.

En el mismo mes, las Autoridades europeas reiteraron la necesidad de limitar el periodo de conservación de las búsquedas en Internet al plazo de seis meses, comunicándolo a Google, Microsoft y Yahoo!.

De este modo la Agencia, en coordinación con otras Autoridades, ha asumido el compromiso de dar un paso adelante en la protección de los usuarios de Internet.

Un paso adelante que no se ha limitado a advertir con claridad sobre el respeto a las *"líneas rojas"* de privacidad sino que ha llevado a investigar presuntos incumplimientos legales.

En octubre de 2010, tras una exhaustiva investigación previa la AEPD ha iniciado un procedimiento sancionador a Google Inc. y Google Spain por la captación y almacenamiento de datos de localización de redes inalámbricas abiertas (redes Wi-Fi) y de datos de tráfico transferidos a través de ellas por los vehículos utilizados para obtener imágenes para el servicio Street View.

El procedimiento imputa a Google Inc. La presunta comisión de dos infracciones de la LOPD, como responsable del servicio y del diseño del software de recogida de los datos y a Google Spain como responsable de su captación y almacenamiento en España y su transferencia a los Estados Unidos de Norteamérica.

Asimismo, en octubre se iniciaron actuaciones de inspección en la red social Facebook solicitando información sobre si se han visto afectados usuarios en España en la transmisión de datos tales como los nombres de los usuarios y de sus amigos por parte de algunas de las aplicaciones más populares programadas sobre la plataforma de Facebook a anunciantes y otras empresas.

En noviembre se han iniciado actuaciones similares sobre la red social My Space.

Las últimas actuaciones son indicativas de la relevancia que tiene la obtención de datos personales para la realización de publicidad en Internet que, como se ha indicado, constituye un modelo habitual de financiación de servicios gratuitos en la red. Circunstancia que hace necesario actualizar las garantías de los usuarios. La modificación en 2009 de la Directiva 2002/58/CE, sobre privacidad en las comunicaciones electrónicas ha abordado esa tarea, aunque su incorporación al derecho interno puede dilatarse hasta el año 2011.

Y, el Grupo de Trabajo del artículo 29 (GT 29) adoptó en el mes de junio un dictamen sobre publicidad basada en el comportamiento que analiza conjuntamente las garantías de la Directiva citada y de la que regula la protección de datos personales (Directiva 95/46/CE). Dictamen que puede servir de orientación a los legisladores nacionales cuando transpongan la Directiva.

La publicidad basada en el comportamiento trata de obtener un perfil detallado de los hábitos on line de los usuarios con el fin de ofrecerles anuncios personalizados adaptados al perfil. Para ello se utilizan cookies de rastreo que permiten recopilar información sobre el comportamiento de los usuarios cuando navegan en Internet.

El debate planteado sobre el tipo de dispositivos responde a las siguientes preguntas: ¿basta con que los usuarios sepan que se utilizan y puedan desactivarlos? (sistema opt-out) ¿o es necesario que se les informe y presten su consentimiento para que se rastree su navegación? (sistema opt-in).

En opinión de las Autoridades europeas de protección de datos, conforme a la Directiva modificada, el sistema opt-out es insuficiente debiendo exigirse un consentimiento informado de los usuarios antes de instalar dispositivos tales como las cookies. La información sobre la finalidad del seguimiento debe ser clara y comprensible para que el usuario pueda tomar la decisión sobre si quiere o no que su comportamiento de navegación sea monitorizado y su consentimiento debe poder revocarse. Por su mayor vulnerabilidad este tipo de publicidad no debería dirigirse a los menores.

Dada la importancia de la publicidad en Internet y la necesidad de ofrecer garantías a los usuarios, el Dictamen hace un llamamiento a la industria para que creen mecanismos sencillos y eficaces para prestar el consentimiento o revocarlo y ofrece la colaboración de las Autoridades de protección de datos para intercambiar información sobre dichos mecanismos.

La necesidad de dar pasos adelante en la protección de los ciudadanos ante la evolución tecnológica y la globalización ha sido unos de los principales motivos que ha impulsado a la Comisión Europea a adoptar un enfoque global sobre la protección de datos que ha de traducirse en una revisión de la Directiva 95/46/CE.

La fijación unilateral de las condiciones de uso por los prestadores de servicios en Internet hace necesario, junto a las políticas reactivas, primar políticas activas dirigidas a mejorar las garantías para la protección de los datos personales, especialmente en relación con los menores y las redes sociales.

La AEPD ha seguido manteniendo contactos con los principales responsables de redes sociales como Tuenti y Facebook para mejorar sus políticas de privacidad y evitar el acceso de menores de 14 años a dichas redes.

Tuenti ha fijado la edad mínima de acceso en 14 años en línea con lo establecido en la legislación española. Adicionalmente ha mejorado el protocolo de investigación y borrado de usuarios menores de 14 años tratando de alcanzar una revisión en torno a 300.000 perfiles anuales. Cuando los usuarios son dados de baja, si intentan registrarse de nuevo con el mismo correo electrónico el sistema lo impide.

Tuenti mantiene para los menores de 18 años el máximo grado de privacidad por defecto, denominado "solo amigos", siendo cerrado para usuarios desconocidos.

Tanto en la página de Ayuda General como en la específica de privacidad, se insta a los usuarios a navegar de forma segura y dando relevancia a la privacidad, mediante consejos claros para cualquier usuario y específicamente para menores de 14 a 18 años.

Facebook, en contestación al requerimiento de la AEPD anunció que aumentaría a 14 años la edad mínima para poder registrarse desde España en su red social, adecuándose así a la vigente normativa de protección de datos.

Asimismo, Facebook manifestó su compromiso de desarrollar mayores garantías incluyendo el análisis de distintas opciones para implantar un sistema de verificación de la edad de los menores y de comprobación del consentimiento paterno.

El Defensor del Pueblo ha manifestado su interés sobre las medidas tendentes a garantizar la protección de los menores en redes sociales mediante tres requerimientos de informe.

B. ¿ESTÁ SEGURA TU HISTORIA CLÍNICA?

La LOPD califica los datos relativos a la salud como una de las categorías de datos especialmente protegidos, a los que se aplica un régimen reforzado de garantías.

Esta protección reforzada se apoya en los siguientes aspectos:

- La exigencia de un consentimiento expreso para su tratamiento, salvo que existan habilitaciones legales.
- La calificación de las infracciones como muy graves.
- La exigencia de medidas de seguridad de nivel alto para garantizar el máximo nivel de seguridad para los datos de salud evitando su alteración, pérdida, tratamiento o acceso no autorizado.

En atención a la relevancia de los datos de salud la AEPD adoptó la iniciativa para elaborar un "Informe de cumplimiento de la LOPD en los hospitales", por ser estos centros sanitarios los principales responsables en el tratamiento de datos de salud.

Esta iniciativa es consecuencia de la constatación de alarmantes casos de incumplimiento de la LOPD vinculados principalmente a la vulneración de los deberes de seguridad y secreto contemplados en la LOPD. Entre estos incumplimientos pueden citarse la difusión de datos clínicos a través de redes de intercambio de archivos P2P, el abandono de datos de salud en la vía pública, el almacenamiento de información clínica en áreas no restringidas de los centros sanitarios y, por tanto, al alcance de cualquiera, la pérdida de historiales clínicos al proceder a su automatización en formato electrónico o la utilización de datos sanitarios para fines no autorizados o su comunicación indebida a terceros.

Junto a ello se pretendió analizar los sistemas de información a los ciudadanos, los procedimientos para el ejercicio de los derechos ARCO, la inscripción de ficheros y la externalización de servicios.

La evaluación se realizó mediante el envío de un cuestionario a más de 600 centros registrados en el Catálogo Nacional de Hospitales que fue atendido por el 92% de los centros.

La primera conclusión del Informe es que, en términos generales, los índices de cumplimiento de la LOPD en los centros sanitarios privados son elevados, mientras que los centros públicos presentan mayores deficiencias y menores niveles de cumplimiento.

La obligación de inscripción de los ficheros en el Registro General de Protección de Datos ofrece elevados niveles de cumplimiento en ambos tipos de centros (99% en los privados y 89% en los públicos). Si bien estos niveles bajan a la hora de modificar la inscripción para mantenerla actualizada.

Facilitar información a los ciudadanos sobre el tratamiento de sus datos a través de formularios o carteles informativos es una práctica habitual en los centros privados (94,5% y 80% respectivamente) y una deficiencia significativa de los centros públicos (55% y 64%).

En materia de seguridad el Informe pone de manifiesto que existe una importante diferencia entre el cumplimiento formal de las medidas de seguridad y su implantación efectiva. Así, aunque la elaboración de un documento de seguridad alcanza cotas elevadas (98% en centros privados y 83% en públicos) se constatan deficiencias en aplicación, destacando las siguientes:

- Ausencia de mecanismos que obstaculicen la apertura de los dispositivos donde se almacenan las historias clínicas en cerca del 10% de los centros privados y en el 35% de los públicos.

- Deficientes medidas para evitar la sustracción, pérdida o acceso indebido a la documentación clínica durante su transporte en el 15% de los centros privados y en el 30% de los públicos.

- Incumplimiento de la exigencia de disponer de registros de acceso a la información para poder conocer quien accede a la historia clínica y a qué datos en casi un 15% de los centros privados y en un 62,6% de los públicos. A lo que se añade la falta de auditorias para verificar si el personal que accede a los datos los utiliza para la finalidad que justificó el acceso.

- No realizar las auditorias bienales obligatorias sobre las medidas de seguridad que se produce en el 12% de los centros privados y en el 54% de los públicos.

Las dos últimas deficiencias señaladas permiten afirmar que existe una falta de diligencia a la hora de conocer quien accede a las historias clínicas, si quienes lo hacen utilizan no los datos para el fin que justificó su acceso -fundamentalmente la asistencia sanitaria a los pacientes-, así como una ausencia de controles sobre la eficacia de las medidas de seguridad.

La externalización de servicios que implican el tratamiento de datos de los pacientes es un práctica generalizada en los centros sanitarios, habiendo optado un 86% de ellos por este modelo de gestión, si bien la mayor parte de ellos adoptan garantías contractuales para que la prestación de servicios por terceras entidades cumpla las exigencias de la LOPD.

La implantación de procedimientos que permitan el ejercicio de los derechos de acceso, rectificación, cancelación se ha llevado a cabo en el 96% de los centros privados y el 84% de los públicos.

Sin embargo esta circunstancia no ha impedido que las reclamaciones ante la Agencia para la tutela del derecho de acceso a la historia clínica se hayan incrementado significativamente. La Agencia ha dictado 95 resoluciones sobre esta materia que constituyen el 40% del total de revoluciones sobre el derecho de acceso. De ellas casi el 78% son estimatorias de las pretensiones de los ciudadanos.

Los principales motivos de las reclamaciones se centran en haberse facilitado de manera incompleta la información clínica o la denegación del acceso al historial clínico de un familiar fallecido.

C. EL INTERNET DE LAS COSAS: SEGURIDAD Y PRIVACIDAD EN LA TECNOLOGÍA RFID

La identificación por radio frecuencia o RFID (Radio Frequency Identification) es una tecnología que permite identificar automáticamente un objeto gracias a una onda emisora incorporada en el mismo que transmite por radiofrecuencia los datos identificativos del objeto, siendo una identificación normalmente unívoca.

En el estado actual de desarrollo, el abaratamiento de los costes y la reducción en su tamaño permite que estas emisoras sean lo suficientemente pequeñas como para tener la forma de etiquetas adhesivas, pudiéndose incorporar casi a cualquier objeto.

Gracias a estas microemisoras (en adelante etiquetas o tags) el producto puede ser localizado a una distancia variable, desde pocos centímetros, hasta varios kilómetros.

La tecnología RFID plantea nuevos riesgos tanto respecto de la seguridad como de la privacidad.

Así lo reconocieron la Comisión Europea a través de la Recomendación sobre Privacidad en comunicaciones RFID (SEC (2009) 3200 final) y el Parlamento Europeo mediante un llamamiento para garantizar la privacidad y la protección de datos personales en el uso de estas tecnologías.

Con el fin de promover el conocimiento de tales riesgos la AEPD ha elaborado en colaboración con el Instituto Nacional de Tecnologías de la Comunicación (INTECO) una guía sobre seguridad y privacidad de la tecnología RFID.

Entre las empresas españolas el uso de la tecnología RFID es aún incipiente entre microempresas y PYMES, si bien el nivel de adopción de esta tecnología por parte de grandes compañías es del 20% previéndose un crecimiento exponencial en los próximos años.

Por sectores, su uso está más extendido en las actividades de transporte y almacenamiento, seguidas de las financieras, informáticas, telecomunicaciones y audiovisuales y comercio mayorista y minorista.

Las aplicaciones mayoritarias en las PYMES y grandes empresas son el seguimiento y control de la cadena de suministro y de inventarios, la identificación de personas y el control de accesos.

El principal riesgo para la privacidad consiste en el acceso no autorizado a la información personal de los usuarios bien porque está incluida en la etiqueta, bien porque está asociada a la misma y se accede al sistema central para consultarla. Este riesgo se manifiesta en las siguientes amenazas:

- Accesos no permitidos a las etiquetas: Éstas pueden contener datos personales, como nombres, fechas de nacimiento, direcciones, etc. Pueden contener también datos personales de cualquier tipo, dependiendo de la aplicación.

- Rastreo de las personas y/o de sus acciones, gustos, etc.: Una persona, portando una etiqueta RFID con sus datos y usándola para pagar compras, transportes públicos, accesos a recintos, etc., podría ser observada y clasificada.

- Uso de los datos para el análisis de comportamiento individuales: Utilizando técnicas de "minería de datos", este análisis permitiría definir perfiles de consumo basados en las preferencias de los clientes, utilizando esta información para diseñar y orientar la estrategia de marketing y publicidad de las empresas.

La guía indica que, junto a los riesgos para la privacidad, la tecnología RFID presenta también riesgos relacionados con la seguridad derivados de acciones dirigidas a deteriorar, interrumpir o aprovecharse del servicio de forma maliciosa.

Estos ataques pueden realizarse, entre otros ejemplos, para sustituir etiquetas de artículos caros con etiquetas suplantadas de otros más baratos o inutilizarlas con el fin de sustraer mercancías a pequeña o gran escala.

Para los usuarios el principal riesgo para su privacidad se centra en la lectura de la información personal almacenada en el dispositivo RFID o asociada al mismo.

Para evitarlos pueden utilizarse etiquetas (watchdog) que informan de los intentos de lectura, aislar las etiquetas (por ejemplo con una funda de material plástico o metálico) evitando la lectura salvo en los momentos en que se desee, utilizar dispositivos que crean una zona segura en torno al usuario anulando la efectividad de RFID o, más sencillamente, inutilizando las etiquetas una vez que se haya realizado la transacción comercial.

Por su parte, los proveedores deben ser conscientes de los posibles riesgos para la protección de los datos personales y tener en cuenta que están "siguiendo" objetos y no a las personas que los portan.

En consecuencia deben considerar desde el planteamiento inicial del sistema RFID la privacidad y la seguridad teniendo en cuenta como buenas prácticas para garantizar la privacidad las que se mencionan a continuación:

- Notificar el uso de RFID, de forma clara y mediante símbolos expuesto en los productos, en los lectores y en las zonas de alcance de los lectores.
- Dar a conocer en todo momento a los usuarios cuándo, dónde y por qué se va a leer una etiqueta. Incluso indicar la lectura con algún tipo de señal luminosa poco llamativa para evitar molestias, pero indicativa de la actividad.
- Tener una política de privacidad relativa a la obtención, uso y eliminación de la información personal asociada a RFID, que deberá ser pública para los usuarios, ofreciendo a estos la posibilidad de conocer, acceder y modificar la información personal asociada a RFID que se almacene.
- Disponer de personal formado en RFID que conozca las características del sistema instalado y accesible al público, siendo capaz de responder a las cuestiones de seguridad y privacidad correctamente.
- No almacenar en los tags RFID información personal, destruyendo lo antes posible dicha información, reduciendo así el riesgo de intromisión en la privacidad del usuario.
- Retirar, destruir o desactivar los tags cuando hayan cumplido su misión. Si se desea mantener el beneficio del servicio postventa se debe permitir que la devolución de un producto implique la eliminación de la asociación del tag con el usuario.
- Ofrecer al usuario facilidades para la retirada, destrucción o desactivación de los tags asociados a productos cuando va a abandonar las instalaciones.
- No ceder a terceras partes información asociada a RFID que pueda ser usada para crear perfiles o realizar vigilancia de usuarios.
- Realizar auditorías de seguridad de sistemas RFID de forma periódica para garantizar su nivel de seguridad.

D. LOS FLUJOS INTERNACIONALES DE DATOS. FLEXIBILIDAD Y GLOBALIZACIÓN

Las transferencias internacionales de datos personales mantienen su tendencia al crecimiento acorde con las necesidades de una economía globalizada. Del mismo modo el desarrollo de países emergentes está determinando una diversificación geográfica de los destinatarios de transferencias internacionales de datos.

En 2010 las solicitudes de autorización de transferencias se han incrementado cerca del 20% (18,6%). Las principales áreas geográficas de destino para la exportación de datos fueron Latinoamérica que con 88 solicitudes supone un 34,5% del total, Estados Unidos con 25 y Asia con 23.

Los países latinoamericanos se consolidan así como el principal foco de destino de flujos internacionales de datos desde España con un total de 220 autorizaciones que se añaden a las aún mayores (377) realizadas a la República Argentina, país en el que, al estar calificado como de nivel adecuado de protección por la Comisión Europea, no es necesaria la autorización, sino sólo la notificación al RGPD.

Dentro de los países latinoamericanos ocupan un papel destacado Colombia, Chile, Méjico, Perú y Uruguay. Son precisamente estos países los que han aprobado ya o están en proceso de hacerlo leyes específicas sobre protección de datos personales. Y en algún caso como el de Uruguay han iniciado el proceso para obtener una Decisión de Adecuación por la Comisión Europea.

Dada la mayor flexibilidad que supone la declaración de país adecuado es previsible que en un futuro próximo los países citados multipliquen su relevancia como importadores de datos desde España con los consiguientes efectos inducidos por su tejido económico.

Las transferencias internacionales de datos a Estados Unidos se mantienen estables. Y, las destinadas a países de Asia prácticamente se asimilan a ellas destacando las realizadas a la India que son más de la mitad del total de las dirigidas a países de dicha área geográfica.

Se aprecia, también un incremento de los flujos de datos hacia Israel, país que en 2011 ha sido declarado con un nivel adecuado de protección.

La principal característica de todas las transferencias internacionales de datos estriba en que la inmensa mayoría (90%) se refieren a prestaciones de servicios que se externalizan en terceros países al amparo de cláusulas contractuales. Lo que confirma un año más la deslocalización de actividades de tratamiento de datos en terceros países.

En este sentido destaca la Decisión 2010/187/CE de la Comisión Europea que sustituye a la 2002/16/CE incorporando formulas más flexibles para posibilitar la subcontratación de operaciones de tratamiento de datos en terceros países.

La Agencia ha participado en el marco del procedimiento coordinado establecido por el Grupo del artículo 29 en la revisión de dos solicitudes de transferencias de grupos multinacionales autorizadas sobre el modelo de reglas corporativas vinculantes (BCR en sus siglas en inglés). Si bien este no es el único modelo por el que optan las grandes corporaciones multinacionales, como lo acredita el que una de ellas haya obtenido una autorización de transferencia a 104 filiales que actúan como encargadas de tratamiento basada en las cláusulas contractuales tipo de la Decisión 2002/16/CE, antes de su derogación. La finalidad de la transferencia es la prestación de servicios centralizados en apoyo de los procesos de negocio del exportador de datos.

4. ACTUALIZAR EL MARCO NORMATIVO DE PROTECCIÓN DE DATOS: UNA NECESIDAD COMPARTIDA

Los cambios provocados por las nuevas tecnologías de la información, el rol cambiante del ciudadano con la Web 2.0 y su participación activa en el tratamiento de la información o la globalización de los servicios, ha conducido a los reguladores en todo el mundo a liderar la discusión sobre la necesidad de actualizar los diferentes instrumentos legales de privacidad y protección de datos, particularmente a nivel internacional. Por esta razón existen actualmente varios procesos de revisión, en los que la Agencia Española de Protección de Datos está involucrada de manera muy activa.

A. ESTÁNDARES INTERNACIONALES PARA LA PROTECCIÓN DE LA PRIVACIDAD EN RELACIÓN CON EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

Respondiendo al mandato contenido en la Resolución de Madrid, que recoge la propuesta conjunta para la redacción de Estándares Internacionales para la Protección de la Privacidad en relación con el tratamiento de Datos de Carácter Personal, una de las prioridades de la AEPD durante el año 2010 ha sido la promoción y difusión de este texto entre entidades privadas, expertos y organismos públicos nacionales e internacionales. Esta difusión se ha llevado a cabo a varios niveles: Por un lado, la AEPD se ha dirigido a diversas organizaciones internacionales para difundir los Estándares y proponerlos como base para futuros desarrollos normativos. Por otro, ha contactado con multinacionales y con la sociedad civil para demostrar su aplicabilidad práctica, lo que ha conducido, por ejemplo, a que varias empresas multinacionales hayan incluido los Estándares como referente en sus políticas globales de privacidad.

El Congreso de los Diputados y el Senado aprobaron sendas iniciativas parlamentarias reconociendo la propuesta de estándares como una base adecuada para avanzar hacia un instrumento internacional vinculante e instando al Gobierno a promoverlo en la Unión Europea, la Comunidad Iberoamericana y las organizaciones internacionales más relevantes.

Es de resaltar que la Ley de Protección de Datos de Méjico, aprobada en julio de 2010 menciona específicamente estos Estándares como base para su normativa.

B. DIRECTRICES DE PRIVACIDAD Y FLUJOS TRANSFRONTERIZOS DE DATOS DE LA ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICO (OECD)

Las Directrices de privacidad y flujos transfronterizos de datos de la OECD, aprobadas en 1980, fueron la primera declaración internacional sobre privacidad y un texto pionero que representaba un consenso sobre el tratamiento de la información personal en el sector público y privado. Sin embargo, a lo largo de los años se han producido cambios espectaculares en el volumen y el uso de datos personales.

Los grandes cambios son además visibles en los flujos de datos, las transferencias internacionales de datos entre las empresas y organizaciones globales, planteando nuevos retos con respecto a la protección de la intimidad. Asimismo, el desarrollo de la sociedad de la información, tecnologías como las etiquetas RFID, o la videovigilancia y la geolocalización, técnicas que no existían cuando se aprobaron estas Directrices, han planteado desafíos a la protección de datos de carácter personal.

Con el fin de culminar con la revisión de sus Directrices de privacidad y coincidiendo con el 30 aniversario de este texto, a lo largo de 2010 la OECD preparó una serie de eventos de conmemoración. El primero de ellos, se centró en el impacto de las Directrices en los actuales textos de privacidad, tanto a nivel internacional como nacional y contó con la participación del Director de la AEPD.

El segundo encuentro, en el que también participó una representación de la AEPD, tuvo lugar en Jerusalén con ocasión de la 32ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, organizada por la Autoridad de Protección de Datos de Israel (ILITA) y se centró en el papel del individuo en la protección de la privacidad, principalmente a consecuencia de su nuevo rol como agente activo en el marco de la Web 2.0.

El tercer evento se refirió a la dimensión económica de la privacidad y tuvo lugar en Paris, reuniendo tanto a agentes del sector privado como autoridades de protección de datos. Junto con estos eventos, la OCDE está preparando un informe de aniversario sobre la evolución de la privacidad desde 1980 que sentará las bases, junto con las conclusiones de estos eventos, de la revisión de las Directrices que tendrá lugar a lo largo de 2011.

C. RESOLUCIÓN SOBRE LA PROTECCIÓN DE DATOS Y LA PRIVACIDAD EN EL TERCER MILENIO

El Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo Adicional son dos instrumentos vinculantes a nivel internacional. Con el fin de encontrar soluciones adecuadas a los nuevos retos planteados por la tecnología y la globalización de la información, el Comité de Ministros del Consejo de Europa aprobó una *"Resolución sobre la Protección de Datos y la Privacidad en el Tercer Milenio"*, en el que Consejo de Europa apoya la modernización del Convenio 108, teniendo en cuenta los desarrollos internacionales en la materia y contando con la participación de otros Estados y Organizaciones. Destacar la expresa mención a la Resolución de Madrid en su exposición de motivos, y el hecho de que se impulse la protección de datos "como una prioridad para el futuro trabajo del Consejo de Europa".

La Agencia Española de Protección de Datos participará en la preparación de los borradores de dictámenes.

D. NUEVOS HORIZONTES PARA LA PROTECCIÓN DE DATOS EN ESTADOS UNIDOS

La Comisión Federal de Comercio (FTC) de los Estados Unidos llevó a cabo durante el año 2009 una serie de mesas redondas para explorar los desafíos para la privacidad actuales desde el punto de vista de la tecnología y las prácticas empresariales. Fruto de los temas planteados y desarrollados en esas mesas redondas, la FTC aprobó en diciembre de 2010 el documento *"Protecting Consumer Privacy in an Era of Rapid Change: A proposed framework for businesses and policy makers"*. Este documento que propone un nuevo marco para tratar los datos de los consumidores se construye sobre el principio de "notificación y elección" (*notice and choice*) y el modelo "basado en el perjuicio" (*harm based models).* Este marco se aplicaría a las entidades comerciales tanto dentro como fuera de Internet que recojan, mantengan, compartan o utilicen datos de consumidores que puedan ser *razonablemente vinculados a un consumidor concreto, ordenador o dispositivo*. El documento propone una serie de medidas como el principio de privacidad desde el diseño (*Privacy by design*) o el sistema *"Do Not Track"*, que supone dar a los usuarios la capacidad de elección en los diferentes tratamientos sobre todo en el entorno online. Por último, el personal de la FTC propone una serie de medidas que las compañías deberían tener en cuenta para que sus prácticas fueran más transparentes. La FTC ha sometido este documento a comentarios, con los que emitirá un informe final en 2011.

Aunque la FTC de los Estados Unidos lleva trabajando en temas de privacidad desde 1970, la propuesta de un marco de privacidad supone un gran avance para la consecución de una mayor armonización de las prácticas de protección de datos a nivel global. Además, este organismo coordina el *Global Privacy Enforcement Network*, una red global de cooperación en el que los miembros, entre los que se encuentra la AEPD, cooperan en casos transfronterizos en materia de privacidad y protección de datos.

E. LA DIRECTIVA EUROPEA DE PROTECCIÓN DE DATOS

En el plano europeo el panorama de tratamiento de datos también ha cambiado. Las nuevas tecnologías de la información, la computación en nube, las redes sociales o el marketing basado en comportamiento son algunos de los desafíos ante los que se encuentra esta norma. Además, los tratamientos internacionales de datos, la globalización de los servicios y sus flujos de datos provocan una disolución de fronteras que requiere una mayor cooperación entre autoridades de protección de datos, así como una mayor dotación de competencias para el ejercicio de su labor garante de privacidad. Todo ello hace necesario actualizar las normas actuales con el fin de adaptarlas a esta realidad cambiante y a la sociedad de la información.

Consciente de esta situación, el 4 de noviembre de 2010, la Comisión hizo pública una Comunicación donde, bajo el título *"Una aproximación global a la protección de los datos personales en la Unión Europea"*, fija las prioridades y esboza las líneas maestras del futuro marco legal europeo.

En esta Comunicación, la Comisión reitera la vigencia de los principios centrales del régimen actual de protección de datos insistiendo en la necesidad de que las adaptaciones que actualicen, clarifiquen, refuercen y doten de mayor coherencia interna al sistema.

Entre los temas que centran la atención de la Comisión podrían destacarse:

- La preocupación por lograr un mayor grado de armonización de las normativas nacionales de protección de datos;
- La búsqueda de una mayor responsabilidad de los titulares de tratamiento de los datos, con la introducción de un principio que el mundo anglosajón conoce como de *"accountability"*, que en castellano podría traducirse aunque inexactamente, como "rendición de cuentas";
- El interés en lograr una simplificación de trámites administrativos, especialmente a través de una remodelación del actual sistema de notificación;
- La intención de reforzar y aumentar la eficacia del régimen sancionador, incluyendo la posibilidad de tipificar como delitos algunos casos de violaciones de la legislación de protección de datos, la de legitimar a las autoridades de protección de datos o a asociaciones especializadas o de afectados para iniciar acciones ante los tribunales o el reforzamiento, clarificación y armonización del papel de las autoridades de protección de datos.

La Comunicación aborda igualmente cómo mejorar el control de los ciudadanos sobre sus propios datos, a través de mayor transparencia en los tratamientos, reglas más claras y eficaces en materia de consentimiento o promoción a nivel europeo de actividades de sensibilización de los ciudadanos.

La Comunicación trata así mismo otros temas como la extensión de las reglas generales a los temas anteriormente incluidos en el denominado "tercer pilar" -cooperación judicial y policial-, la simplificación y clarificación de las disposiciones relativas a transferencias internacionales o una mejor definición de datos sensibles.

La Comunicación concluye con el anuncio de que la Comisión presentará propuestas de nueva legislación europea en 2011.

5. LAS AUTORIDADES EUROPEAS DE PROTECCION DE DATOS ANTE LOS NUEVOS RETOS

El Grupo de Trabajo del Artículo 29 (GT 29) 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. La Agencia Española de Protección de Datos, que forma parte del mismo desde su inicio en febrero de 1997, asumió la vicepresidencia del mismo en febrero de 2010. Para este grupo el año 2010 se ha caracterizado por una intensa actividad, que se ha materializado en la aprobación de varios dictámenes de muy diversa índole en los que la Agencia ha participado activamente.

En concreto, dado el carácter consultivo de este grupo para la Comisión Europea, ha estado involucrado en todo el proceso de revisión de la Directiva, razón por la cual ha aprobado a lo largo del año 2010 diversos dictámenes que la interpretan y que complementan al documento sobre el Futuro de la Privacidad adoptado en 2009.

A. DICTAMEN 8/2010 SOBRE LEY APLICABLE (WP 179)

Este dictamen aclara el contenido del artículo 4 de la Directiva 95/46/CE de protección de datos, relativo a su ámbito de aplicación. Además de los criterios establecidos ya en la Directiva, se refiere a una serie de criterios adicionales que podrían aplicarse cuando el responsable del tratamiento está establecido fuera de la Unión Europea, con el fin de asegurar que existe una conexión suficiente con el territorio de la UE, y evitar el que éste pueda llevar a cabo tratamientos de datos ilegales. Uno de estos criterios sería el de "servicios dirigidos a los individuos", que implica la introducción de un criterio para la aplicación de la legislación de protección de datos de la Unión Europea cuando la actividad de tratamiento de datos personales esté dirigida a las personas dentro de este territorio.

B. DICTAMEN 3/2010 SOBRE EL PRINCIPIO DE *RESPONSABILIDAD* ("ACCOUNTABILITY") (WP 173)

El dictamen presenta la propuesta de introducir el principio de rendición de cuentas de los responsables del tratamiento, que ya se recogía en las Directrices de Privacidad de la OECD y que se refiere a la responsabilidad sobre la aplicación de medidas apropiadas y eficaces que garanticen los principios y obligaciones que dispone la Directiva. Así mismo, supone capacidad de demostrarla cuando se solicite por las autoridades de control. El Dictamen contiene sugerencias para garantizar que el principio de responsabilidad aporte seguridad jurídica.

C. DICTAMEN 1/2010 SOBRE LOS CONCEPTOS DE "RESPONSABLE DEL TRATAMIENTO" Y "ENCARGADO DEL TRATAMIENTO" (WP 169)

Estos conceptos desempeñan un papel fundamental en la aplicación de la Directiva 95/46/CE, puesto que determinan quienes son los sujetos responsables del cumplimiento de las normas de protección de datos, cómo pueden ejercer sus derechos los interesados, cuál es la legislación nacional aplicable y con qué eficacia pueden operar las autoridades de protección de datos.

D. INFORME 1/2010 SOBRE LA SEGUNDA INVESTIGACIÓN CONJUNTA: CUMPLIMIENTO A NIVEL NACIONAL DE LOS PROVEEDORES DE TELECOMUNICACIONES Y PROVEEDORES DE SERVICIOS DE INTERNET EN RELACIÓN CON LAS OBLIGACIONES REQUERIDAS POR LA LEGISLACIÓN DE CONSERVACIÓN DE DATOS (WP 172)

El GT 29 aprobó el informe sobre la segunda inspección conjunta a nivel europeo, que se centró en esta ocasión sobre la transposición de la directiva de retención de datos de telecomunicaciones en cada uno de los Estados miembros. El documento presenta una doble perspectiva: Por un lado, supone un ejercicio práctico dirigido a analizar el tratamiento de los datos por parte de los proveedores de telecomunicaciones y proveedores de servicios de Internet y por otro, dar un mensaje para la Comisión, que durante el año 2010 trabajó en un informe de evaluación de la Directiva de Retención de Datos, elaborado de forma conjunta por los gabinetes de tres comisarios. A resaltar que, fruto de esta investigación conjunta, se constató que la trasposición y aplicación de la Directiva de conservación de datos se ha producido de forma heterogénea en los Estados Miembros.

La realización de la inspección conjunta supone un avance hacia la necesaria actuación coordinada de las Autoridades europeas.

La lista completa de todos los documentos aprobados en 2010 por el GT 29 puede consultarse en el siguiente hipervínculo:

http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm

E. ACTUACIONES EN EL ÁREA DE COOPERACIÓN POLICIAL Y JUDICIAL

La Agencia Española de Protección de Datos ha participado activamente en los principales desarrollos relativos a la protección de datos en el ámbito de la cooperación policial y judicial, bien a través de su participación en los órganos comunes de control, como parte de las tareas asumidas por el Grupo del Artículo 29 y por Grupo de Trabajo de Policía y Justicia, así como por su colaboración con las autoridades nacionales competentes en materia de Policía y Justicia.

No se puede dejar de lado en este ámbito el impacto que el nuevo marco jurídico que emana del Tratado de Lisboa va a tener en esta área. La desaparición de la estructura de pilares conduce de forma necesaria a la unificación en la normativa de protección de datos en todos los ámbitos de actuación si bien desde diversos estamentos se subraya la necesidad de mantener un cierto grado de especificidad en la aplicación de la norma para este tipo de tratamientos. Por otro lado, la existencia de normativa preexistente -Decisión Marco, normativa de Europol, Eurojust, Schengen y otros- augura un proceso de transición largo y no exento de dificultades.

Tres son los desarrollos que han centrado la atención en este ámbito a lo largo de 2010:

Acuerdo TFTP II (Swift: transferencia de datos financieros)

Por decisión del Consejo de fecha 13 de julio de 2010 quedaba aprobado el Acuerdo entre la Unión Europea y los Estados Unidos sobre el tratamiento y la transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos a efectos del Programa de Seguimiento de la Financiación del Terrorismo. Dicho acuerdo tiene como objeto principal permitir la transferencia de datos sobre transacciones financieras desde la UE a Estados Unidos con la finalidad de que puedan ser usados por las autoridades estadounidenses para la prevención y lucha contra el terrorismo. Este acuerdo sucede a uno anterior que fue rechazado por el Parlamento Europeo al considerar insuficientes las disposiciones referidas a la protección de datos de carácter personal.

Tanto el Grupo del Artículo 29 como el Grupo de Policía y Justicia han expresado su preocupación por el contenido del acuerdo toda vez que, si bien supone una mejora respecto al anterior al incluir garantías adicionales sobre protección de datos, se han identificado algunos aspectos, tanto en relación con los derechos de las personas como en lo referido a las competencias de control por parte de las Autoridades de Protección de Datos, en los que el nivel de protección no sería suficiente. Igualmente se han señalado deficiencias relacionadas con la posibilidad de realizar transferencias masivas de datos a la vez que se insiste en la necesidad de asegurar que no se producen transferencias de datos procedentes del Área Única de Pagos Europea.

Decisión Marco sobre protección de datos en el ámbito de la cooperación policial y judicial

La Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, nace con la idea de ofrecer un alto nivel de protección en los tratamientos de datos personales en el marco de la cooperación policial y judicial en materia penal garantizando a su vez un alto nivel de seguridad pública.

La comunidad de protección de datos fue muy activa durante el proceso de desarrollo de la norma señalando aquellos elementos que suponían un riesgo o una limitación a la protección efectiva de los derechos de los ciudadanos. Elemento de particular discusión fue el ámbito de aplicación de la norma, que finalmente dejó fuera de su protección los tratamientos realizados a nivel doméstico lo que podría implicar que, en algunos casos, datos transferidos de un país tengan un mayor nivel de protección que los datos tratados a nivel nacional.

En el año 2010 se han iniciado los procesos de incorporación de la norma a los ordenamientos jurídicos de los Estados miembros, que deberán concluir en 2011.

Registro de datos de viajeros

A lo largo del año se han llevado a cabo los trabajos que han culminado en la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre el uso de registros de datos de viajeros para la prevención, detección, investigación y persecución de delitos de terrorismo y de delincuencia grave que ha visto la luz en febrero de 2011. La propuesta deberá recibir el visto bueno del Consejo y del Parlamento Europeo para convertirse en una realidad y los Estados tendrán un periodo de adaptación para trasponer la norma a sus legislaciones.

En cuanto a los acuerdos PNR con terceros países, la Comisión Europea, tras hacer pública una Comunicación sobre el enfoque global de las transferencias de datos de los registros de nombres de los pasajeros (PNR) a terceros países, inició el proceso de negociación de forma simultánea con Australia, Canadá y los Estados Unidos.

Por su parte, el Parlamento Europeo, que mantiene un seguimiento activo de este tema, emitió el 11 de noviembre de 2010 una resolución sobre el enfoque global de las transferencias de datos de los registros de nombres de los pasajeros (PNR) a los terceros países en el que señala que el fundamento jurídico debe incluir el artículo 16 del TFUE, la necesidad de respetar el principio de proporcionalidad así como su firme oposición a que los datos sean utilizados para la elaboración de perfiles.

F. AVANCES EN OTROS FOROS INTERNACIONALES

El Comité de Ministros del Consejo de Europa aprobó, el 23 de noviembre de 2010 una *Recomendación sobre la protección de las personas en relación al tratamiento automatizado de sus datos para la elaboración de perfiles*. Este documento, tiene especial importancia en sectores como el financiero o el publicitario, puesto que trata de regular las normas y condiciones en las cuales se puede recabar información de los interesados a los efectos de crear perfiles, y cómo la asignación de uno de dichos perfiles puede influir sobre el acceso a bienes y servicios.

Los días 15 y 16 de abril de 2010, la AEPD organizó en Granada la 42ª reunión del Grupo de Berlín de Telecomunicaciones a la que asistieron 50 autoridades de protección de datos, expertos internacionales e instituciones como la OCDE, el Supervisor Europeo de Protección de Datos, la Comisión Federal de Comercio (FTC) y el Departamento de Seguridad de EE.UU., la Agencia de Seguridad de la Información de Corea y la Comisión Europea.

Fruto de la reunión, se aprobó la *"Carta de Granada de derechos a la privacidad en el mundo digital"*

http://www.datenschutz-berlin.de/attachments/696/Granada_Charter_675_40_11.pdf?1292413679 (Inglés),

documento de referencia para la estandarización de las garantías de privacidad que define los principios que deben respetar usuarios, proveedores y autoridades públicas para garantizar el derecho a la privacidad en este entorno. Esta Carta supone la aprobación de un catálogo de los derechos básicos de privacidad en el entorno digital.

G. LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS: LA CONSOLIDACIÓN DE UN PROYECTO

El año 2010 debe considerarse un hito en el marco de la Red Iberoamericana de Protección de Datos por los avances normativos que se han producido en países latinoamericanos en relación con la protección de datos personales.

En el mes de junio se publicó en el portal del Congreso de la República de Perú el proyecto de Ley de datos personales, para su tramitación parlamentaria. En julio entró en vigor en México la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. En diciembre el Congreso de la República de Colombia aprobó la Ley de Protección de Datos Personales. La República oriental del Uruguay, tras la aprobación de la normativa sobre protección de datos personales se encuentra en proceso de obtener una Declaración de la Adecuación de la Comisión Europea que la homologue, en este ámbito, con los Estados miembros de Unión. A lo que se une la obtención por el Principado de Andorra, en el mes de octubre, de dicha Declaración de Adecuación.

Los avances legislativos en Latinoamérica, inspirados en la normativa europea y en los estándares internacionales de la "Resolución de Madrid", pueden considerarse como el mayor avance regional en materia de protección de datos en un mundo globalizado.

La consolidación de la Red Iberoamericana de Protección de Datos se ha manifestado, también, en su estructura organizativa. Por primera vez desde su constitución formal en 2003 la Presidencia de la Red, atribuida desde entonces a la AEPD, ha pasado a ser asumida por el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) de México, renovándose asimismo el Comité Ejecutivo integrado por representantes de Colombia, Costa Rica, Uruguay y España.

La rotación de la Presidencia y la consolidación del Comité Ejecutivo revelan el nivel de madurez alcanzado por la Red Iberoamericana.

La Red ha seguido desarrollando iniciativas de promoción para la protección de los datos personales. En junio se celebró en Montevideo un Seminario regional en el que participaron 11 países que forman parte de MERCOSUR, Portugal, España y asociaciones civiles y del sector privado, representativas de 32 instituciones. Se abordaron temas relacionados con las Transferencias Internacionales de Datos, la armonización entre las leyes de transparencia y los estándares internacionales de protección de datos, la interoperabilidad frente a la Privacidad en el entorno de las Administraciones Públicas, el tratamiento de los datos personales en el ámbito jurisdiccional, así como la regularización Internacional de los Bureau de información crediticia y el tratamiento de datos sensibles por parte de las empresas.

En julio tuvo lugar en Cartagena de Indias (Colombia) el seminario "Nuevas tecnologías: Seguridad vs. Privacidad" con participación de 15 países, representado por 36 instituciones, el Supervisor Europeo de Protección de Datos, el Cuerpo Nacional de Policía de España y expertos de asociaciones civiles y del sector privado (Google, Yahoo! y Telefónica). Se abordaron temas relacionados con la Seguridad y Privacidad en el marco de las Telecomunicaciones, el sector financiero, el transporte aéreo, la criminalidad en la Red, los movimientos migratorios, la cooperación Policial y Judicial y la tecnología avanzada como límite a la privacidad.

En septiembre se celebró en Ciudad de México el VIII Encuentro Iberoamericano de Protección de Datos en el que se adoptó la Declaración de México que aborda el incremento de los riesgos a los derechos fundamentales como consecuencia del vertiginoso avance de las tecnologías de la información; la prestación de servicios a través del "Cloud Computing"; las oportunidades y riesgos para la integridad física y moral, sobre todo de niños y adolescentes que genera Internet debido a la información compartida sin límite a través de las redes sociales; los desafíos del avance de la genética y la necesidad de un marco legal indispensable y de órganos responsables de su aplicación que cuenten con las condiciones óptimas para el cabal cumplimiento de sus funciones.

La Declaración recoge un listado de compromisos relativos al impulso gubernativo de leyes que reconozcan la tutela efectiva de este derecho fundamental; la promoción de la solidez, experiencia e independencia así como la obtención de recursos necesarios por parte de las autoridades garantes de este derecho; sensibilizar a la población sobre la importancia que reviste la protección efectiva de los datos personales y promover la adopción de estándares regionales e internacionales que ofrezcan un modelo de regulación que garantice un alto nivel de protección y facilite un eficiente intercambio internacional de datos personales.

La relevancia internacional de la Red Iberoamericana se ha proyectado en la designación del IFAI, que ostenta su Presidencia, como organizador de la 33º Conferencia Internacional de Comisionados de Privacidad y Protección de Datos que tendrá lugar en 2011.

6. COOPERACIÓN CON LAS AGENCIAS AUTONÓMICAS DE PROTECCIÓN DE DATOS

Los aspectos más destacados en la cooperación entre las Agencias de protección de Datos han sido los siguientes:

- La mejora de los intercambios de información entre los Registros de las respectivas Agencias encontrándose en fase de desarrollo el sistema RENO (Registro de Notificaciones).

- La coordinación de criterios para la aplicación de la normativa de protección de datos en el ámbito de la Administración de Justicia tanto en lo relativo a los órganos jurisdiccionales como respecto de las Administraciones Autonómicas con competencia para la provisión de medios a aquellos.

- La política de promoción de información a menores y adolescentes mediante la puesta en común de iniciativas propios o de terceros ya elaboradas con el fin de evaluarlas y tratar de articular conjuntamente una propuesta formativa.

- El intercambio de información sobre las acciones desarrolladas para la promoción e impulso de la Resolución de Madrid.

- El intercambio de información sobre el grupo de trabajo que a nivel internacional está analizando el concepto de "accountability".

Las Agencias de Protección de Datos han colaborado también en la participación en las Jornadas sobre Tecnologías de la Información para la Modernización de las Administraciones Públicas (TECNIMAP 2010) permitiendo tener una presencia institucional relevante.

En el ámbito normativo cabe destacar la aprobación de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos que adecúa sus funciones al Estatuto de Autonomía de Cataluña de 2006 e incorpora como novedad la designación parlamentaria por mayoría cualificada de su Director o Directora.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

RECOMENDACIONES

RECOMENDACIONES

RECOMENDACIONES NORMATIVAS

a) Revisión de los procedimientos de notificación de resoluciones administrativas previstos en la Ley 30/1992, de 26 de noviembre.

Son múltiples los supuestos en que se hacen públicos en boletines o tablones de anuncios de actos administrativos que permanecen indefinidamente en la red habitualmente sujetos a la captura por buscadores y que afectan a la privacidad del notificado: indultos, sanciones administrativas, notificaciones de emplazamientos, multas de tráfico, etc...

La actual previsión normativa requiere que se produzca una identificación inequívoca del destinatario, planteándose dudas acerca de si cualquier información que no incluya el nombre del mismo resultaría suficientemente identificativa corriendo el riesgo en caso contrario de que la notificación sea susceptible de anulación.

La conciliación de la obligación de identificar al destinatario con la necesaria salvaguardia de su privacidad en el presente y en el futuro amenazada por la inserción en Internet y la captación por buscadores puede realizarse si se utiliza como forma identificativa los dígitos y letra del Documento Nacional de Identidad o documentos asimilados como NIF, CIF o pasaporte, información habitualmente no accesible a terceros sin esfuerzos desproporcionados pero que el destinatario conoce.

Por ello la AEPD recomienda analizar la posible modificación de la Ley 30/1992, de 26 de noviembre, con el fin de incorporar procedimientos de notificación que faciliten la conciliación con la privacidad de los afectados.

RECOMENDACIONES EJECUTIVAS

a) Creación del Responsable de protección de datos.

La figura de una persona o departamento que se encargue de coordinar las tareas relacionadas con el cumplimiento en materia de privacidad y protección de datos personales se considera como una buena práctica en aquellas empresas, corporaciones o Administraciones Públicas en las que el tratamiento de datos de carácter personal represente una parte relevante de su gestión.

Las funciones de esta persona o departamento conllevarían un conocimiento profundo de todas las áreas de negocio pudiendo estar relacionadas con la seguridad de la información, el cumplimiento normativo, las políticas de recursos humanos, la auditoría, el diseño o la adquisición de sistemas de información, etc.

El pleno respaldo de la dirección a la adopción de esta función proporcionaría una mejora significativa en el grado de madurez de la organización afrontando un enfoque proactivo en los temas relacionados con la privacidad y la protección de datos de carácter personal.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

LA AGENCIA EN CIFRAS

1. INSPECCIÓN

ACTUACIONES PREVIAS Y TUTELAS DE DERECHOS INICIADAS

TIPO	2008	2009	2010	% VAR. 2009/2010
Tutela de los derechos de acceso, rectificación, cancelación y oposición	1.687	1.881	**1.643**	-12,65
Actuaciones previas (iniciadas a partir de denuncia o a iniciativa del Director)	2.362	4.136	**4.302**[1]	+4,01
TOTAL	**4.049**	**6.017**	**5.945**	**-0,20**

[1] Las cifras incluyen procedimientos AT (admisión a trámite, solicitudes de mejora de la solicitud no subsanadas), AR (acuerdos de no inicio de PS) y EI (actuaciones de inspección incoadas).

RESOLUCIONES

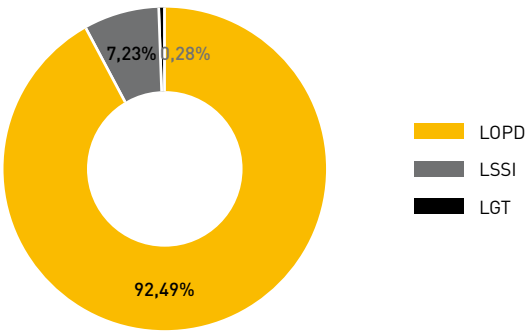
PROCEDIMIENTOS DE LA INSPECCIÓN DE DATOS	2008	2009	2010	% VAR. 2009/2010
Reclamaciones de tutela de los derechos de acceso, rectificación, cancelación y oposición (capitulo II)	1.229	1.947	**1.830**	-6,01
Procedimientos relativos al ejercicio de la potestad sancionadora (capítulo III)	2.419	3.905	**4.359**	11,63
Archivo de actuaciones previas	1.710	3.107	**3.516**	13,16
Procedimientos sancionadores resueltos	630	709	**767**	8,18
Resolución sancionadora	535	621	**591**	-4,83
Resolución de archivo	95	88	**176**	100
Procedimientos de infracción LOPD de las AAPP	79	89	**76**	-14,61
Declaración de infracción	59	71	**61**	-14,08
Declaración de no infracción	20	18	**15**	-16,67
TOTAL CAPÍTULOS II Y III	**3.648**	**5.852**	**6.189**	**5,76**

SANCIONES IMPUESTAS

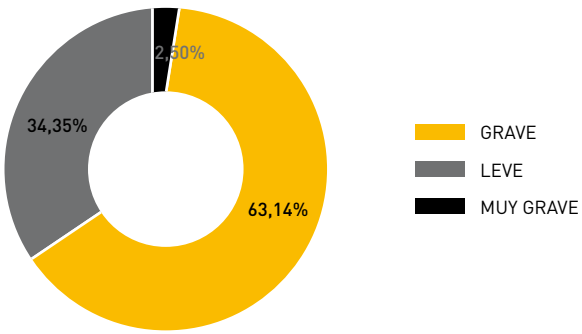
	2008	2009	2010	% VAR. 2009/2010
TOTAL	**22.013.632,57 €**	**24.872.979,72 €**	**17.497.410,02 €**	-29,65

La tabla recoge el total de sanciones declaradas.

SANCIONES IMPUESTAS SEGÚN LEY INFRINGIDA 2010



SANCIONES IMPUESTAS SEGÚN LA GRAVEDAD 2010



DISTRIBUCIÓN DE LAS ACTUACIONES PREVIAS

ACTIVIDAD	2009	2010	% relativo	% VAR. 2009/2010
Telecomunicaciones	908	1.170	**27,2**	28,85
Videovigilancia	721	819	**19,04**	13,59
Entidades financieras	768	691	**16,06**	-10,03
Administración pública	218	194	**4,51**	-11,01
Servicios de Internet (excepto *spam*)	156	168	**3,91**	7,69
Profesionales, admón. fincas, comunidades de propietarios	160	137	**3,18**	-14,38
Comunicaciones electrónicas comerciales - *spam* (LSSI)	180	126	**2,93**	-30
Sanidad	123	114	**2,65**	-7,32
Recursos humanos, asuntos laborales	120	106	**2,46**	-11,67
Publicidad y prospección comercial (excepto *spam*)	52	91	**2,12**	75
Asociaciones, federaciones, colegios profesionales, clubes, fundaciones, ONG's	119	75	**1,74**	-36,97
*Inscripción de ficheros / Información artículo 5	-	75	**1,74**	-
Suministro y comercialización de gas, electricidad y agua	53	74	**1,72**	39,62
Comercios, transporte, hostelería	137	68	**1,58**	-50,36
Medios de comunicación	51	63	**1,46**	23,53
Seguros	47	59	**1,37**	25,53
Fuerzas y cuerpos de seguridad	32	54	**1,26**	68,75
Sindicatos	24	48	**1,12**	100
*Documentación desechada sin destruir o borrar	-	28	**0,65**	-
Enseñanza	34	19	**0,44**	-44,12
Partidos políticos	15	19	**0,44**	26,67
*Derechos ARCO	-	13	**0,3**	-
Procedimientos judiciales	3	9	**0,21**	200
Comunicaciones comerciales por fax (LGT)	25	8	**0,19**	-68
Seguridad privada	10	5	**0,12**	-50
Otros	180	69	**1,6**	-61,67
TOTAL	**4.136**	**4.302**	**100**	**4,01**

* Nuevos epígrafes que en años anteriores se incluían en el apartado "Otros".

DISTRIBUCIÓN DE LOS PROCEDIMIENTOS SANCIONADORES RESUELTOS

ACTIVIDAD	2008	2009	2010	% relativo	% VAR. 2009/2010
Videovigilancia	44	145	**262**	34,16	80,69
Telecomunicaciones	203	182	**169**	22,03	-7,14
Entidades financieras	127	100	**94**	12,26	-6
Comunicaciones electrónicas comerciales - *spam* (LSSI)	46	46	**52**	6,78	13,04
Asociaciones, federaciones, colegios profesionales, clubes	11	24	**26**	3,39	8,33
Comercio, transporte, hostelería	39	23	**23**	3,00	0
Recursos humanos, asuntos laborales	9	18	**20**	2,61	11,11
Suministro y comercialización de gas, electricidad y agua	13	21	**18**	2,35	-14,29
Profesionales, comunidades de propietarios, admón. fincas	13	19	**17**	2,22	-10,53
Servicios de Internet (excepto *spam*)	13	17	**15**	1,96	-11,76
Publicidad y prospección comercial (excepto *spam*)	26	28	**14**	1,83	-50
Sanidad	10	8	**11**	1,43	37,50
*Inscripción de ficheros / Información artículo 5	-	-	**10**	1,30	-
Seguros	6	10	**8**	1,04	-20
Partidos políticos	6	7	**3**	0,39	-57,14
Comunicaciones comerciales por fax (LGT)	9	12	**2**	0,26	-83,33
Administración pública	3	5	**2**	0,26	-60
*Derechos ARCO	-	-	**2**	0,26	-
Otros	41	28	**19**	2,48	-32,14
TOTAL	**630**	**709**	**767**	**100**	**8,18**

* Nuevos epígrafes que en años anteriores se incluían en el apartado "Otros".

Se incluyen procedimientos que acaban con archivo o sanción.

DISTRIBUCIÓN DE LAS RESOLUCIONES SANCIONADORAS

ACTIVIDAD	2008	2009	2010	% relativo	% VAR. 2009/2010
Videovigilancia	27	117	**176**	29,78	50,43
Telecomunicaciones	190	170	**134**	22,67	-21,18
Entidades financieras	111	89	**82**	13,87	-7,87
Comunicaciones electrónicas comerciales - *spam* (LSSI)	39	39	**44**	7,45	12,82
Asociaciones, federaciones, colegios profesionales, clubes	10	20	**22**	3,72	10,00
Recursos humanos, asuntos laborales	5	17	**16**	2,71	-5,88
Suministro y comercialización de gas, electricidad y agua	11	21	**16**	2,71	-23,81
Comercio, transporte, hostelería	31	22	**16**	2,71	-27,27
Profesionales, comunidades de propietarios, admón. fincas	10	15	**14**	2,37	-6,67
Servicios de Internet (excepto *spam*)	10	16	**13**	2,20	-18,75
Publicidad y prospección comercial (excepto *spam*)	22	24	**12**	2,03	-50,00
*Inscripción de ficheros / Información artículo 5	-	-	-	1,35	-
Sanidad	9	6	**7**	1,18	16,67
Seguros	5	8	**7**	1,18	-12,50
Comunicaciones comerciales por fax (LGT)	7	11	**2**	0,34	-81,82
Administración pública (entidades Derecho privado)	2	5	**2**	0,34	-60,00
*Derechos ARCO	-	-	**2**	0,34	-
Partidos políticos	6	5	**2**	0,34	-60,00
Enseñanza	1	5	**1**	0,17	-80,00
Sindicatos	5	4	**1**	0,17	-75,00
Medios de comunicación	3	2	**1**	0,17	-50,00
Otros	31	25	**13**	2,20	-48,00
TOTAL	**535**	**621**	**591**	**100**	**-4,83**

* Nuevos epígrafes que en años anteriores se incluían en el apartado "Otros".

Resoluciones que finalizan con imposición de sanción.

SECTORES CON MAYOR IMPORTE GLOBAL DE SANCIONES

ACTIVIDAD	2010 (€)	% relativo
Telecomunicaciones	9.185.877,87	52,50
Entidades financieras	3.772.072,00	21,56
Suministro y comercialización de gas, electricidad y agua	949.720,17	5,43
Comunicaciones electrónicas comerciales - *spam* (LSSI)	621.114,42	3,55
Videovigilancia	507.327,47	2,90
TOTAL 5 PRIMEROS	**15.036.111,93**	**85,94**
Publicidad y prospección comercial (excepto *spam*)	437.810,28	2,50
Recursos humanos, asuntos laborales	394.013,32	2,25
Comercio, transporte, hostelería	392.713,12	2,24
Sanidad	252.606,86	1,44
Servicios de Internet (excepto *spam*)	170.909,09	0,98
TOTAL 10 PRIMEROS	**16.684.164,60**	**95,35**

SECTORES CON MAYOR NÚMERO DE INFRACCIONES DECLARADAS

ACTIVIDAD	Infracciones declaradas	% relativo
Videovigilancia	230	31,99
Telecomunicaciones	168	23,37
Entidades financieras	86	11,96
Comunicaciones electrónicas comerciales - *spam* (LSSI)	55	7,65
Asociaciones, federaciones y clubes	21	2,92
TOTAL 5 PRIMEROS	**560**	**77,89**
Suministro y comercialización de gas, electricidad y agua	21	2,92
Recursos humanos, asuntos laborales	20	2,78
Comercio, transporte, hostelería	19	2,64
Servicios de Internet (excepto *spam*)	16	2,23
Publicidad y prospección comercial (excepto *spam*)	15	2,08
TOTAL 10 PRIMEROS	**651**	**90,54**

En cada resolución sancionadora puede declararse más de una infracción y, por tanto, imponerse más de una sanción.

PROCEDIMIENTOS DE DECLARACIÓN DE INFRACCIÓN DE LAS ADMINISTRACIONES PÚBLICAS RESUELTOS

TIPO ADMINISTRACIÓN	2008	2009	2010	% relativo	% VAR. 2009/2010
Local	32	22	**32**	42,11	45,45
Estatal	21	17	**25**	32,89	47,06
Autonómica	21	29	**16**	21,05	-44,83
Otras Entidades de Derecho Público	5	21	**3**	3,95	-85,71
TOTAL	**79**	**89**	**76**	**100**	**-14,61**

En un mismo procedimiento de infracción pueden figurar imputados de distintas administraciones territoriales, computándose la resolución en una sola de las administraciones.

Se incluyen procedimientos que finalizan con archivo o declaración de infracción de las AAPP.

INFRACCIONES DE LAS ADMINISTRACIONES PÚBLICAS

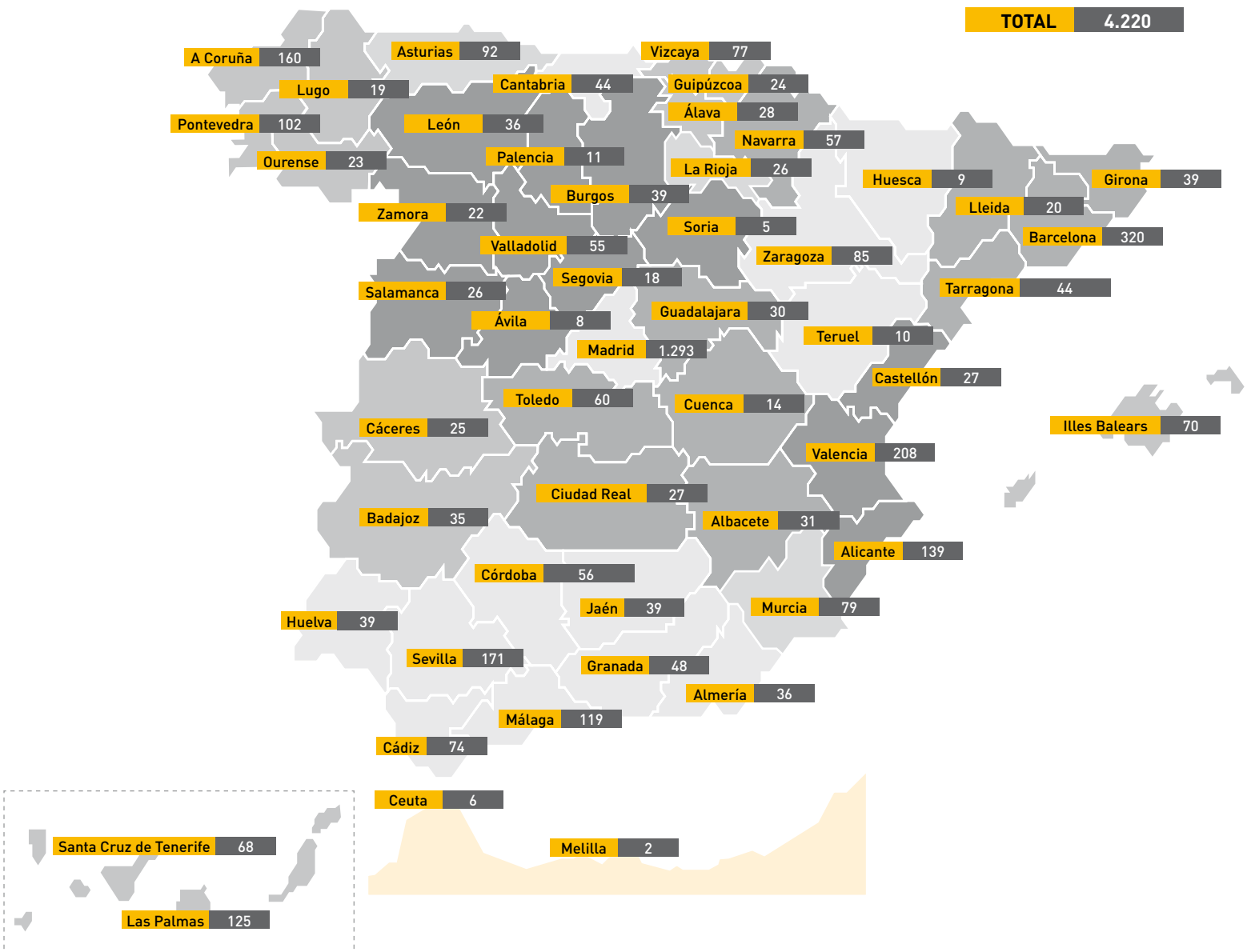
TIPO ADMINISTRACIÓN	2010	% relativo
Local	**29**	41,43
Estatal	**20**	28,57
Autonómica	**19**	27,14
Otras Entidades de Derecho Público	**2**	2,86
TOTAL	**70**	**100**

Resoluciones que finalizan con declaración de infracción de las AAPP.

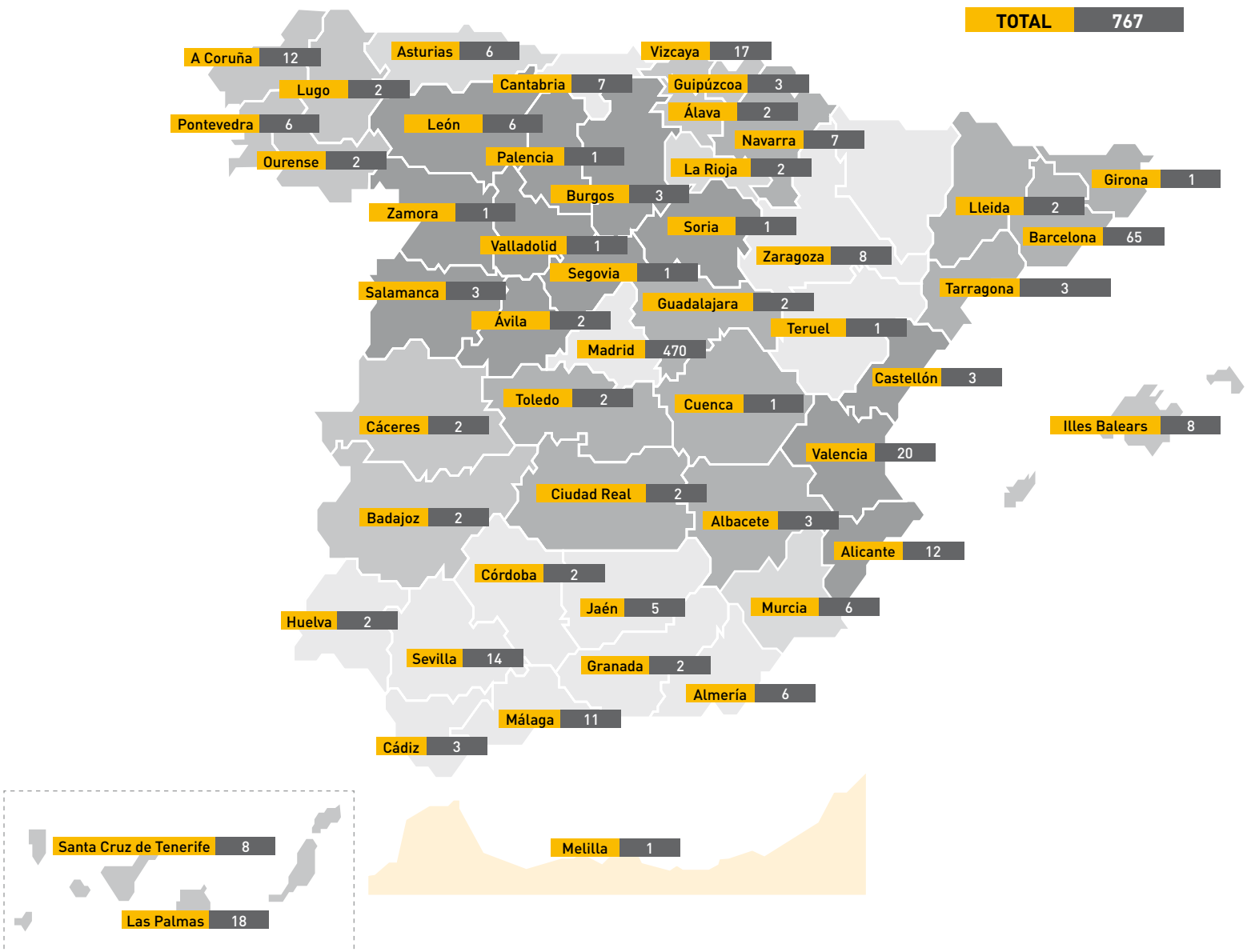
TUTELAS DE DERECHOS RESUELTAS

DERECHOS TUTELADOS	RESOLUCIÓN Estimatoria	Estimatoria Formal-Parcial	Desestimat.	Archiv. Inad./Desi.	Total
Cancelación	232	118	168	470	988
Acceso	236	119	105	202	662
Rectificación	14	11	8	26	59
Oposición	41	14	15	37	107
Varios derechos	2	3	4	5	14
TOTAL	**525**	**265**	**300**	**740**	**1.830**

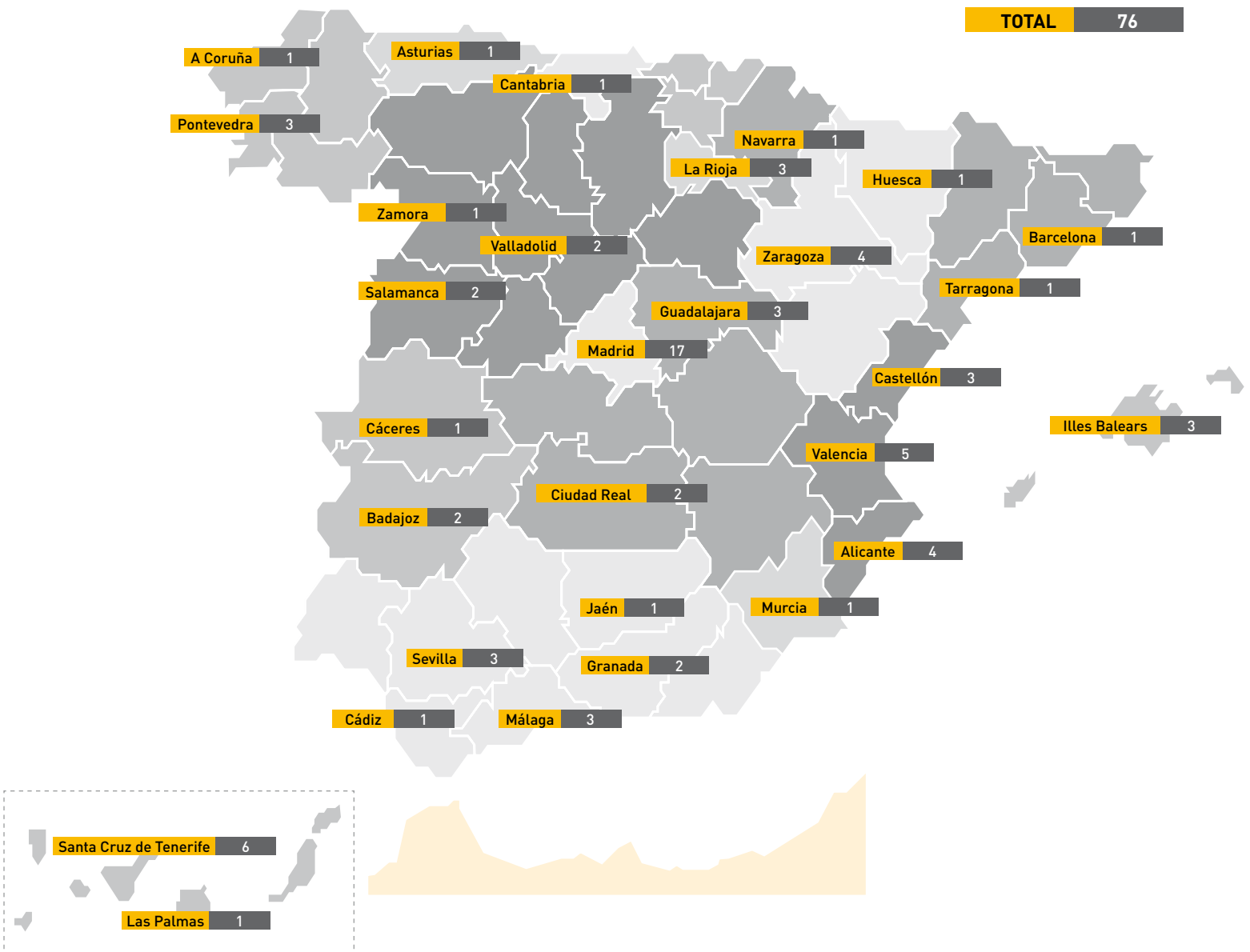
DISTRIBUCIÓN GEOGRÁFICA DE LAS DENUNCIAS (PROVINCIA DEL DENUNCIANTE)



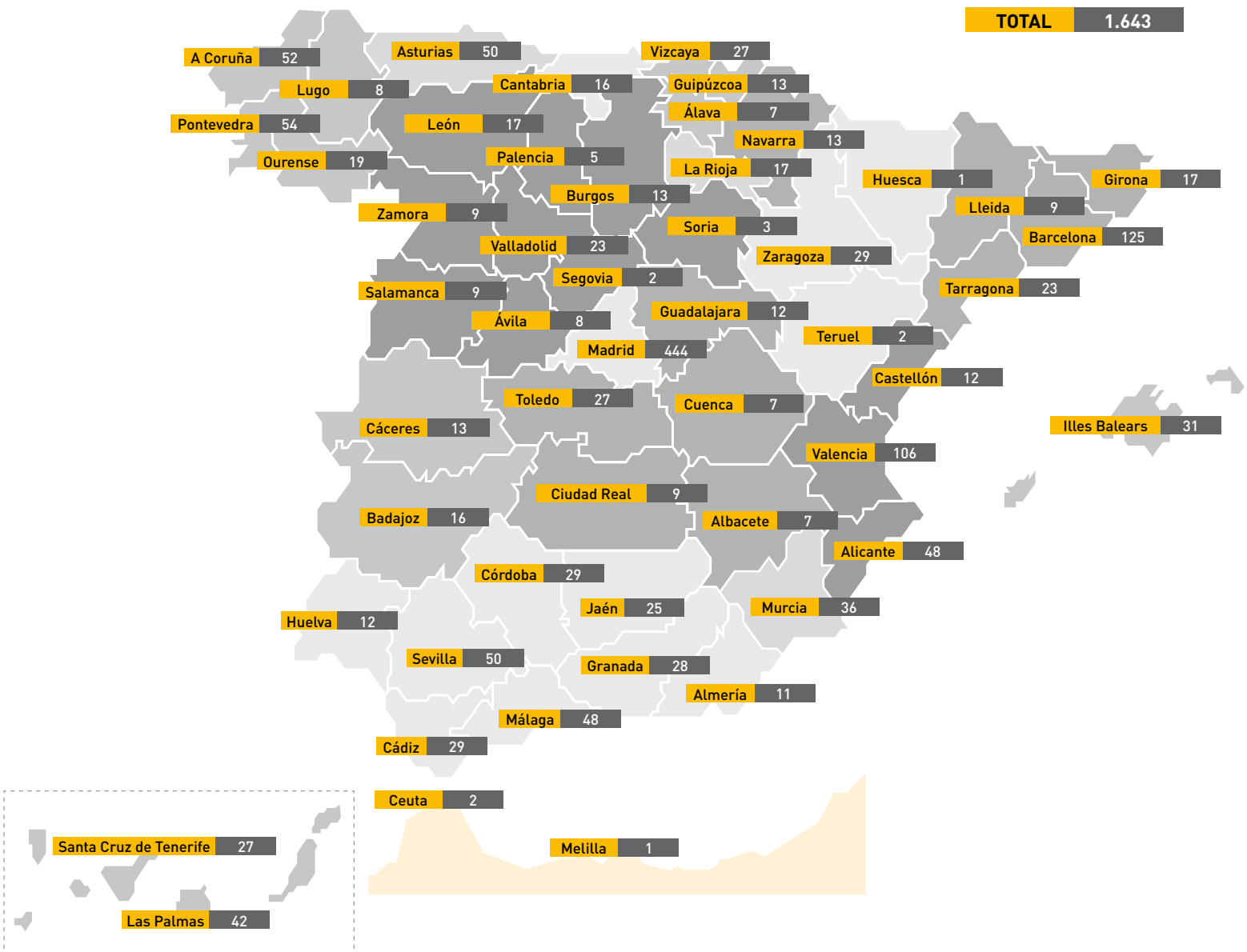
DISTRIBUCIÓN GEOGRÁFICA DE LOS PROCEDIMIENTOS SANCIONADORES



DISTRIBUCIÓN GEOGRÁFICA DE LOS PROCEDIMIENTOS DE DECLARACIÓN DE INFRACCIÓN DE LAS AAPP



DISTRIBUCIÓN GEOGRÁFICA DE LOS PROCEDIMIENTOS DE TUTELA DE DERECHOS (PROVINCIA DEL RECLAMANTE)



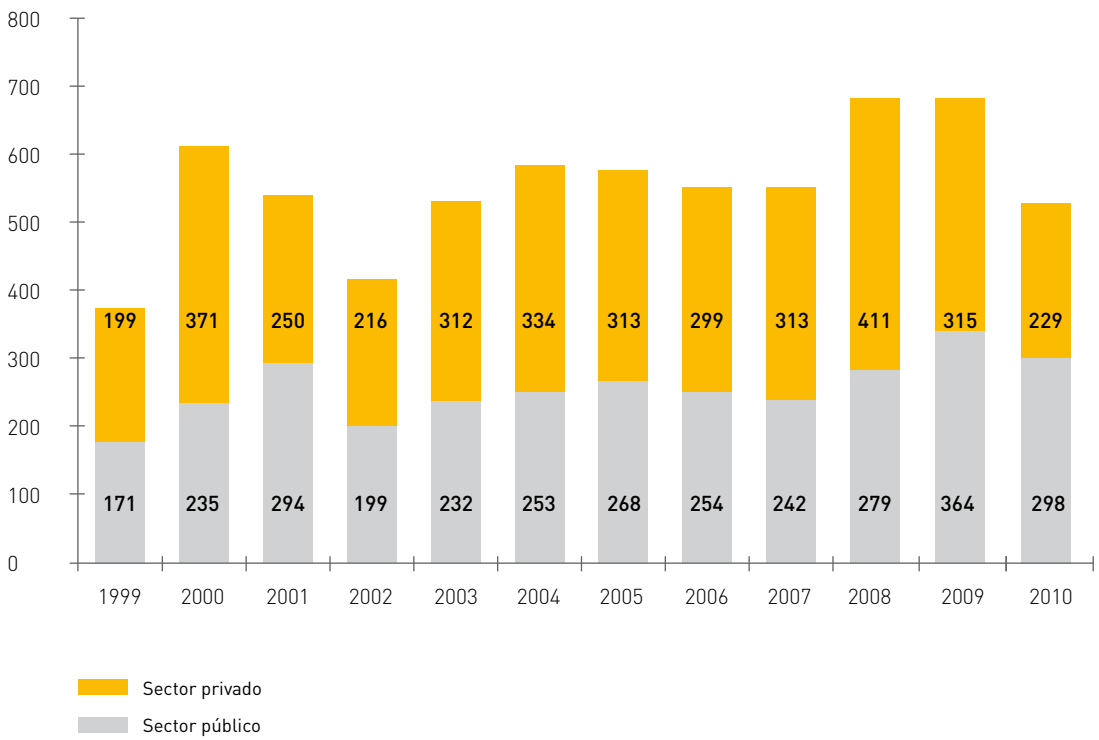
2. GABINETE JURÍDICO

CONSULTAS

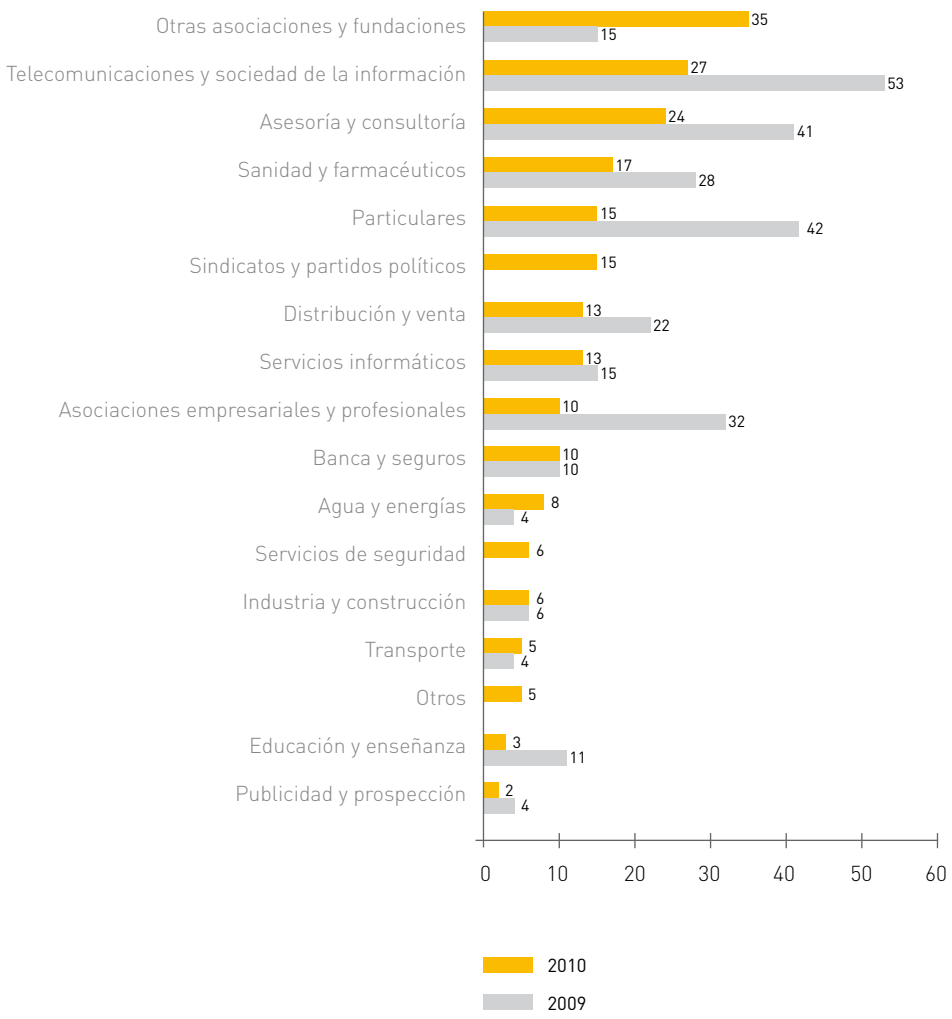
ADMINISTRACIONES PÚBLICAS	298
Administración General del Estado	142
Comunidades Autónomas	36
Entidades Locales	58
Otros Organismos Públicos	62

CONSULTAS PRIVADAS	229
Empresas	152
Particulares	15
Asociaciones/Fundaciones	46
Sindicatos/Partidos políticos	15
Otros	1

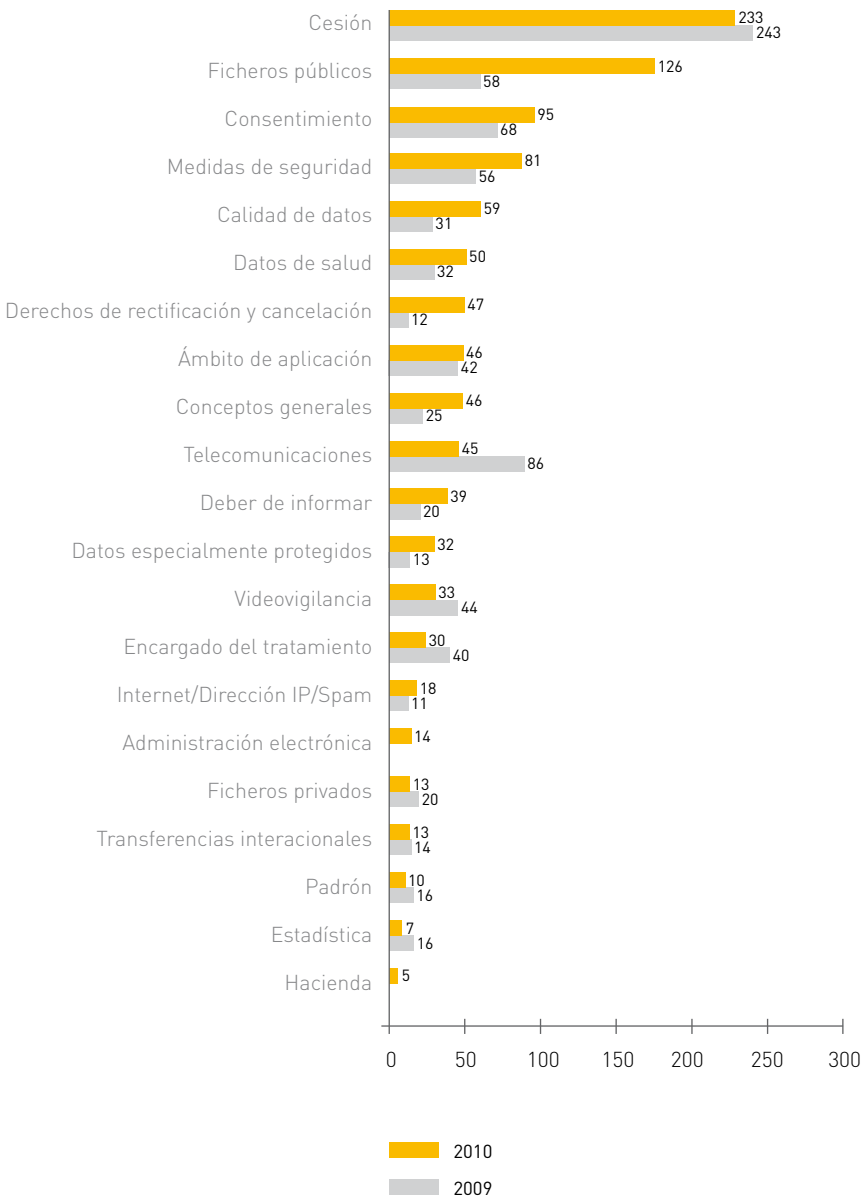
EVOLUCIÓN DE LAS CONSULTAS (1999-2010)



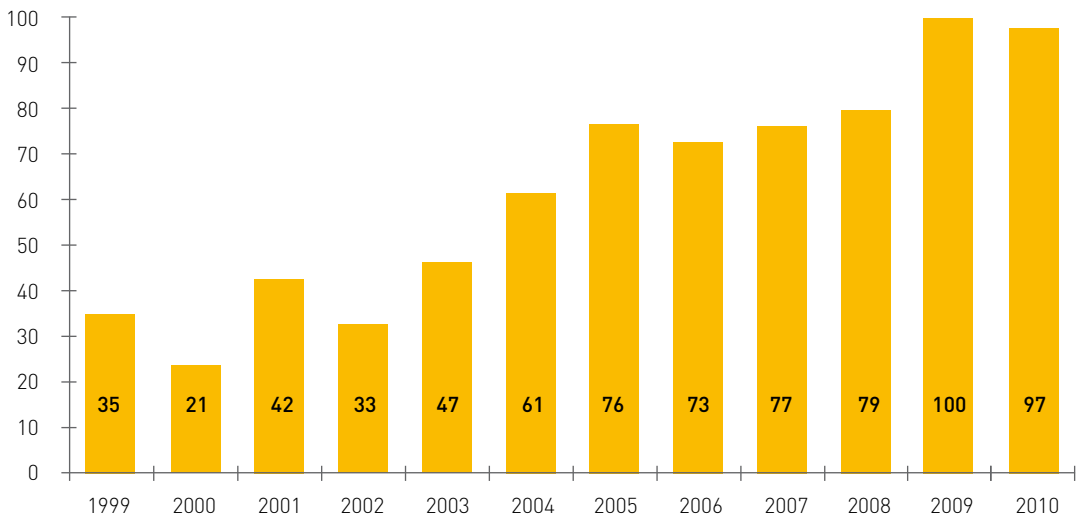
EVOLUCIÓN POR SECTORES (2009-2010)



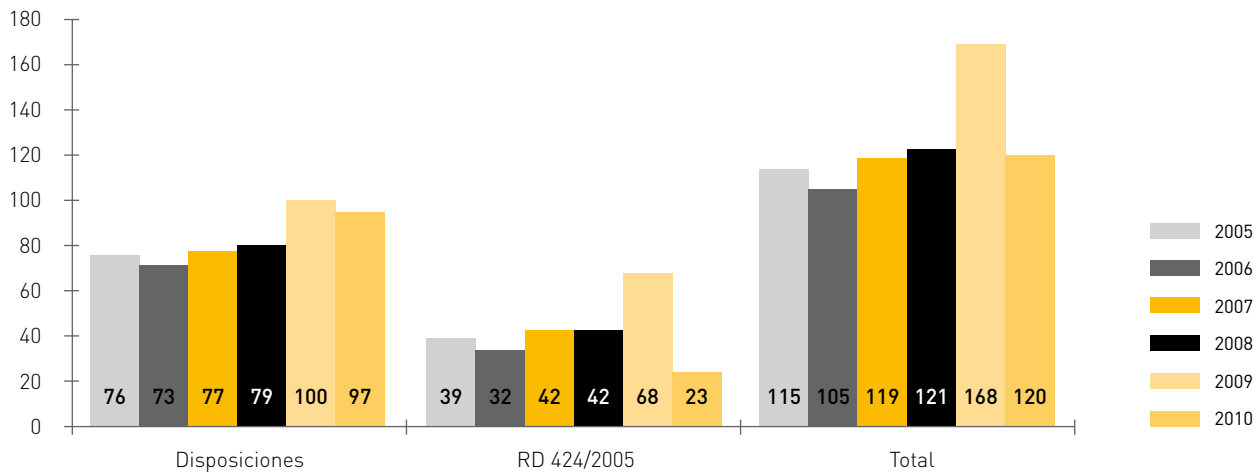
EVOLUCIÓN CONSULTAS POR MATERIAS (2009-2010)



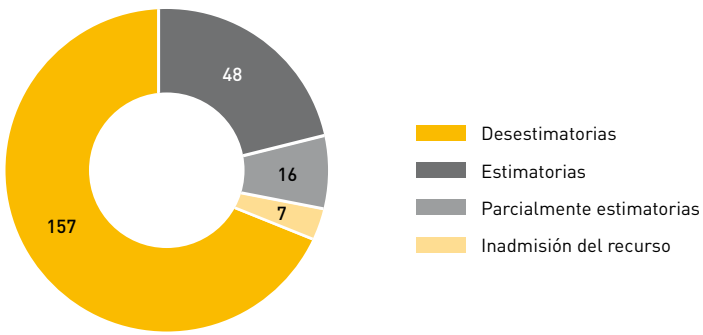
EVOLUCIÓN DE INFORMES PRECEPTIVOS A DISPOSICIONES GENERALES (1999-2010)



INFORMES PRECEPTIVOS (2005-2010)

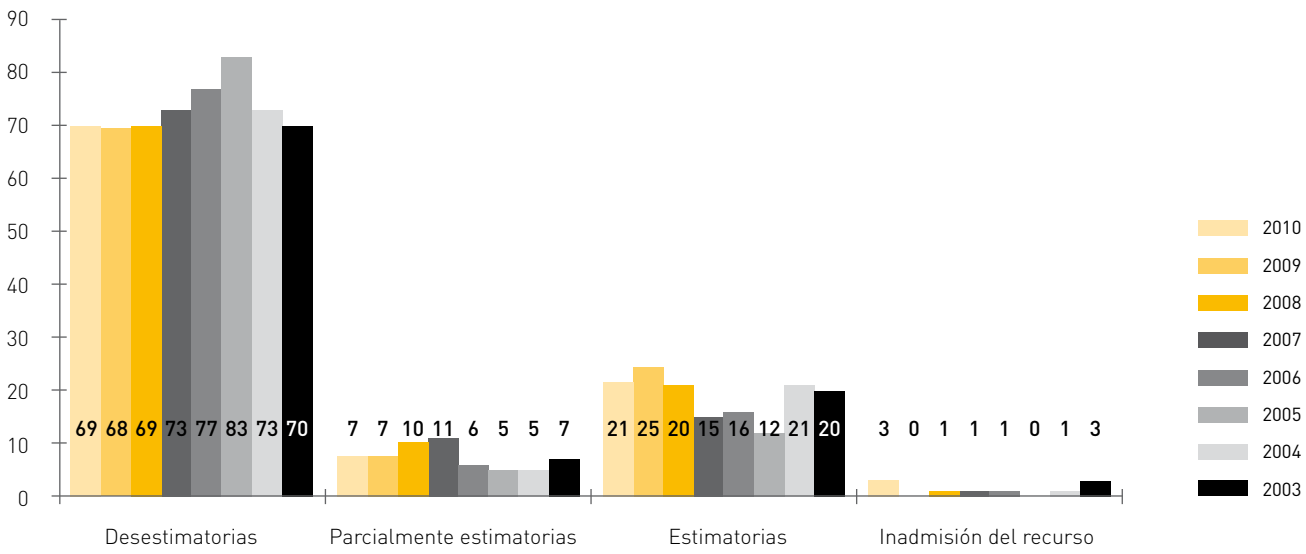


SENTENCIAS DE LA AUDIENCIA NACIONAL



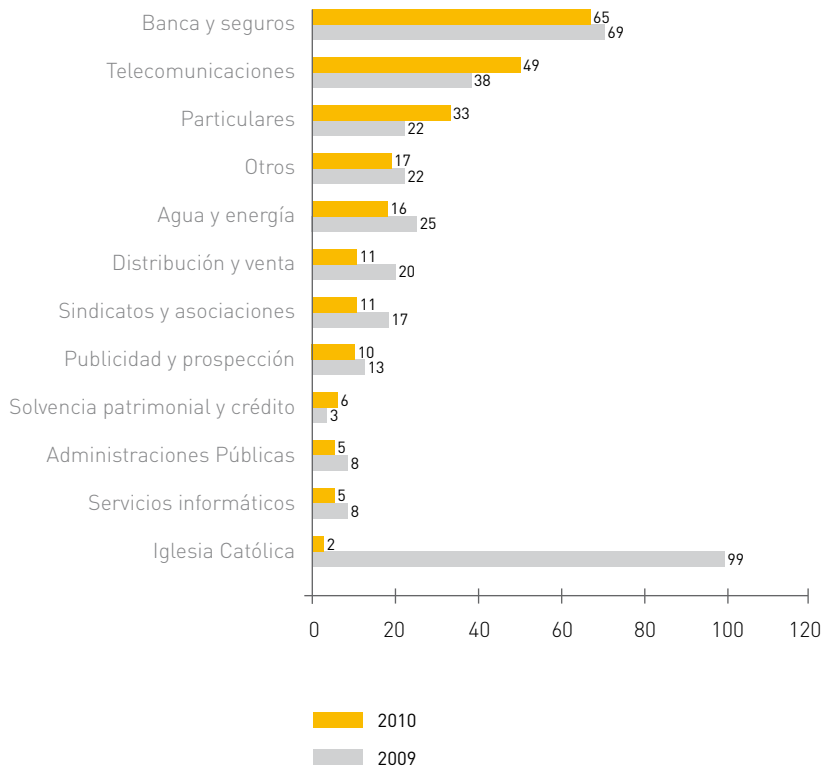
El gráfico exceptúa las cifras relativas a las sentencias dictadas por la AN referidas al ejercicio de cancelación en libros de bautismo.

EVOLUCIÓN DE PORCENTAJES EN SENTENCIAS DE LA AUDIENCIA NACIONAL

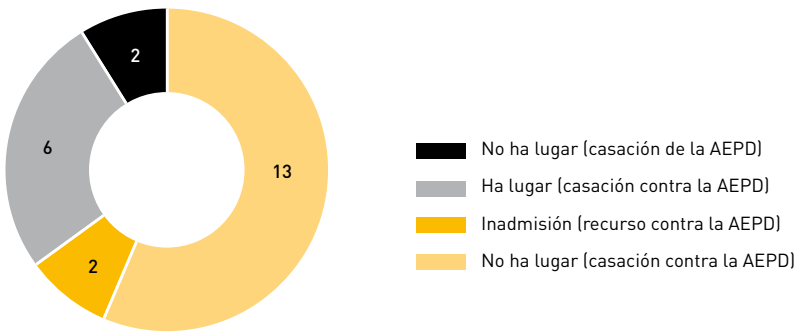


El gráfico exceptúa las cifras relativas a las sentencias dictadas en 2008, 2009 y 2010 por la AN referidas al ejercicio de cancelación en libros de bautismo.

COMPARATIVA SENTENCIAS AUDIENCIA NACIONAL POR SECTOR DEL RECURRENTE (2009-2010)



SENTENCIAS DEL TRIBUNAL SUPREMO



El gráfico exceptúa las cifras relativas a las sentencias dictadas por el TS referidas al ejercicio de cancelación en libros de bautismo.

3. ATENCIÓN AL CIUDADANO

CONSULTAS TOTALES PLANTEADAS ANTE EL ÁREA DE ATENCIÓN AL CIUDADANO

	Atención telefónica	Atención presencial	Atención por escrito	Total	Porcentaje de incremento
Año 2006	27.486	2.030	6.323	35.839	0,9%
Año 2007	33.908	4.185	9.648	47.741	30,09%
Año 2008	58.143	4.785	9.722	72.650	52,17%
Año 2009	77.359	4.277	15.587	97.223	33,82%
Año 2010	**85.276**	**4.093**	**15.457***	**104.826**	**8,2%**

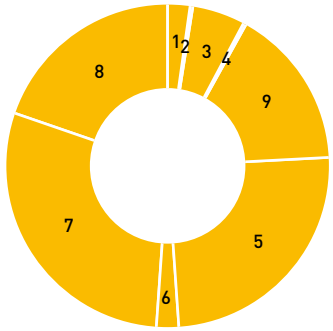
* En el año 2010, 13.600 consultas escritas se contestaron a través de la página Web.

COMPARACION DE ACCESOS A LA PÁGINA WEB CON EL AÑO 2009

AÑO	2009	2010
Acceso a web	2.998.276	**2.499.179**
Promedio diario	8.214,4	**7.619**

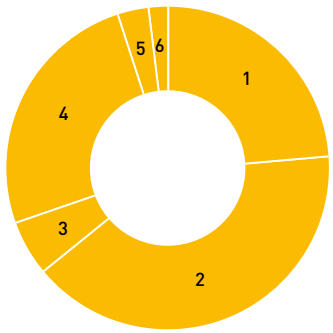
ANÁLISIS DE LAS CONSULTAS POR TEMAS 2010

TEMAS	Porcentaje
1. Información	2,25%
2. Inscripción ficheros	0,34%
3. Principios LOPD	5,38%
4. Infracciones y sanciones	0,14%
5. Ambito de aplicación	24,41%
6. Cesión	2,25%
7. Derechos	28,81%
8. Ficheros concretos	19,56%
9. Otros	16,14%



CONSULTAS SOBRE DERECHOS 2010

TEMAS	Porcentaje
1. Acceso	23,63%
2. Cancelación	40,64%
3. Rectificación	5,44%
4. Oposición	25,51%
5. Información	2,89%
6. Otras consultas sobre derechos	1,87%



4. REGISTRO GENERAL DE PROTECCIÓN DE DATOS

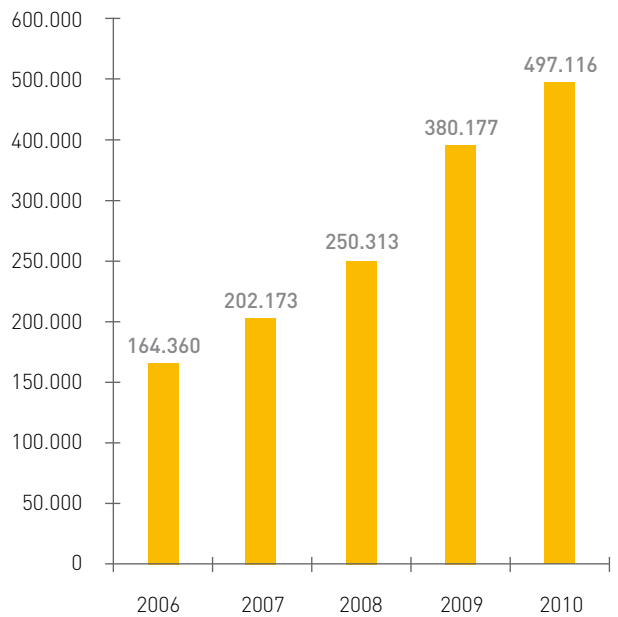
DERECHO DE CONSULTA AL REGISTRO

TITULARIDAD	2009	2010
Privada	1.356.216	**2.002.499**
Pública	1.070.173	**506.351**
TOTAL	**2.426.389**	**2.508.850**

EVOLUCIÓN DE LA INSCRIPCIÓN DE FICHEROS EN EL RGPD

FICHEROS INSCRITOS	2006	2007	2008	2009	2010
Privada	758.955	955.713	1.182.496	1.552.060	**2.036.583**
Pública	56.138	61.553	85.083	95.696	**108.289**
TOTAL	**815.093**	**1.017.266**	**1.267.579**	**1.647.756**	**2.144.872**

Incremento anual total

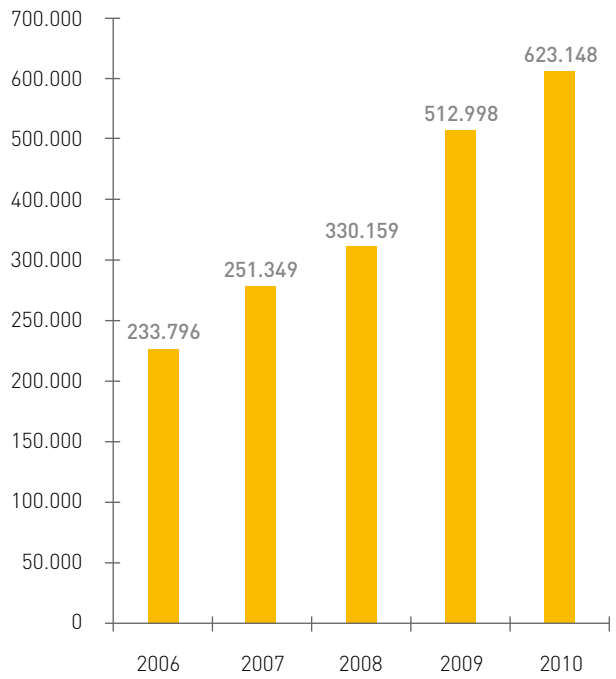


EVOLUCIÓN DE LA INSCRIPCIÓN EN EL RGPD

Datos relacionados con la inscripción

	2009	2010	% VAR. 2009/2010	Media diaria en 2009	Media diaria en 2010
Operaciones de inscripción	512.998	**623.148**	+21	2.137	**2.596**
Total de ficheros inscritos	1.647.456	**2.144.872**	+31	1.584	**2.071**

Incremento anual de las operaciones de inscripción



INSCRIPCIÓN DE TITULARIDAD PRIVADA

Distribución de ficheros

	Responsables		Ficheros	
	2010	Total	2010	Total
Comunidad Autónoma de Andalucía	**36.476**	**101.187**	94.452	**291.032**
Almería	**3.554**	9.996	**9.237**	30.055
Cádiz	**4.605**	11.450	**10.524**	31.496
Córdoba	**3.255**	9.714	**8.449**	27.254
Granada	**4.676**	15.018	**12.094**	47.837
Huelva	**1.952**	4.242	**4.814**	13.051
Jaén	**2.804**	8.191	**7.902**	26.841
Málaga	**8.003**	23.519	**21.021**	58.341
Sevilla	**7.686**	19.594	**20.411**	56.157
Comunidad Autónoma de Aragón	5.981	**29.110**	15.563	**68.791**
Huesca	**1.211**	5.736	**3.321**	13.562
Teruel	**681**	2.359	**1.847**	5.998
Zaragoza	**4.092**	21.063	**10.395**	49.231
Comunidad Autónoma del Principado de Asturias	5.804	**24.255**	14.497	**74.453**
Comunidad Autónoma de Canarias	5.435	**22.035**	14.039	**75.818**
Las Palmas	**2.580**	9.898	**6.649**	35.457
Santa Cruz de Tenerife	**2.862**	12.194	**7.390**	40.361
Comunidad Autónoma de Cantabria	2.583	**8.331**	6.140	**19.233**
Comunidad Autónoma de Castilla y León	12.225	**36.597**	30.590	**96.298**
Ávila	**560**	2.262	**1.318**	4.827
Burgos	**1.690**	6.504	**3.733**	15.534
León	**2.226**	7.215	**5.722**	18.776
Palencia	**1.196**	3.117	**2.579**	7.733
Salamanca	**1.637**	4.116	**4.316**	10.979
Segovia	**939**	2.517	**2.309**	6.381
Soria	**534**	1.341	**1.431**	3.800
Valladolid	**2.399**	7.187	**5.852**	19.174
Zamora	**1.047**	2.428	**3.330**	9.094

	Responsables		Ficheros	
	2010	Total	2010	Total
Comunidad Autónoma de Castilla-La Mancha	**8.658**	**24.625**	21.294	**72.622**
Albacete	**2.187**	7.519	**6.065**	23.982
Ciudad Real	**1.932**	4.896	**4.338**	14.960
Cuenca	**682**	2.515	**1.617**	6.154
Guadalajara	**1.012**	2.549	**2.273**	6.592
Toledo	**2.853**	7.208	**7.001**	20.934
Comunidad Autónoma de Cataluña	**27.098**	**164.045**	74.261	**402.212**
Barcelona	**18.245**	120.995	**48.069**	291.702
Girona	**4.119**	20.468	**13.058**	52.197
Lleida	**1.482**	8.431	**3.573**	20.821
Tarragona	**3.261**	14.448	**9.561**	37.492
Comunidad de Madrid	**31.044**	**125.896**	63.819	**296.942**
Comunidad Valenciana	**26.624**	**91.577**	65.909	**222.415**
Alicante	**8.690**	30.582	**19.955**	69.837
Castellón de la Plana	**3.442**	11.104	**8.332**	28.878
Valencia	**14.502**	49.996	**37.622**	123.700
Comunidad Autónoma de Extremadura	**3.128**	**12.328**	8.648	**33.869**
Badajoz	**2.184**	8.377	**6.207**	22.422
Cáceres	**945**	3.969	**2.441**	11.447
Comunidad Autónoma de Galicia	**16.126**	**53.567**	42.218	**153.736**
A Coruña	**6.901**	23.321	**18.350**	64.370
Lugo	**1.810**	7.297	**4.457**	20.323
Ourense	**2.452**	5.693	**5.494**	15.621
Pontevedra	**4.974**	17.395	**13.917**	53.422
Comunidad Autónoma de las Illes Balears	**4.898**	**15.493**	13.538	**50.978**
Comunidad Foral de Navarra	2.161	**8.757**	5.156	**23.853**
Comunidad Autónoma del País Vasco	**8.379**	**30.213**	17.158	**76.344**
Álava	**1.371**	4.079	**2.734**	10.658
Guipúzcoa	**2.050**	9.050	**4.260**	22.705
Vizcaya	**4.963**	17.142	**10.164**	42.981
Comunidad Autónoma de la Rioja	**1.878**	**7.736**	3.740	**18.785**
Comunidad Autónoma de la Región de Murcia	**8.822**	**23.643**	18.307	**56.757**
Ciudad Autónoma de Ceuta	149	**405**	215	**928**
Ciudad Autónoma de Melilla	224	**390**	958	**1.433**

INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN DE FICHEROS SEGÚN TIPOS DE DATOS	2010	Total
Datos especialmente protegidos (ideología, creencias, religión y afiliación sindical)	**12.995**	64.637
Otros datos especialmente protegidos (origen racial, salud y vida sexual)	**53.844**	284.359
Datos de carácter identificativo	**510.518**	2.036.583
Datos de características personales	**233.825**	878.998
Datos de circunstancias sociales	**129.561**	491.208
Datos académicos y profesionales	**137.379**	482.790
Detalles de empleo y carrera administrativa	**155.260**	649.660
Datos de información comercial	**149.304**	539.513
Datos económico-financieros	**277.489**	1.161.844
Datos de transacciones	**226.004**	804.543
Otros tipos de datos	**24.703**	77.791

INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN DE FICHEROS SEGÚN SU FINALIDAD	2010	Total	% sobre total
Gestión de clientes, contable, fiscal y administrativa	**288.742**	1.316.726	+ 21,93
Recursos humanos	**120.389**	465.039	+ 25,89
Gestión de nóminas	**72.049**	258.381	+ 27,88
Prevención riesgos laborales	**49.864**	153.468	+ 32,49
Publicidad y prospección comercial	**34.041**	157.199	+ 21,65
Videovigilancia	**31.443**	65.052	+ 48,34
Gestión y control sanitario	**18.772**	99.481	+ 18,87
Historial clínico	**11.987**	66.280	+ 18,09
Comercio electrónico	**10.282**	27.008	+ 38,07
Seguridad y control acceso a edificios	**8.442**	27.817	+ 30,35
Análisis de perfiles	**7.831**	22.888	+ 34,21
Cumplimiento/incumplimiento de obligaciones dinerarias	**5.966**	39.663	+ 15,04
Fines históricos, científicos o estadísticos	**5.831**	77.998	+ 7,48
Educación	**5.507**	28.841	+ 19,09
Actividades asociativas diversas	**5.180**	37.153	+ 13,94
Servicios económico-financieros y seguros	**4.560**	61.227	+ 7,45
Seguridad privada	**3.028**	11.026	+ 27,46
Prestación de servicios de telecomunicaciones	**2.496**	10.317	+ 24,19
Gestión de asociados o miembros de partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro	**2.319**	10.046	+ 23,08
Asistencia social	**1.861**	8.631	+ 21,56
Guías/repertorios de servicios de telecomunicaciones	**988**	3.974	+ 24,86
Investigación epidemiológica y actividades análogas	**831**	7.798	+ 10,66
Prestación de servicios de solvencia patrimonial y crédito	**750**	6.756	+ 11,10
Prestación de servicios de certificación	**258**	1.819	+ 14,18
Otras finalidades	**88.103**	301.823	+ 29,19

INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN DE FICHEROS SEGÚN EL SECTOR DE ACTIVIDAD	2010	Total	% sobre total
Comunidades de propietarios	**69.698**	264.805	+ 26,32
Comercio	**62.361**	230.278	+ 27,08
Sanidad	**33.436**	161.661	+ 20,68
Turismo y hostelería	**24.523**	81.554	+ 30,07
Construcción	**21.219**	85.283	+ 24,88
Contabilidad, auditoría y asesoría fiscal	**18.407**	113.392	+ 16,23
Transporte	**12.247**	45.209	+ 27,09
Educación	**12.149**	51.066	+ 23,79
Industria química y farmacéutica	**10.732**	53.858	+ 19,93
Actividades inmobiliarias	**10.616**	76.244	+ 13,92
Actividades jurídicas, notarios y registradores	**9.341**	56.170	+ 16,63
Asociaciones y clubes	**9.123**	49.519	+ 18,42
Actividades relacionadas con los productos alimenticios, bebidas y tabacos	**6.357**	28.517	+ 22,29
Servicios informáticos	**5.746**	33.864	+ 16,97
Maquinaria y medios de transporte	**5.165**	33.691	+ 15,33
Actividades diversas de servicios personales	**4.982**	20.561	+ 24,23
Agricultura, ganadería, explotación forestal, caza y pesca	**4.561**	24.282	+ 18,78
Actividades de servicios sociales	**3.626**	18.953	+ 19,13
Producción de bienes de consumo	**3.565**	19.610	+ 18,18
Seguros privados	**3.359**	24.746	+ 13,57
Sector energético	**2.978**	16.698	+ 17,83
Actividades políticas, sindicales y religiosas	**2.623**	7.274	+ 36,06
Comercio y servicios electrónicos	**2.449**	6.458	+ 37,92
Servicios de telecomunicaciones	**2.102**	10.031	+ 20,96
Actividades de organizaciones empresariales, profesionales y patronales	**1.669**	11.133	+ 14,99
Publicidad directa	**1.174**	8.636	+ 13,59
Seguridad	**1.152**	6.185	+ 18,63
Actividades relacionadas con los juegos de azar y apuestas	**1.050**	5.382	+ 19,51
Inspección Técnica de vehículos y otros análisis técnicos	**885**	2.271	+ 38,97
Entidades bancarias y financieras	**786**	12.584	+ 6,25
Investigación y desarrollo (I+D)	**734**	3.337	+ 22,00
Organización de ferias, exhibiciones, congresos y otras actividades relacionadas	**635**	2.582	+ 24,59
Selección de personal	**468**	3.917	+ 11,95
Actividades postales y de correo (operadores postales, empresas prestadoras de servicios postales, transportistas y empresas de actividades auxiliares y complementarias del transporte)	**233**	2.459	+ 9,48
Solvencia patrimonial y crédito	**84**	970	+ 8,66
Mutualidades colaboradoras de los organismos de la Seguridad Social	**41**	834	+ 4,92
Otras actividades	**160.239**	428.035	+ 37,44

INSCRIPCIÓN DE TITULARIDAD PÚBLICA

DISTRIBUCIÓN DE FICHEROS POR TIPO DE ADMINISTRACIÓN	2010	Total
Administración General	**1.334**	5.460
Administración CC.AA.	**2.940**	19.690
Administración Local	**9.130**	58.637
Otras personas jurídico-públicas	**1.093**	24.502
TOTAL	**14.497**	**108.289**

DISTRIBUCIÓN DE FICHEROS DE LA ADMINISTRACIÓN GENERAL

	Ficheros
Presidencia del Gobierno	44
Ministerio de Asuntos Exteriores y de Cooperación	542
Ministerio de Justicia	126
Ministerio de Defensa	460
Ministerio de Economía y Hacienda	435
Ministerio del Interior	218
Ministerio de Fomento	454
Ministerio de Educación	116
Ministerio de Trabajo e Inmigración	1.291
Ministerio de la Presidencia	77
Ministerio de Política Territorial y Administración Pública	306
Ministerio de Sanidad y Política Social e Igualdad	513
Ministerio de Medio Ambiente y Medio Rural y Marino	343
Ministerio de Industria, Turismo y Comercio	255
Ministerio de Cultura	105
Ministerio de Ciencia e Innovación	175
TOTAL	**5.460**

DISTRIBUCIÓN DE FICHEROS DE COMUNIDADES AUTÓNOMAS

	2010	Ficheros
Comunidad Autónoma de Andalucía	**283**	1.853
Comunidad Autónoma de Aragón	**32**	316
Comunidad Autónoma del Principado de Asturias	**38**	332
Comunidad Autónoma de Canarias	**40**	468
Comunidad Autónoma de Cantabria	**33**	187
Comunidad Autónoma de Castilla y León	**44**	779
Comunidad Autónoma de Castilla-La Mancha	**74**	616
Comunidad Autónoma de Cataluña	**265**	1.050
Comunidad de Madrid	**1.714**	10.222
Comunidad Valenciana	**126**	707
Comunidad Autónoma de Extremadura	**18**	373
Comunidad Autónoma de Galicia	**19**	457
Comunidad Autónoma de las Illes Balears	**90**	461
Comunidad Foral de Navarra	**9**	148
Comunidad Autónoma del País Vasco	**55**	939
Comunidad Autónoma de La Rioja	**55**	327
Comunidad Autónoma de la Región de Murcia	**44**	362
Ciudad Autónoma de Ceuta	**-**	23
Ciudad Autónoma de Melilla	**1**	70
TOTAL	**2.940**	**19.690**

DISTRIBUCIÓN DE FICHEROS DE LA ADMINISTRACIÓN LOCAL

	Entidades	Ficheros
Comunidad Autónoma de Andalucía	**744**	8.202
Almería	104	1.178
Cádiz	45	772
Córdoba	77	738
Granada	173	1.468
Huelva	86	1.183
Jaén	86	574
Málaga	63	827
Sevilla	110	1.462
Comunidad Autónoma de Aragón	**521**	**4.444**
Huesca	186	1.593
Teruel	63	336
Zaragoza	272	2.515
Comunidad Autónoma del Principado de Asturias	**71**	**825**
Comunidad Autónoma de Canarias	**95**	**1.386**
Las Palmas	40	589
Santa Cruz de Tenerife	55	797
Comunidad Autónoma de Cantabria	**55**	**566**
Comunidad Autónoma de Castilla y León	**643**	**3.764**
Ávila	82	919
Burgos	101	382
León	202	1.203
Palencia	23	187
Salamanca	83	360
Segovia	18	105
Soria	10	37
Valladolid	85	390
Zamora	39	181

	Entidades	Ficheros
Comunidad Autónoma de Castilla-La Mancha	**430**	**6.139**
Albacete	97	3.471
Ciudad Real	111	737
Cuenca	87	750
Guadalajara	19	138
Toledo	116	1.043
Comunidad Autónoma de Cataluña	**825**	**8.014**
Barcelona	399	4.197
Girona	168	1.826
Lleida	150	1.123
Tarragona	111	868
Comunidad de Madrid	**209**	**2.734**
Comunidad Valenciana	**442**	**5.150**
Alicante	144	1.726
Castellón de la Plana	94	746
Valencia	205	2.678
Comunidad Autónoma de Extremadura	**213**	**1.925**
Badajoz	162	1.586
Cáceres	51	339
Comunidad Autónoma de Galicia	**300**	**2.590**
A Coruña	95	839
Lugo	63	488
Ourense	77	690
Pontevedra	65	573
Comunidad Autónoma de las Illes Balears	**79**	**1.288**
Comunidad Foral de Navarra	**131**	**1.193**
Comunidad Autónoma del País Vasco	**265**	**4.340**
Álava	50	392
Guipúzcoa	99	1.738
Vizcaya	117	2.210
Comunidad Autónoma de la Rioja	**37**	**264**
Comunidad Autónoma de la Región de Murcia	**46**	**885**

DISTRIBUCIÓN DE FICHEROS DE OTRAS PERSONAS JURÍDICO-PÚBLICAS

	Total
Cámaras Oficiales de Comercio e Industria	414
Notariado	7.699
Universidades	993
Colegios Profesionales	1.931
Otros	13.465
TOTAL	**24.502**

INSCRIPCIÓN DE TITULARIDAD PÚBLICA

DISTRIBUCIÓN DE FICHEROS SEGÚN TIPOS DE DATOS	2010	Total
Datos especialmente protegidos (ideología, creencias, religión y afiliación sindical)	**774**	17.882
Otros datos especialmente protegidos (origen racial, salud y vida sexual)	**3.677**	29.723
Datos relativos a infracciones	**1.412**	20.119
Datos de carácter identificativo	**14.497**	108.289
Datos de características personales	**6.409**	58.099
Datos de circunstancias sociales	**4.202**	31.035
Datos académicos y profesionales	**4.106**	33.977
Detalles de empleo y carrera administrativa	**3.672**	37.268
Datos de información comercial	**2.235**	14.105
Datos económico-financieros	**5.607**	50.054
Datos de transacciones	**1.408**	20.796
Otros tipos de datos	**2.035**	16.951

INSCRIPCIÓN DE TITULARIDAD PÚBLICA

DISTRIBUCIÓN DE FICHEROS CON DATOS SENSIBLES	2010	Total
Datos especialmente protegidos	**774**	**17.882**
Ideología	294	8.915
Creencias	74	8.347
Religión	148	8.486
Afiliación Sindical	445	16.995
Otros datos especialmente protegidos	**3.677**	**29.723**
Origen Racial	441	10.668
Salud	3.642	29.589
Vida Sexual	434	9.337
Datos relativos a infracciones	**1.412**	**20.119**
Infracciones Penales	486	14.994
Infracciones Administrativas	1.291	19.497

INSCRIPCIÓN DE TITULARIDAD PÚBLICA

DISTRIBUCIÓN DE FICHEROS SEGÚN SU FINALIDAD	2010	Total	% sobre total
Procedimiento administrativo	**4.562**	34.315	+ 13,29
Recursos humanos	**1.763**	20.099	+ 8,77
Gestión contable, fiscal y administrativa	**1.607**	16.942	+ 9,49
Educación y cultura	**1.454**	10.017	+ 14,52
Fines científicos, históricos o estadísticos	**1.358**	19.005	+ 7,15
Gestión y control sanitario	**1.174**	4.685	+ 25,06
Historial clínico	**1.095**	2.976	+ 36,79
Servicios sociales	**1.088**	8.089	+ 13,45
Función estadística pública	**848**	12.189	+ 6,96
Gestión de nómina	**762**	10.566	+ 7,21
Investigación epidemiológica y actividades análogas	**677**	2.404	+ 28,16
Videovigilancia	**667**	1.095	+ 60,91
Seguridad y control de acceso a edificios	**643**	2.802	+ 22,95
Seguridad pública y defensa	**561**	3.652	+ 15,36
Hacienda pública y gestión de administraciones tributarias	**554**	9.258	+ 5,98
Trabajo y gestión de empleo	**482**	5.041	+ 9,56
Prevención de riesgos laborales	**443**	1.680	+ 26,37
Gestión económica-financiera pública	**443**	6.263	+ 7,07
Gestión sancionadora	**422**	4.364	+ 9,67
Padrón de habitantes	**337**	5.741	+ 5,87
Justicia	**302**	10.357	+ 2,92
Publicaciones	**198**	1.550	+ 12,77
Actuaciones de fuerzas y cuerpos de seguridad con fines policiales	**171**	2.639	+ 6,48
Gestión del censo poblacional	**161**	457	+ 35,23
Prestación de servicios de certificación electrónica	**156**	1.442	+ 10,82
Otras finalidades	**4.280**	21.523	+ 19,89

TRANSFERENCIAS INTERNACIONALES DE DATOS

Resoluciones de autorización

	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	Total Auto.
Estados Unidos	1	9	2	6	40	9	16	10	31	28	**25**	**177**
Latinoamérica												**220**
Brasil	-	-	-	-	-	-	-	1	3	-	**1**	**5**
Colombia	-	-	-	-	-	1	4	9	4	12	**22**	**52**
Costa Rica	-	-	-	-	-	-	-	1	1	-	**1**	**3**
Chile	-	-	-	-	-	1	7	9	1	8	**9**	**35**
Ecuador	-	-	-	-	-	-	-	-	-	-	**1**	**1**
Guatemala	-	-	-	-	-	-	1	-	1	1		**3**
México	-	-	-	-	-	-	-		3	8	**20**	**31**
Nicaragua	-	-	-	-	-	-	-	1		-	**-**	**1**
Panamá	-	-	-	-	-	2	-	-	-	-	**-**	**2**
Paraguay	-	-	-	-	-	-	1	1	4	4	**1**	**11**
Perú	-	-	-	-	-	-	4	5	4	19	**20**	**52**
El Salvador	-	-	-	-	-	-	-	1	-	-	**-**	**1**
Uruguay	-	-	-	-	-	1	1	1	4	3	**13**	**23**
India					4	-	3	2	30	28	**14**	**81**
Otros países												**110**
Andorra											**1**	**1**
Australia	-	-	-	-	-	-	-	1	-	7	**-**	**8**
Barbados	-	-	-	-	-	-	-	-	-	-	**3**	**3**
Bermudas	-	-	-	-	-	-	-	-	-	-	**1**	**1**
Canadá	-	-	-	-	-	-	-	1	-	-	**-**	**1**
China	-	-	-	-	-	-	1	1	3	3	**1**	**9**
Egipto	-	-	-	-	-	-	-	1	-	-	**-**	**1**
Filipinas	-	-	-	-	-	-	3	1	5	4	**3**	**16**
Hong Kong	-	-	-	-	-	-	1	-	-	1	**1**	**3**
[1] Internacional											**3**	**3**
Israel	-	-	-	-	-	-	-	-	-	1	**6**	**7**
Japón	-	-	-	-	-	1	-	1	-	1	**1**	**4**
Malasia	-	-	-	-	-	1	1	1	-	3	**-**	**6**
Marruecos	1	-	-	-	2	2	2	1	3	8	**7**	**26**
Mónaco	-	-	-	-	-	-	-	-	-	1	**-**	**1**
Nigeria	-	-	-	-	-	-	-	1	-	-	**-**	**1**
Rep. Bielorrusa	-	-	-	-	-	-	-	-	3	-	**-**	**3**
Singapur	-	-	-	-	1	-	1	2	-	-	**1**	**5**
Sudáfrica	-	-	-	-	-	-	-	-	3	-	**-**	**3**
Tailandia	-	-	-	-	-	1	-	1	-	-	**-**	**2**
Túnez	-	-	-	-	-	-	-	1	-	-	**2**	**3**
Vietnam	-	-	-	-	-	-	-	-	-	-	**3**	**3**
Solicitudes presentadas	2	9	2	19	56	45	54	127	137	166	**197**	**814**
Archivadas	-	-	-	13	6	16	17	68	42	24	**31**	**217**
TOTAL AUTO.	**2**	**9**	**2**	**6**	**47**	**19**	**46**	**43**	**103**	**128**	**155**	**560**

[1] En 2010 se autorizó una transferencia internacional solicitada por un grupo multinacional con destino a 104 filiales que actúan en el flujo de datos como encargados del tratamiento y que firman un documento estándar basado en la Decisión 2002/16/CE. La finalidad de la transferencia es la prestación de servicios centralizados en apoyo de los procesos de negocio del exportador de datos.

FICHEROS DE VIDEOVIGILANCIA

AÑO DE INSCRIPCIÓN	Titularidad Privada	Titularidad Pública	Total
1994-2006	1.000	17	1.017
2007	4.760	89	4.849
2008	9.136	180	9.316
2009	21.834	282	22.116
2010	32.134	791	32.925
TOTAL	**68.864**	**1.359**	**70.223**

FICHEROS DE VIDEOVIGILANCIA DE TITULARIDAD PRIVADA

ACTIVIDAD PRINCIPAL	2009	2010	% variación
Comercio	7.325	**15.181**	+ 107,25
Turismo y hostelería	4.749	**8.536**	+ 79,74
Comunidades de propietarios	2.712	**5.277**	+ 94,58
Sanidad	2.273	**3.766**	+ 65,68
Construcción	1.022	**1.809**	+ 77,01
Industria química y farmacéutica	1.055	**1.773**	+ 68,06
Actividades relacionadas con los productos alimenticios, bebidas y tabacos	997	**1.675**	+ 68,00
Transporte	799	**1.384**	+ 73,22
Actividades inmobiliarias	693	**1.073**	+ 54,83
Seguridad	698	**987**	+ 41,40
Servicios informáticos	608	**971**	+ 59,70
Educacion	559	**969**	+ 73,35
Maquinaria y medios de transporte	575	**925**	+ 60,87
Sector energético	505	**846**	+ 67,52
Asociaciones y clubes	409	**656**	+ 60,39
Actividades relacionadas con los juegos de azar y apuestas	411	**650**	+ 58,15
Contablidad, auditoría y asesoría fiscal	363	**631**	+ 73,83
Producción de bienes de consumo	366	**624**	+ 70,49
Servicios de telecomunicaciones	357	**548**	+ 53,50
Agricultura, ganadería, explotación forestal, caza, pesca	276	**501**	+ 81,52
Actividades diversas de servicios personales	286	**491**	+ 71,68
Actividades de servicios sociales	309	**436**	+ 41,10
Actividades jurídicas, notarios y registradores	190	**301**	+ 58,42
Comercio y servicios electrónicos	174	**301**	+ 72,99
Entidades bancarias y financieras	226	**269**	+ 19,03
Actividades de organizaciones empresariales, profesionales y patronales	129	**186**	+ 44,19
Seguros privados	122	**181**	+ 48,36
Inspección técnica de vehiculos y otros análisis técnicos	50	**98**	+ 96,00
Actividades políticas, sindicales o religiosas	42	**87**	+ 107,14
Investigación y desarrollo (i+d)	50	**81**	+ 62,00
Organización de ferias, exhibiciones, congresos y otras activ. relac.	55	**78**	+ 41,82
Publicidad directa	49	**73**	+ 48,98
Actividades postales y de correo (oper. postales, serv. post., transport.	30	**50**	+ 66,67
Selección de personal	12	**20**	+ 66,67
Mutualidades colaboradoras de los organismos de la seguridad social	16	**16**	+ 0,00
Solvencia patrimonial y crédito	5	**8**	+ 60,00
Otras actividades	8.516	**17.384**	+ 104,13
TOTAL	**37.035**	**68.864**	**+ 85,94**

5. PRESENCIA INTERNACIONAL DE LA AEPD

COMISIÓN EUROPEA

Sesiones Plenarias GT29 en Bruselas - 5

- 15 y 16 de febrero.
- 10 de mayo.
- 12 y 13 de julio.
- 12 de octubre.
- 7 y 8 de diciembre.

Reuniones de Subgrupos en la Comisión Europea (Bruselas) a las que asiste la AEPD - 18

- Subgrupo de Tecnología (19 de enero, 18 de marzo, 16 de abril, 17 de noviembre).
- Subgrupo Ad Hoc Programa de Trabajo (3 de febrero).
- Subgrupo Datos biométricos (16 de diciembre).
- Cumplimiento y aplicación de la Legislación ("*enforcement*") (4 de febrero, 13 de abril).
- Subgrupo responsable-encargado (25 de marzo, 2 de julio).
- Subgrupo asuntos financieros (28 de mayo, 8 de septiembre).
- Subgrupo datos de viajeros (21 de enero, 4 de noviembre).
- Subgrupo de futuro de la privacidad (9 de junio, 23 de junio, 3 de septiembre, 12 de noviembre).

CONSEJO DE LA UNIÓN EUROPEA - 22

- ACC del Convenio de Schenguen (9 de marzo y 22 de junio, 10 de octubre, 7 de diciembre).
- ACC del Convenio de Europol (9 de marzo y 21 de junio, 11 de octubre, 7 de diciembre).
- ACC Sistema de Información Aduanero (9 de marzo y 22 de junio, 11 de octubre, 8 de diciembre).
- ACC Eurodac (8 de marzo, 12 de octubre, 8 de diciembre).
- Grupo de Trabajo de Policía y Justicia (10 de marzo, 23 de junio, 12 de octubre, 6 de diciembre).
- EUROJUST (26 de junio).
- Evaluación Schengen (9 y 10 de noviembre).
- Presentación informe Europol (10 y 11 de Noviembre).

CONSEJO DE EUROPA - 2

- Reunión del Boureau del Comité Consultivo del Consejo de Europa. (14-17 de noviembre, Estrasburgo, Francia).
- Plenario del Consejo de Europa. (1-4 de junio, Estrasburgo, Francia).

OCDE - 4

- Grupo de trabajo de privacidad y seguridad (8 de marzo, Paris).
- Grupo de trabajo de privacidad y seguridad (2 de octubre, Paris).
- Conferencia 30 aniversario Directrices de Privacidad de la OECD (22 de octubre, Jerusalén).
- Conferencia "*Economics of Privacy*" (30 de noviembre, Paris).

GRUPOS DE TRABAJO SECTORIALES - 10

Grupo de telecomunicaciones de Berlín: (2)
- 15 y 16 de abril, Granada.
- 6 y 7 de septiembre, Berlín.

Grupo del Taller de Reclamaciones: (2)
- 24 de marzo, Bruselas.
- 20 y 21, Manchester.

Grupo de Trabajo de la Comisión sobre Retención de datos (2)
- 17 de marzo y 14 de julio.

Grupo de Trabajo PD Acuerdo Marco en cooperación policial y judicial
- 2 de febrero.

High Level Contact Group (1)
- 2 de Marzo.

Grupo de Trabajo de la Comisión de Internet de las cosas (2)
- 22 y 23 de septiembre, 19 de noviembre.

RELACIONES BILATERALES

Programas de Hermanamiento (Twinnings)

Israel:

En el año 2008, la Agencia fue adjudicataria, tras competir con diversas Agencias de Protección de Datos Europeas, del primer proyecto de hermanamiento entre la UE y el Estado de Israel (IS-2007-ENPAP-JH-01). El proyecto que ha hermanado a la Agencia con su homóloga Israelí (ILITA) ha estado financiado por la UE con 1 millón de euros y su ejecución se ha realizado durante un periodo de 20 meses entre Junio de 2009 y enero de 2011. Durante el ejercicio de 2010 se han llevado a cabo las siguientes actividades en el marco del proyecto:

- Seminario sobre el registro de ficheros de protección de datos.
- Seminario sobre la gestión de reclamaciones e inspección y la atención al ciudadano.
- Seminario sobre los procedimientos de instrucción penal relativos a protección de datos.
- Seminario sobre la seguridad en protección de datos.
- Visitas de estudios a las agencias de protección de datos del Reino Unido, Italia y Francia.
- Seminario sobre protección de datos en Internet.
- Seminario sobre protección de datos en el sector del Marketing Directo.
- Seminario sobre protección de datos en las Fuerzas y Cuerpos de Seguridad del Estado.
- Seminario sobre protección de datos en la Administración Pública.
- Seminario sobre protección de datos en las transferencias internacionales de datos y en las subcontrataciones de servicios.
- Seminario sobre protección de datos en los servicios públicos de transporte.
- Seminario sobre protección de datos en la educación y los menores.
- Seminario sobre protección de datos en video-vigilancia.
- Seminario sobre la figura del responsable de protección de datos en las organizaciones.
- Seminario sobre protección de datos y transparencia en el acceso a la información pública.

Las actividades anteriores han contado con la participación de expertos de la Agencia española así como de expertos procedentes del sector público y privado de España, Reino Unido, Francia, Italia, Alemania, Holanda, Eslovenia, Noruega, Irlanda, República Checa, Suecia, Portugal, Finlandia. Lituania, Polonia y Chipre.

Croacia:

En junio de 2009 la Agencia Española de Protección de Datos resultó adjudicataria, tras competir con diversas Agencias de Protección de Datos Europeas, de un Proyecto Twinning a desarrollar en Croacia. Este proyecto tiene por objetivo hermanar a la Agencia Española con su homóloga croata (Croatian Agency for Protection of Personal Data, CAPPD) para preparar su ingreso en la UE. Está financiado por la UE con 1.350.000 € y tiene una duración prevista de 22 meses. Su ejecución ha comenzado en Julio de 2010 y, hasta ahora, se han llevado a cabo las siguientes actividades:

- Realización de una Conferencia Internacional (Kick Off) como inauguración del proyecto en la que se ha abordado la situación de la protección en Europa, espacialmente en España y en Croacia.
- Elaboración de un Informe General sobre la totalidad del marco normativo croata, con especial hincapié en su Ley de Protección de Datos, así como la correspondientes proposiciones de modificación para su armonización a las Directivas Europeas.
- Diferentes Seminarios sectoriales relacionados con el campo de la protección de datos a fin de proponer modificaciones a la normativa croata para su adecuación a la normativa comunitaria. Entre otras materias, dichos Seminarios han versado sobre Videovigilancia, Ficheros de Morosos o Acceso de los ciudadanos a la documentación obrante en poder de las Administraciones. Tras la realización de dichos Seminarios han sido elaboradas las correspondientes guías sectoriales.
- Definición y realización de una encuesta entre la población croata para conocer su grado de concienciación en materia de protección de datos.
- Seminario sobre la definición e implantación de un Plan de Comunicación la Agencia Croata de Protección de Datos para el período 2010-2013.
- Seminario para establecer una metodología común para la realización de diferentes guías sectoriales en Croacia.
- Seminario para abordar la problemática del sector del Internet y las Redes Sociales en Europa en general y en España en particular, así como su especial incidencia en los menores de edad. Elaboración de una guía sobre la protección de datos en el sector de las telecomunicaciones en Croacia.
- Realización de diferentes Seminarios dirigidos a la mejora de los sistemas informáticos (IT) y de las medidas de seguridad de la CAPPD. A tal efecto, está previsto que a tiempo de concluir este Proyecto Twinning esté implementada una política de seguridad adecuada a los estándares europeos y a la ISO 27001. Estos Seminarios están dirigidos igualmente a la formación de los funcionarios de la CAPPD y a la propuesta de modificaciones en la normativa croata sobre IT. Dentro de este grupo de actividades se ha realizado una visita a la Agencia Española a la Agencia con el fin de conocer *in-situ* el modelo español en este aspecto.

Las actividades anteriores han contado con la participación de expertos de la Agencia española así como de expertos procedentes del sector público y privado de Alemania, Austria, Italia, Irlanda, Portugal y Checoslovaquia.

IBEROAMÉRICA

Seminarios y Encuentros

- **1 al 4 de junio**: Celebración del **Seminario Regional de Protección de Datos** en el Centro de Formación de la Agencia Española de Cooperación Internacional para el Desarrollo (AECID) en Montevideo (Uruguay).
- **21 al 23 de julio**: Celebración del **Seminario "Nuevas tecnologías: Seguridad vs. Privacidad"** en el Centro de Formación de la AECID en Cartagena de Indias (Colombia).
- **29 y 30 de septiembre**: Celebración del VIII Encuentro Iberoamericano de Protección de Datos (EIPD), Ciudad de México.

Visitas Institucionales

De otras delegaciones a la AEPD:

- **8 de abril**: Visita de una delegación del gobierno colombiano con el fin de presentar el proyecto normativo de "Habeas Data".
- **13 de julio**: Visita de una delegación chilena (Consejo para la Transparencia, Corporación de Fomento de la Producción-CORFO- y Foro Innovación).

De la AEPD a otras instituciones:

- **10 al 12 de noviembre**. Asistencia del Director a la Sexta Versión del Seminario "Jueces y Estado de Derecho", Santiago de Chile.

CONFERENCIAS INTERNACIONALES

- Conferencia Europea de Autoridades de Protección de Datos, 29 y 30 de abril, Praga).
- Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (26 a 30 de Octubre, Jerusalem).

OTRAS

- EURODIG (19 de enero de 2010 y 29 y 30 de abril, Madrid).
- *"A European Index of Convicted Third-Country Nationals (ECRIS-TCN)? Expectations, possibilities, requirements"*. (19 de enero de 2010, Bruselas).
- International Association of Privacy Professionals, 20 y 21 de abril, Washington).
- International Standard Organization -ISO-, (23 y 24 de febrero, Berlín).
- Encuentro Ibérico (10-12 de febrero, Lisboa).
- Reunión del Grupo de Trabajo de Standard - Setting, Banco Mundial (28 al 30 de enero, Méjico DF y 12, 13 de abril, Roma).
- Accountability (9 de marzo Paris, y 24 y 25 de junio, Paris).
- ICANN Studienkreis (22 de enero, Barcelona).
- Global Network of Enforcement Authorities (10 de marzo, Paris).
- Seminario "Seguridad, vida privada y protección de datos" (9 de junio, Madrid).
- International Working Group on Privacy & Security. IWGPS Meeting. (10 de junio, Madrid).
- Conferencia Internet Government Forum (13-16 septiembre, Vilna).
- Med Sourcing Marruecos (7-8 octubre, Casablanca).
- ISO International Privacy Conference, (8-10 de octubre, Berlin).
- Conferencia Public Voice (23 de octubre, Jerusalén).
- Research Conference: "Research and privacy: From Obstruction to construction" (23 de noviembre, Bruselas).
- Journée d'études sur: Le droit à la protection des données privées au Maroc et en Espagne. (23 y 24 de noviembre, Rabat-Agdal).
- Conferencia europea de la International Association of Privacy Professionals (29-30 noviembre, Paris).
- Data Retention Conference (3 diciembre, Bruselas).

6. SECRETARÍA GENERAL

RECURSOS HUMANOS

PERSONAL a 31/12/2010	Dotación	Efectivos
	Funcionarios **157**	Funcionarios **147**
	Laborales **7**	Laborales **7**
	Alto Cargo **1**	Alto Cargo **1**

NIVEL	30	29	28	26	24	22	20	18	17	16	15	14
Efectivos 2010	5	3	21	46	2	14	2	12	2	7	12	21

GRUPO	A1	A2	B	C1	C2
Efectivos 2010	31	47	0	21	48

GRUPO	TOTAL
Hombres	66
Mujeres	89

EVOLUCIÓN DEL PRESUPUESTO DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS DURANTE LOS EJERCICIOS 2007 A 2010

CAPÍTULO	Crédito ejer. 2007 (euros)	Crédito ejer. 2008 (euros)	Crédito ejer. 2009 (euros)	Crédito ejer. 2010 (euros)
I	3.970.471,82	5.292.866,85	6.692.929,00	**6.747.004,93**
II	5.094.745,78	6.189.248,11	6.701.771,00	**6.620.095,07**
III	5.998,51	47.555,34	12.290,00	**127.290,00**
VI	1.471.340,00	1.900.770,00	1.900.770,00	**1.900.770,00**
VIII	10.000,00	10.000,00	10.000,00	**30.000,00**
TOTAL	**10.552.556,11**	**13.440.440,30**	**15.317.760,00**	**15.425.160,00**

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

SPANISH DATA PROTECTION AGENCY: CURRENT SITUATION AND FUTURE PROSPECTS

1. BETTER-INFORMED CITIZENS WHO ARE MORE AWARE OF THEIR RIGHTS

A. THE 'RIGHT TO BE FORGOTTEN' ON THE INTERNET: AN EMERGING DEMAND

The right to be forgotten on the Internet has become one of the most hotly discussed topics in the area of new Internet services. In this context, the public is ever more vehement in calling for the ability to exercise control over their personal data, including the right not to appear on the Net. The increase in the number of enquiries into how to disappear from the Internet and in the exercise of the rights to erase and to object is evidence of the strength of this demand.

Among the enquiries received by the Agency's Help Line regarding how to exercise rights of access, rectification, erasure and objection, those relating to the rights of erasure and objection -which constitute the two means of exercising the right to be forgotten- account for 66.15% of the total. In particular, enquiries regarding the right to objection have increased several fold, from 8.66% of the total in 2009 to 25.51% in 2010.

As regards the exercise of rights vis-à-vis Internet search engines, 98 resolutions were issued regarding the protection of these rights (87% associated with Google and the rest with Yahoo!, Lycos, Altavista, Bing and Terra), upholding the citizens' claims in 75.5% of the cases. These complaints have their origin in the publication of personal data in official gazettes and journals, digital media, judicial decisions and other websites.

The Spanish Data Protection Agency (AEPD) has responded to the public's complaints relating to services rendered by multinationals by taking the view that to offer such services these companies make use of equipment in Spanish territory and specifically target users living in Spain. Appeals against some of the resolutions have been brought before the *Audiencia Nacional* (Spanish central court), though no decisions have yet been announced. The 'right to be forgotten' has also been added to the agenda of the European Commission, which has stressed the need to examine the means of clarifying 'the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes'.

.

B. INFORM THE CITIZENS: PROMOTE THEIR RIGHTS

Media have established as the most effective means of informing the public about the protection of their data. That requires the Agency to play an active role in answering requests for information and in having a direct presence in the media. These new demands have led to 67 press releases and notifications being written for publication in the media, along with 65 informative notes for the Agency's website and around 700 interviews and requests for information from the media.

Among the main issues which have attracted the media's attention are the right to be forgotten on the Internet, privacy on social networking sites (especially the risks to minors) and the collection of data from open Wi-Fi networks by Google's Street View service. Other prominent issues have been video surveillance, commercial communications and data processing in credit histories.

The growing coverage on data protection in the media has led to an increase in the number of enquiries received by the Agency's Help Line, which have grown by 8.2% to exceed 100,000 (104,826), establishing the telephone as the principal channel for contacting the Agency. The highest growth has been in enquiries about the possibility of removing personal information from the Internet, especially in connection with the results of Google searches.

Video surveillance is settled as one of the citizens' most frequent concerns, principally focused on the installation of cameras in residential buildings, hallways and garages. Enquiries about credit histories have also increased several fold, reflecting the rise in the number of questions relating to the collection of debts by third parties other than the creditor, such as law firms or companies specialising in debt collection.

As far as personal data processing is concerned, minors are one of the most sensitive groups, both because of the risks to which they are exposed and because of the lack of information about how to tackle them. For this reason, the AEPD has stepped up the offer of information aimed at the protection of minors, creating a specific section on its website with up-to-date informative content, which includes practical guides, recommendations, videos, reports and links to other useful pages.

2. ENSURING COMPLIANCE WITH THE LAW

A. A BID TO FACILITATE COMPLIANCE WITH SPANISH DATA PROTECTION LAW

In order to make it easier for data controllers and processors to comply with the Organic Law on the Protection of Personal Data (LOPD, after the Spanish) and its implementing Regulation, a self-assessment tool, EVALÚA, was added to the Agency's website. It allows the user to check compliance with the law, assess the security measures laid down in the Regulation, and obtain a report detailing any deficiencies detected, so that, if necessary, the relevant corrective measures can be taken. By the end of 2010, EVALÚA had been accessed 20,294 times.

The Agency has continued with its policy of informing experts and individuals involved in the implementation of the LOPD by holding the 3rd Open Annual Session of the AEPD, which was attended by over 800 people, and it has expanded the catalogue of informative guides about the LOPD with the publication of the 'Guide to RFID Technology Security and Privacy', in collaboration with the National Communications Technology Institute (INTECO), and by re-editing the 'Guide to Security'. This includes a model 'Security Document', which serves as a guide and facilitates implementation of the rules on data protection and compliance with them.

Furthermore, in the sphere of the judicial system, the General Judicial Council (Consejo General del Poder Judicial) and the AEPD signed a collaboration agreement which establishes a protocol for carrying out inspections regarding data protection in judicial bodies, as well as implementing initiatives which promote the effective application of the rules on data protection in the judicial system as a whole.

As regards more complex enquiries aimed at facilitating the application of the LOPD by controllers in both the public and private sectors, a total of 527 were dealt with, of which 298 (57%) were from public authorities and 229 (43%) from the private sector. This represents a reduction in the number of enquiries made in relation to previous years. This could be due to a mitigation of the effect caused by the passing of the Regulation implementing the LOPD, which caused the number of enquiries to increase substantially in the years following its entry into force in 2008. Likewise, it can be seen how there has been a return to the usual pattern of similar numbers of enquiries from the public and private sectors, with a slight preponderance of those from the public sector (57% of the total this year).

As regards the matters covered by these enquiries, the following, among others, particularly stand out: The very notable rise (117%) in the number of enquiries related to defining the concepts of publicly and privately owned files; the rise in the number of questions related to exercising rights of rectification and erasure (which practically tripled in 2010); those referring to sensitive data (which have doubled, with those referring to health-related data rising by 56%); as well as enquiries regarding compliance with the principles of data quality, which have risen by 90%; and the maintenance of a significant number of questions addressing security measures and the scope of the LOPD.

Looking at the distribution by sector of enquiries from the private sector, the main conclusions include the importance assumed this year by enquiries from non-professional associations and foundations, as well as political parties and unions; the continuing importance of enquiries from business and professional associations and from the financial, pharmaceutical and transport sectors; the fall by more that 40% in enquiries from institutions offering advisory and consultancy services, as well as the reduction in the volume of enquiries from the education and telecommunications sectors, and those made by private individuals, which had increased notably in 2009.

As regards specific matters which have been examined and their conclusions, mention should be made of those related to defining the territorial scope of Organic Law 15/1999 and, where appropriate, to the existence or non-existence of international data transfers; likewise, those related to the application of the regulatory rules concerning the security measures which may be required in relation to certain forms of data processing, and compliance with what is laid down in Organic Law 15/1999 on the publication in the media of the unabridged content of court sentences, provided that the requirements stipulated by the Constitutional Court are met, so that the

right to information may be thought to prevail over the rights to honour, to privacy and to freedom from injury to reputation, honour or feeling.

Also worthy of mention are enquiries referring to the requirements for compliance with the duty to inform the individual concerned in circumstances in which the exception to disclosure laid down in article 19 of the implementing Regulation of the LOPD is applicable (merger and segregation operations, transfer of assets or liabilities, or commercial transactions of a similar nature), taking into account the doctrine of the *Audiencia Nacional* (Spanish central court), according to which, if there is a breach of the duty to inform, this will be considered disclosure of data.

The registration of files on the General Data Protection Register (RGPD) is an important indicator for assessing the level of knowledge of and compliance with the LOPD. In 2010, nearly half a million files were registered on the RGPD, an increase of 31% on the number of files registered in 2009. The number of files registered has, with this increase, surpassed the figure of 2 million, closing the year with 2.1 million active files.

To be specific, among the stated aims of the files registered in 2010 are client, accounting, tax and administrative management, along with the management of human resources and payrolls. Advertising and market research also figure as one of the main aims of personal data processing in the private sector. In the sphere of the public sector, the number of files registered on the RGPD reached 108,289 during the course of 2010, with the registration of 14,497 files in total.

B. LEGAL CERTAINTY AS THE PRIME OBJECTIVE

The AEPD has carried on working towards the objective of achieving greater legal certainty by means of binding reports on regulations of a general nature. Reports were issued on 97 regulations, including the Sustainable Economy Bill, the Civil Registry Act, the Consumer Credit and Gambling Regulation Act, as well as draft Royal Decrees, such as that approving prison regulation.

Analysing the degree of legal certainty in the application of the LOPD also requires consideration of the extent to which the resolutions of the AEPD are ratified or revoked by the courts. During the course of 2010, the administrative disputes divisions of the National Court and the Supreme Court issued 230 and 29 rulings respectively. As regards the rulings of the National Court:

- 158 rejected appeals brought against agency resolutions (which were fully upheld). (69%).
- 16 partially upheld appeals (7%).
- 49 (21% compared to 25% the year before) entirely upheld attempts to overturn agency resolutions
- 7 (3%) appeals brought against agency resolutions were not admitted.

It is worthy of mention that in 2010 appeals concerning requests to delete data from the baptism records of the Catholic Church practically disappeared, with two rulings having been issued this year compared to the 99 issued in 2009.

For its part, the Supreme Court issued a total of 29 rulings referring to appeals or appeals for the unification of doctrine, brought against rulings issued in proceedings in which the agency was involved. At the same time, three rulings of 15 July 2010 resolving appeals brought against the implementing regulation of the LOPD are of particular importance, as are two court orders, of the same date, raising matters of a preliminary nature relating to article 10.2 b) of the same regulation. With regard to these appeals, the rulings of the High Court broadly uphold the regulation, revoking 5 of its 158 articles, and raise legal certainty in the Spanish data protection system.

Finally, and aside from matters to do with erasing baptism records, the Supreme Court ratified the agency's criteria on 15 of the 23 occasions on which its opinion was sought.

C. A GROWING DEMAND FOR GUARANTEES: AN ACTIVE RESPONSE FROM THE AGENCY

It is notable that not only has the 75% increase in the number of complaints in 2009 over 2008 been consolidated, but there was an additional 4% increase, taking the figure to 4,300. Conversely, the decrease by almost 13% in requests for protection relating to the exercise of rights of access, rectification, erasure and blocking also stands out. The principal reason for this decrease must lie in the practical disappearance of requests for protection in view of the refusal by the Catholic Church to erase baptism records, after the Supreme Court handed down a ruling in September 2009 which found that the LOPD was not applicable to baptism records.

Notable among requests for protection, along with those relating to the Internet (which grew by more than 56% in relation to the year before) are those relating to the right of erasure, alleging wrongful inclusion in files on defaulters (17% of the total).

Telecommunications and video surveillance are the sectors which has raised the greatest number of complaints, with increases of close to 29% and 14%, respectively. Other sectors in which the number of complaints has risen are Internet services, advertising and market research (except spam), security forces and corps, and gas, electricity and water. It should be stressed that the number of complaints referring to the actions of trade unions in the use of personal data (48) has doubled, and along with it, the phenomenon of the social networking sites, with a rising trend of complaints and requests for protection for alleged violations of privacy on social networking sites (40 in 2010 compared to 32 in 2009).

On the other hand, there have been substantial reductions in the commercial communications sector for spam and faxes (by two thirds) and in complaints regarding the use of data in trade, transport, hotels and catering, and education.

The increase of 4% in the number of complaints made in 2010 must be seen in the context of an increase of 8% in the number of sanctioning procedures, with video surveillance standing out as the sector in which the greatest number of rulings involving sanctions have been handed down. In telecommunications, which is still the sector attracting the greatest number of complaints, there have been fewer sanctioning procedures. The explanation is to be found in errors frequently made by complainants concerning the competence of the AEPD, by referring to matters such as invoicing or consumption, deficiencies in service provision, interpreting clauses of contracts and sending premium-rate messages.

The reasons for the increase of 13.16% in rulings that there is no case to answer and complaints not admitted are to be found in the following:

- The LOPD not being applicable on grounds of being outside its territorial scope.
- Dealing with a case of debt transfer for a penalty has already been handed down.
- The LOPD not being applicable on grounds that the complainant or person affected is a corporation.
- Processing of data relating to deceased persons not protected by the LOPD.
- Lack of minimum evidence for opening an investigation which would invert the principle of *in dubio pro reo*.
- Prevalence of the right to freedom of expression in the media.
- Prevalence of the right to effective legal protection as authorisation for the processing of data.
- It being appropriate to seek erasure or rectification beforehand, when it is an option provided for by the system and when no damage has been done.

For their part, rulings attesting to infringements by public authorities have fallen by 14%; notable are those referring to the publication in the press of health-related data, the installation of cameras in women's toilets and the publication of data referring to fines paid months earlier in the Official State Gazette (BOE).

An important fact is the year-on-year fall of 30% in the amount of sanctions imposed, which is even more striking in view of the 8% rise in sanctioning procedures. The main reason for this imbalance lies in the prominence of video surveillance as the leading sector in terms of the number of sanctions, in which the infringements are frequently those categorised as minor and the fact that those sanctioned are usually individuals and SMEs and often meet the criteria for mitigation envisaged by the law.

The majority of sanctioning resolutions are still being imposed pursuant to the LOPD (92.5%), but there is a notable increase (27%) in those imposed within the framework of the Information Society Services Act (LSSI), which is the law applicable to infringements by unconsented electronic commercial communications (spam) with no possibility of blocking them. Conversely, there is a substantial fall (80%) in the number of sanctions imposed under the General Telecommunications Act for sending commercial faxes without regulatory approval.

Those sanctions showing the greatest increase are those classified as minor (Δ 62.5%), with those classified as very serious and serious decreasing substantially (∇ 45.5% and ∇ 14%, respectively).

A qualified reduction in the lawbreaker's liability could be observed in 31.64% of all sanctioning resolutions.

The agency's inspection services have also acted - either at the request of one of the parties or on the initiative of the director - to investigate general problems detected in different areas, such as the disclosure of data to companies (by means of sector inspections concerning the sale of debt by telecommunications companies and financial institutions and the analysis of clauses of contracts for debt recovery in telecommunications companies) auditing the Schengen Information System in Spain, analysing clauses of telecommunications company contracts, investigating the legality of large databases, and investigating the access criterion based on 'legitimate interest'.

3. CHALLENGES FOR PRIVACY: THE MAJOR ISSUES

A. INTERNET: A STEP FORWARD IN USER PROTECTION

Internet service providers affect users' privacy by means of the unilateral setting of terms and conditions and privacy policies, which have an impact on the information that users receive -deficient as regards clarity and accessibility-, the purposes of the processing of their data and the relevant retention periods. In turn, the business model itself that supports these services also has an impact on privacy, on account of the fact that they are generally services provided for free which are financed by advertising income. This has led to ever more sophisticated strategies for tracking users' behaviours, profiling them and personalising advertising.

In this area, the AEPD has had periodic meetings with the main Internet service providers to exchange information and suggestions which increase user guarantees. But this policy cannot prevent an appropriate reaction when privacy boundaries are crossed, or citizens demand the rights and guarantees granted by law.

In this respect, in April 2010, the AEPD, along with nine authorities from various different regions, addressed a joint letter to Google Inc. expressing their concern at the lack of attention paid to data protection in the deployment of new applications, in particular the problems raised by the social networking service Google Buzz.

The authorities' reaction reflects the fact that it was not an isolated case and seeks the incorporation of fundamental privacy principles into the design of new online services. And it represents a precedent regarding the need for the data protection and privacy commissioners to adopt co-ordinated initiatives when dealing with global services. With this and other examples, the Agency, working together with other authorities, has thus made a commitment to taking a step forward in the protection of Internet users.

This step forward has also led to the investigation of alleged legal breaches. In October 2010, the AEPD began a sanctioning procedure against Google Inc. and Google Spain for collecting and storing information about the location of Wi-Fi networks and payload data via the vehicles used for the Street View service. Inspections on Facebook were also begun in October, requesting information about whether users in Spain have been affected by the disclosure of data to advertisers or other companies by any of the most popular applications on Facebook. And in November similar actions were begun regarding MySpace.

These latest actions are indicative of the importance of obtaining personal data for carrying out Internet advertising, which is the usual financing model for free services on the Net. This fact makes it necessary to update users' guarantees. The amendment in 2009 of Directive 2002/58/EC, concerning privacy in electronic communications, broached this issue, and, in June, the Article 29 Working Party (WP29) adopted an opinion on online behavioural advertising which examines comprehensively the guarantees offered both by this directive and the directive that regulates the protection of personal data (Directive 95/46/EC).

The debate which took place addresses the following questions: Is it enough that users know that tracking cookies are used and are able to deactivate them (opt-out system)? Or is it necessary for them to be informed and consent to their browsing being tracked (opt-in system)? In the opinion of the European data protection authorities, in accordance with the modified directive, the opt-out system is insufficient and users' informed consent should be required before installing devices such as cookies. Information about the purpose of tracking must be clear and comprehensible, so that users can make a decision about whether or not they want their browsing behaviour to be monitored, and it must be possible for them to withdraw their consent.

Furthermore, the AEPD has continued to have contact with key figures in charge of social networking sites such as Tuenti and Facebook, to improve their privacy policies and prevent minors under the age of 14 from gaining access to such networks.

In this context, Tuenti has set the minimum age required to sign up at 14; it has improved its protocol for identifying and deleting users under the age of 14 and maintains the highest level of privacy by default for users under the age of 18. In response to the AEPD's request, Facebook announced that it would increase the minimum age for registering on its social networking site from Spain to 14, bringing it into line with the current data protection regulations; it also stated its commitment to developing stronger guarantees, including examining options for introducing an age verification system to prevent access from minors and checking that they have parental consent.

B. ARE YOUR MEDICAL RECORDS SECURED?

In view of the importance of health data, the AEPD adopted the initiative of drawing up a 'Report on compliance with the LOPD in hospitals', given the discovery of alarming cases of infringements of the LOPD, principally linked to breaches of the duties of security and secrecy provided for under the LOPD. The assessment was carried out by sending a questionnaire to more than 600 centres included in the national register of hospitals, which was answered by 92% of them.

The report's first conclusion is that, in general terms, there are strong signs of compliance with the LOPD in private health centres, while there are greater deficiencies and lower levels of compliance in public centres. The obligation to notify files to the General Data Protection Register shows high levels of compliance in centres of both types (99% in private and 89% in public centres). Providing the public with information about the processing of their data by means of forms and informative posters is standard practice in private centres (94.5% and 80%, respectively) and a significant deficiency of public centres (55% and 64%).

With regard to security, the report reveals that there is a significant difference between formal compliance with security measures and their implementation in practice. Deficiencies can be observed in the way that they are applied, such as the absence of mechanisms which make it difficult to access devices where medical records are stored in nearly 10% of private centres and 35% of public ones; inadequate measures for avoiding loss, alteration, unauthorized disclosure or access of medical documents during transport in 15% of private centres and 30% of public ones; and breaches of the requirement to have access logs, that allow to track who has accessed a medical record and what data they have accessed, in nearly 15% of private centres and 62.6% of public ones.

Furthermore, procedures which allow the rights of access, rectification, erasure and blocking to be exercised have been introduced in 96% of private centres and 84% of public ones. However, this fact has not prevented that complaints to the Agency for the protection of the right to access medical records increased significantly. The Agency has issued 95 resolutions on this matter, which account for 40% of all resolutions on the right of access. Of these, nearly 78% uphold the data subjects' claims. The reasons for these complaints principally focus on having been provided with incomplete medical information or having been denied access to the medical record of a deceased relative.

C. THE INTERNET OF THINGS: SECURITY AND PRIVACY WITH RFID TECHNOLOGY

Radio-frequency identification or RFID (which allows an object to be identified automatically due to a built-in electronic tag which transmits its identifying data by radio frequency) presents new risks with regard to both security and privacy.

With the aim of furthering knowledge of such risks, the AEPD, in collaboration with the National Institute of Communication Technologies (INTECO), has drawn up a guide to RFID technology security and privacy. The main risk to privacy consists of unauthorised access to users' personal information. This risk is apparent in threats such as unauthorised access to tags; tracking of individuals and/or their actions and preferences, and the use of the data to analyse individual's behaviour.

With regard to risks related to security, the guide indicates those arising from actions aimed at maliciously damaging, interrupting or taking advantage of the service.

To avoid these, the guide points out the possibility of using tags (watchdog) which give information about attempts to read them; isolating tags, preventing them being read except when desired; using devices which create a safe area around the user, making RFID ineffective, or disabling tags once a transaction has been completed. For providers of this technology, good practice to guarantee privacy is also included, such as clearly notifying users of that RFID is being used, making users aware at all times of when, where and why a tag is going to be read, not storing personal information in the RFID tags, and offering the user facilities for the withdrawal, destruction or deactivation of tags associated with products when they are going to leave the premises.

D. INTERNATIONAL DATA FLOWS: FLEXIBILITY AND GLOBALISATION

In 2010, transfer authorisation requests increased by 18.6%. The main destinations for exporting data were Latin America, which represents 34.5% of the total with 88 requests, the United States, with 25, and Asia, with 23.

The Latin American countries are consolidated as the main destination for international data transfers from Spain, with a total 220 authorisations; these are in addition to the even greater number (377) made to Argentina, a country for which, being classified as having an adequate level of protection by the European Commission, authorisation is not necessary, with notification of the General Data Protection Register being sufficient.

Colombia, Chile, Mexico, Peru and Uruguay, countries which have passed specific laws on the protection of personal data, or are in the process of doing so, play an important role. International data transfers to the United States remain stable. And those destined for Asian countries are practically on a par with them, with those made to India being of particular note.

The main characteristic of all international data transfers lies in the fact that the vast majority (90%) is to do with the provision of services which are outsourced to third countries, confirming once again the offshoring of data-processing activities to third countries.

4. UPDATING THE DATA-PROTECTION REGULATORY FRAMEWORK: A SHARED NEED

The changes triggered by the new information technologies, the varying role of the public with the Web 2.0 as well as their active participation in the processing of information and the globalisation of services, has led to regulators all of over the world to lead the discussion on the need to update the different existing legal instruments for privacy and data protection, particularly at international level. For this reason, there are currently various review processes in progress, in which the AEPD is very actively involved.

A. INTERNATIONAL STANDARDS FOR THE PROTECTION OF PRIVACY IN RELATION TO THE PROCESSING OF PERSONAL DATA

One of the AEPD's priorities in 2010 was to promote and spread this text among private institutions, experts and national and international public bodies. In that spirit, the Agency has addressed several international organisations to disseminate the standards and propose them as a basis for future regulatory developments, and it made contact with multinationals and civil society to demonstrate its applicability in practice. The Spanish Congress and the Senate also approved separate initiatives, both were recognising the proposed standards as a suitable basis for moving towards a binding international instrument. The Mexican Data Protection Act, passed in July 2010, makes specific mention of the standards as a basis for their regulation.

B. PRIVACY AND CROSS-BORDER DATA-FLOW DIRECTIVES FROM THE ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD)

In the aim to culminate with the review of its Privacy Guidelines and coinciding with the 30th anniversary of this instrument, the OECD has organised a series of events as they work on a report about the evolution of privacy since 1980 which will lay the foundations, along with the conclusions of the aforementioned events, for the review of the Guidelines, which will take place over the next year.

C. RESOLUTION ON DATA AND PRIVACY PROTECTION IN THE THIRD MILLENNIUM

The Committee of Ministers of the Council of Europe approved a '*Resolution on the Protection of Data and Privacy in the Third Millennium*', in which the Council of Europe supports the modernisation of Convention 108, taking into account relevant international developments and with the participation of other states and organisations. Specific mention is made of the Madrid Resolution in the explanatory memorandum. The AEPD will be involved in drawing up the drafts of the reports.

D. NEW HORIZONS FOR PERSONAL DATA PROTECTION IN THE UNITED STATES

In December 2010, the Federal Trade Commission (FTC) approved a document which proposes a new legal framework for processing consumer data. In particular, it sets out a number of actions as the establishing of the principle of *privacy by design* and the adoption of the '*Do Not Track*' system, which involve giving users the ability to choose in the different forms of processing, particularly all related to the online environment. Likewise, it suggests measures which companies should take into account in order to encourage transparency. The FTC will deliver its final report in 2011.

E. THE EUROPEAN DATA PROTECTION DIRECTIVE

On 4 November 2010, the European Commission published a communication under the heading '*A comprehensive approach to personal data protection in the European Union*', which identifies the priorities and outlines the key points of the future European data protection legal framework. In this communication, the Commission reaffirms the validity of the core principles of the current legal regime, by insisting on the need for adjustments aiming to update, clarify, strengthen and making for greater consistency to the system.

The Commission stresses its concern for achieving a greater degree of harmonisation of national data protection regulations; its wish to see the responsibles for data processing taking on greater responsibility; its interest in reducing administrative burden, and also its intention to develop an effective penalty system. It also tackles how to improve the citizen's control over their own data, by means of greater transparency with regard to data processing, clearer and more effective rules related to consent and activities helping raise public awareness. The communication also deals with other issues such as the simplification and clarification of the regulations relating to international transfers and a better definition of what constitutes sensitive data. The Commission will present its proposal for new European legislation in 2011.

5. EUROPEAN DATA PROTECTION AUTHORITIES IN THE LIGHT OF THE NEW CHALLENGES

The Article 29 Working Party (WP 29) - of which the AEPD took on the deputy chair in February 2010 - has been involved in the whole process of revising Directive 95/46/EC, for which reason, over 2010, it has approved various opinions which interpret it and which complement the document on the future of privacy which was adopted in 2009.

A. OPINION 8/2010 ON APPLICABLE LAW (WP 179)

This opinion clarifies the content of article 4 of the Directive, concerning to the scope. It refers to set of criteria which might be applied when the data controller is established outside the European Union, with the aim of ensuring that there is a sufficient legal connection with European Union territory and preventing unlawful processing.

B. OPINION 3/2010 ON THE ACCOUNTABILITY PRINCIPLE (WP 173)

The opinion proposes introducing this principle for those responsible for data processing, referring to of the responsibility for applying appropriate and effective measures which guarantee the principles and obligations laid down by the Directive. Likewise, it implies the ability to demonstrate this when requested by the supervisory authorities.

C. OPINION 1/2010 ON THE CONCEPTS OF 'CONTROLLER' AND 'PROCESSOR' (WP169)

These concepts play a fundamental role in the application of Directive 95/46/EC, since they determine who the individuals responsible for compliance with data protection rules are, how those involved can exercise their rights, what the applicable national legislation is and how effectively data protection authorities can operate.

D. REPORT 1/2010 ON THE SECOND JOINT ENFORCEMENT ACTION: COMPLIANCE AT NATIONAL LEVEL OF TELECOM PROVIDERS AND ISPS WITH THE OBLIGATIONS REQUIRED FROM NATIONAL DATA RETENTION LEGISLATION (WP 172)

The document involves, on the one hand, a practical exercise aimed at analysing data processing by telecommunications and internet service providers and, on the other hand, giving a message to the Commission, which in 2010 worked on a report assessing the Data Retention Directive, drawn up jointly by the offices of the three commissioners.

E. ACTIONS IN THE AREA OF POLICE AND JUDICIAL CO-OPERATION

The AEPD has actively participated in the main developments relating to data protection in the law enforcement area. Three developments have focused their attention on this area during the course of 2010:

- **TFTP II Agreement (SWIFT: transfer of financial data)**. Its main goal is to allow the transfer of data related financial transactions from the EU to the United States in order to prevent and fight terrorism. Both WP29 and the Working Party on Police and Justice have expressed concern because certain cases have been identified in which the level of protection would not be sufficient; they have also pointed out deficiencies related to the possibility of carrying out transfers of bulk data, and at the same time insist on the need to avoid data transfers from the Single European Payments Area.

- **Framework decision on the protection of data in the area of police and judicial co-operation**. It has grown from the belief of offering a high level of protection in the processing of personal data in the framework of police and judicial co-operation in criminal matters, in turn ensuring a high level of public security. One aspect which was particularly controversial was the definition of the scope of the regulation, which finally left domestic processing outside its protection; this could imply, in some cases, that data transferred from another country could enjoy a greater level of protection than data processed nationally.

- **Registration of passengers' data**. Work has been done which culminated in the proposal for a directive on the use of passenger name records' data for the prevention, detection, investigation and prosecution of terrorist crimes and other serious offences, which was published in February 2011. The proposal will need to receive the approval of the Council and the European Parliament to become a reality. As regards PNR agreements with third countries, the European Commission simultaneously began negotiation processes with Australia, Canada and the United States.

F. ADVANCES IN OTHER INTERNATIONAL FORUMS

On 23 November 2010, the Committee of Ministers of the Council of Europe approved a Recommendation on the protection of individuals with regard to automatic processing of personal data in the framework of profiling, a document of particular importance in sectors such as the financial and advertising sectors. Furthermore, and as a result of the 42nd meeting of the Berlin Working Group on Data Protection in Telecommunications, organised by the AEPD in Granada on 15 and 16 April, the 'Granada charter on privacy rights in the digital world' was passed, which involves the approval of a number of basic privacy rights in the digital environment.

G. THE IBEROAMERICAN DATA PROTECTION NETWORK: DEFINITIVE CONSOLIDATION

The year 2010 must be thought of as a milestone in the framework of the Latin American Data Protection Network on account of the regulatory advances which took place in Latin American countries with regard to data protection, toolking their inspiration from both the European regulations and the international standards of the Madrid Resolution.

The network has continued to undertake initiatives to promote the protection of personal data. In June, a regional seminar was held in Montevideo; in July, the seminar 'New Technologies: Security vs. Privacy' took place in en Cartagena de Indias (Colombia) with the participation of 15 countries; and in September, the 8th Latin American Data Protection Conference was held in Mexico City, which passed the Mexico Declaration. The international status of the Iberoamerican Data Protection Network has resulted in the designation of the Mexican Federal Dta Protection Authority (IFAI), which currently chairs the network, as organiser of the 33rd International Conference of Privacy and Data Protection Authorities, which will take place in 2011.

6. CO-OPERATION WITH REGIONAL DATA PROTECTION AGENCIES

Notable in this context are the improvement in exchanges of information between the records of the respective agencies, the RENO (Notifications Registry) system being in a development phase, the policy of promoting the information of minors and teenagers, and the exchange of information about the working party which is analysing the concept of 'accountability'. They have also taken part in the Seminars on Information Technologies for the Modernisation of Public Authorities (TECNIMAP 2010), allowing them to have an important institutional presence.

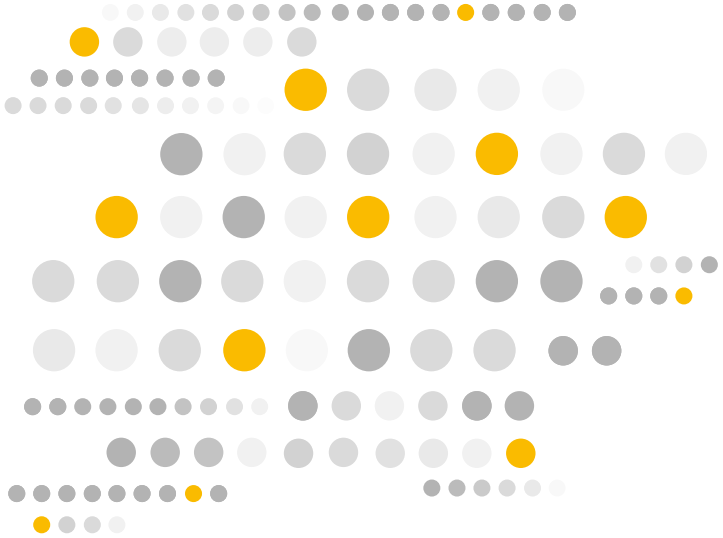
7. RECOMMENDATIONS

REGULATIONS

Review of the notification procedures for administrative resolutions provided for in Law 30/1992, of 26 November, with the aim of including notification procedures which facilitate reconciling the obligation to identify the addressee with the safeguarding of their privacy.

EXECUTIVE

Creation of a data protection controller: the figure of a person or department responsible for co-ordinating tasks related to compliance in matters of privacy and data protection is considered good practice in those companies, corporations or public authorities in which personal data processing is a significant part of their management.



AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

D.L.: M-17848-2011

Diseño Gráfico: www.ardifusion.com
Impresión: Nilo Industria Gráfica, S.A.