AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

MEMORIA AEPD 2011

PRÓLOGO

Es para mí un motivo de especial satisfacción presentar, por vez primera como Director de la Agencia Española de Protección de Datos, la Memoria de esta institución correspondiente al ejercicio 2011.

En el año transcurrido desde que asumí esta nueva responsabilidad, he tenido sobradas ocasiones de constatar la dimensión y la complejidad de los retos a los que hoy en día tienen que hacer frente las instituciones que, como la Agencia Española, tienen encomendada la salvaguarda del derecho fundamental a la protección de datos. Por fortuna, en nuestro país contamos con un nivel de garantía y protección de este derecho que, no sólo está a la altura de los muy exigentes estándares europeos, sino que, si comparamos su eficacia real, se sitúa en muchos aspectos por encima de los países de nuestro entorno, razón por la cual España cuenta actualmente con un notable grado de reconocimiento en las instituciones y los foros internacionales. Ello es en parte merecimiento de quienes me han precedido en el cargo pero, sobre todo, es mérito del excelente equipo de profesionales que diariamente desempeñan sus funciones en la Agencia con una dedicación y un compromiso encomiables.

Con todo, la justificada satisfacción sobre lo alcanzado no debe llevar en modo alguno a desconocer que todavía son necesarios importantes esfuerzos adicionales para lograr una adecuada implantación de la normativa de protección de datos en determinados ámbitos. Y, menos aún, debe conducir a ignorar o infravalorar la magnitud de los retos que la garantía eficaz de este derecho tiene planteados en la sociedad actual como consecuencia de los continuos avances tecnológicos y de los procesos de globalización. A la espera de que la revisión del marco normativo iniciada en la Unión Europea dé sus frutos y proporcione un instrumental actualizado, las Autoridades de Protección de Datos están llamadas a afrontar los nuevos retos con un planteamiento decididamente innovador, reinterpretando los principios y las reglas tradicionales a la luz de las nuevas realidades, con el fin de continuar garantizando a los ciudadanos una protección adecuada de sus derechos.

Como los lectores podrán observar, la estructura de la Memoria 2011 no difiere significativamente de la de años precedentes y trata de ofrecer una panorámica detallada de la actuación de la Agencia que, a su vez, permita obtener una visión de conjunto acerca del estado y la evolución de la protección de datos en nuestro país.

La primera parte está dedicada a exponer las actividades desarrolladas por la Agencia, analizando y valorando aquellos datos o tendencias que pueden resultar más relevantes para conocer la evolución de la protección de los datos personales en España. En este sentido, resultan especialmente reseñables los incrementos producidos tanto en el número de denuncias presentadas (más de un 50%), como en el de consultas ciudadanas (casi un 30%), así como el crecimiento en un 22% de los ficheros inscritos, por cuanto son reveladores del mayor grado de conocimiento y de concienciación de la ciudadanía en relación con sus derechos y están en el origen de la notable intensificación de la actividad de la Agencia. En segundo lugar, se presentan las principales resoluciones del año 2011 y los informes más relevantes evacuados durante este periodo, junto con

las novedades más significativas habidas el ámbito normativo y jurisprudencial. En un capítulo específico se analizan los grandes retos que actualmente tiene planteados la protección de datos y se expone el modo en el que la Agencia los está afrontando: la seguridad y la protección de la privacidad en Internet, las demandas de "derecho al olvido", el nuevo paradigma de cloud computing, los riesgos derivados de la geolocalización y del reconocimiento facial, el crecimiento de los flujos internacionales de datos fruto de la globalización, son objeto de estudio individualizado. Finalmente, se da cuenta de la evolución europea e internacional en materia de protección de datos y de la contribución de la Agencia Española a esta evolución, sea directamente o en el marco de las instituciones que están promoviendo los nuevos desarrollos.

La segunda parte de la Memoria, que se presenta bajo el título la "**Agencia en cifras**", ofrece información estadística detallada y tabulada en función de distintos indicadores con el fin de proporcionar una "imagen fiel" de la actividad desarrollada por la institución en sus diferentes áreas durante el año 2011.

Confío en que la información contenida esta nueva Memoria pueda resultar útil a los profesionales y estudiosos de la privacidad así como, en general, a todos los interesados en la protección de los datos personales. En todo caso, invito a quienes deseen saber más sobre la actuación de la Agencia -y sobre el derecho fundamental cuya garantía tiene encomendada- a visitar nuestra renovada página web (**www.agpd.es**) en la que podrán encontrar las últimas resoluciones e informes jurídicos, junto con diversos materiales y herramientas de ayuda para conocer mejor el derecho y facilitar el cumplimiento de ley.

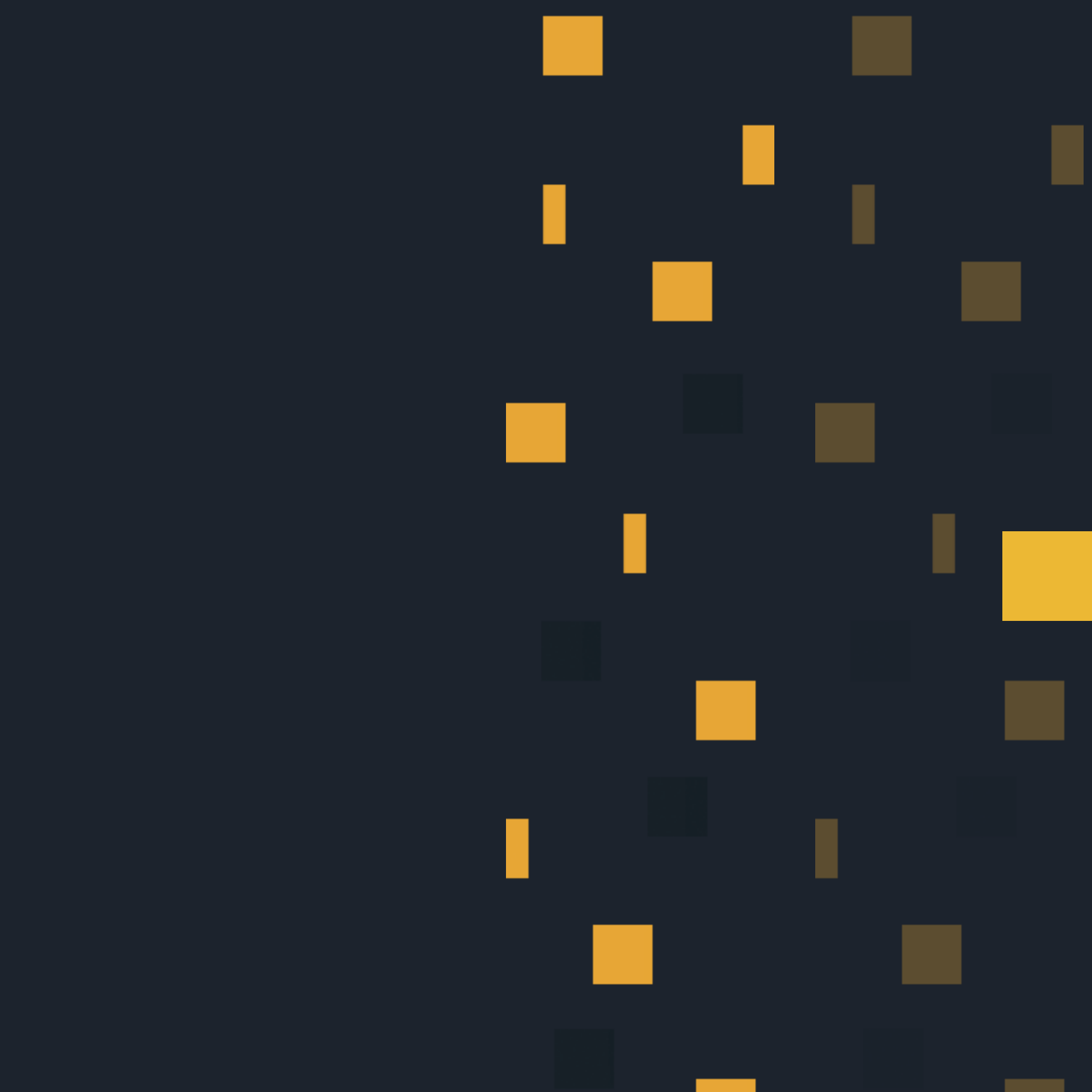
José Luis Rodríguez Álvarez
Director de la Agencia Española de Protección de Datos

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

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

índice

LA AGENCIA EN CIFRAS



MEMORIA 2011

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

CIUDADANOS MEJOR INFORMADOS Y MÁS CONCIENCIADOS SOBRE SUS DERECHOS

El creciente conocimiento de los ciudadanos sobre la protección de sus datos personales se ha traducido en un incremento de las solicitudes de información al Servicio de Atención al Ciudadano, así como del número de denuncias y de solicitudes de tutela de los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO).

Las **consultas al servicio de Atención al Ciudadano** no sólo consolidan la tendencia de crecimiento de años anteriores, sino que se han ampliado en un porcentaje significativo que se aproxima al 30% (28,4%), alcanzando la cifra de 134.635.

Asimismo, se han incrementado los accesos a la página web de la Agencia que se aproximan a los 3 millones (2.892.516), con un promedio diario cercano a los 8.000 accesos (7.923).

El canal telefónico, con 113.579 consultas, continúa siendo el preferido por los ciudadanos para informarse sobre la normativa de protección de datos, seguido de la consulta por escrito (17.715) y la presencial, que disminuye respecto al año anterior (3.341 consultas frente a 4.093). En las consultas por escrito se aprecia una importante reducción de las tramitadas a través de la página web que pasan a ser algo más de la mitad de las contestadas por escrito, frente a casi el 90% del año anterior. Aunque es necesario contar con más tiempo para valorar este descenso en función de su evolución, parece poner de manifiesto las dificultades para consolidar el uso de medios electrónicos en las relaciones entre la Administración y los ciudadanos.

Junto a las tradicionales consultas relacionadas con la inscripción de ficheros, el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (ARCO) se mantiene como principal objeto de consulta por los ciudadanos en un porcentaje próximo al 30% (28,81%).

Más de la mitad de estas cuestiones (50,35%) están relacionadas con el ejercicio del derecho de cancelación, lo que resulta indicativo del rechazo que a los ciudadanos les suscita que se utilice indebidamente su información personal. Este indicador se ve reforzado con el amplio porcentaje de quienes consultan acerca del modo de ejercer el derecho de oposición al tratamiento de sus datos personales, que asciende al 27,85% de las que versan sobre el ejercicio de derechos.

Estas últimas consultas adquieren especial relevancia si se tiene en cuenta que el ejercicio del derecho de oposición constituye una de las principales vías para hacer frente al fenómeno de la indexación de datos publicados en medios de comunicación y en diarios y boletines oficiales por parte de los buscadores en Internet, posibilitando el acceso universal y permanente a la información disponible en Internet.

En esta misma línea resultan también reseñables por su novedad -pese al reducido porcentaje de consultas (2,50%)- las solicitudes de información sobre las posibilidades de exclusión de las guías telefónicas para evitar la publicidad telefónica. En este sentido, debe recordarse la opción de restringir la recepción de publicidad mediante la incorporación voluntaria a la "Lista Robinson" de Adigital en la que, según los últimos datos disponibles (marzo de 2012), figuran 1.208.974 usuarios inscritos.

Sumados los porcentajes mencionados se constata que algo más del 80% de las consultas sobre el ejercicio de derechos están relacionadas con la decisión de los ciudadanos de evitar el tratamiento de sus datos personales.

El derecho de acceso a la información objeto de tratamiento motiva el 15,7% de las consultas sobre el ejercicio de derechos destacando las relativas al acceso a la historia clínica, mientras que las efectuadas sobre el derecho de rectificación ocupan una posición marginal (3,57 %).

Junto a las consultas sobre el ejercicio de derechos son destacables las que afectan al ámbito de aplicación de la LOPD no sólo en España, sino también sobre el tratamiento de datos de residentes en nuestro país en páginas web alojadas en terceros países. Esta circunstancia es indicativa de la mayor preocupación de los ciudadanos respecto a las garantías que la normativa española de protección de datos les ofrece sobre el uso que las corporaciones multinacionales que prestan servicios en Internet realizan de su información.

En cuanto al fenómeno de la videovigilancia las principales consultas se refieren al control por el empresario de las condiciones de trabajo y al periodo de conservación de las grabaciones.

Finalmente, ha de reseñarse que comienzan a plantearse consultas sobre nuevos servicios como el "cloud computing", que suscitan múltiples interrogantes desde el punto de vista de la protección de datos.

Mantener un alto nivel de calidad en el Servicio de Atención a los ciudadanos es una de las prioridades de la AEPD, tanto como mecanismo de respuesta a sus inquietudes, como de conocimiento de las garantías que los protegen.

Las encuestas de satisfacción sobre este servicio permiten constatar que se mantiene un elevado nivel de calidad tanto en lo que respecta a las instalaciones de la Agencia como en lo que se refiere a la utilidad y suficiencia de la información obtenida, los impresos y documentación disponible, el tiempo de espera y el índice general de atención y asistencia.

Los resultados generales de las encuestas son los siguientes:

- En relación con las instalaciones en las que se ubica la Agencia (su accesibilidad, comodidad y funcionalidad), el 83% de los ciudadanos encuestados las valoraron de modo satisfactorio o muy satisfactorio.

- El 92,5% de las encuestas reflejaron una valoración satisfactoria o muy satisfactoria en relación con la utilidad y la suficiencia de la información facilitada por el personal de Agencia.

- Respecto a los impresos y demás documentación disponible para el ciudadano, se observa que el 94,1% de las encuestas valoraron satisfactoria o muy satisfactoriamente su idoneidad.

- En cuanto al tiempo de espera necesario para poder ser atendido por el personal, el 87,5 % de los encuestados se pronunciaron de forma satisfactoria o muy satisfactoria.

- Y, finalmente, sobre la atención y asistencia facilitadas desde la sede de la Agencia y por su personal, se concluye que el 86,6% de las valoraciones de los ciudadanos resultaron ser satisfactorias o muy satisfactorias.

La evaluación específica del canal telefónico que, como se ha indicado, es el elegido mayoritariamente por los ciudadanos, ofrece aún un resultado más satisfactorio sobre la calidad del servicio en los siguientes términos:

- El 96,96% se manifestaron satisfechos con la información recibida.

- El 97,09% consideraron que la persona que les atendió tenía los suficientes conocimientos sobre la materia objeto de consulta.

- El 98,02% estimaron que el trato recibido por parte del teleoperador fue correcto.

Todo ello hace a los empleados públicos que desarrollan esta actividad en la Agencia acreedores del reconocimiento de su profesionalidad e implicación personal en el asesoramiento y la asistencia para una mejor protección de los datos de los ciudadanos.

La política de información basada en la elaboración de guías prácticas sobre protección de datos se ha concretado este año en la elaboración de una nueva edición de la "**Guía del Derecho Fundamental a la Protección de datos de Carácter personal**" revisada y actualizada.

El objetivo de esta publicación es difundir en un lenguaje claro, sencillo y fácilmente comprensible para cualquier ciudadano los aspectos básicos de la protección de datos.

Partiendo de esta premisa, la guía trata las principales cuestiones de interés como son los principios generales que rigen la materia, -calidad de los datos, obligación de consentimiento-, los derechos de las personas, -consulta, ejercicio de los derechos de acceso, rectificación, cancelación y oposición al tratamiento-, y los mecanismos de defensa ante una posible vulneración de estos derechos.

Además se analizan los principales riesgos que puede comportar el tratamiento de datos en algunos contextos específicos –menores, internet, publicidad y solvencia patrimonial- ofreciendo recomendaciones y consejos de carácter práctico.

Los **medios de comunicación** se han consolidado como cauce esencial de difusión de la normativa de protección de datos personales a los ciudadanos.

Aunque desde el punto de vista cuantitativo se ha producido un leve descenso de las informaciones sobre esta materia, continúa existiendo un alto nivel de interés informativo que se ha traducido en 44 notas de prensa y convocatorias enviadas a los medios de comunicación, 57 notas de agenda informativa de la Agencia y en torno a 550 solicitudes de entrevistas o demandas de información de medios de comunicación atendidas.

Estos datos ponen de manifiesto que la mayor parte de las informaciones difundidas sobre la protección de los datos personales ha sido a iniciativa de los propios medios de comunicación, lo cual revela que la información sobre la protección de datos personales ha pasado a formar parte de los asuntos de interés cotidiano para dichos medios.

Esta conclusión se ve reforzada, adicionalmente, por el incremento de los trabajos que han concurrido a la obtención de los premios anuales de protección de datos personales en la categoría de comunicación (19 candidaturas).

El premio principal en la categoría de Comunicación se otorgó a dos periodistas de los informativos de fin de semana de Antena 3, por la realización y emisión de destacados reportajes relacionados con la privacidad y la protección de datos en los que abordaron asuntos como el derecho al olvido, la geolocalización, o el acceso y difusión sin consentimiento de información personal procedente de teléfonos móviles.

Asimismo, se concedieron sendos accésit a dos periodistas del diario Público, por varios artículos en los que se abordan asuntos como la computación en nube, el reconocimiento facial en redes sociales, la protección de la privacidad en Internet, la transferencia de los datos de usuarios de servicios de Internet a servidores de otros países, la captación y almacenamiento de datos de localización de redes WIFI y de datos de tráfico asociados a estas redes por parte del servicio Street View de Google, o el robo de datos a Sony como consecuencia de una brecha de seguridad en sus servidores.

Desde una perspectiva sustantiva, el abanico de temas tratados por los medios de comunicación se ha ampliado considerablemente. Así, junto a los asuntos habituales que han seguido siendo objeto de atención como el derecho al olvido en Internet, la protección de los menores en las redes sociales, la videovigilancia o el tratamiento de datos asociados a la morosidad y a las empresas de recobro, se han multiplicado las informaciones sobre nuevos temas entre los que destacan los siguientes:

- La suplantación de identidad en servicios en Internet y, en particular, en las redes sociales.
- El tratamiento de datos de localización en dispositivos inteligentes (smartphones).
- Las brechas de seguridad en la custodia de información personal.
- Los servicios de computación en nube ("Cloud computing").

A los que hay que añadir la amplia difusión que ha alcanzado la sentencia del Tribunal de Justicia de la Unión Europa, de 24 de noviembre de 2011, por la que se declaró el efecto directo del artículo 7.f) de la Directiva 95/46 del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 a la que más adelante se hará referencia.

A FACILITAR EL CUMPLIMIENTO DE LA LOPD

La AEPD ha impulsado diversas iniciativas dirigidas a facilitar el cumplimiento de la LOPD a los responsables del tratamiento de datos personales que abarcan los siguientes ámbitos:

- Permitir la autoevaluación sobre el adecuado cumplimiento de la Ley.
- Dar a conocer y debatir las principales novedades del año.
- Ofrecer un cauce para resolver consultas complejas sobre la aplicación de la normativa de protección de datos.
- Actualizar la información del RGPD.
- Mejorar los procedimientos de notificación de ficheros.
- Promover la autorregulación a través de los Códigos Tipo.

En esta línea de actuación se sitúa en primer lugar EVALUA, una herramienta de autoevaluación creada por la AEPD y disponible en la web de la Agencia, que permite a los responsables del tratamiento comprobar de forma gratuita su adecuación al sistema de garantías de la LOPD y, específicamente, las obligaciones en materia de medidas de seguridad. El número total de encuestas realizadas accediendo a EVALUA ascendió ligeramente este año, hasta alcanzar las 21.557, siendo mayoritarias las relacionadas con el test general (16.311) frente a las del test de seguridad (5.246).

La AEPD mantiene su compromiso de ofrecer periódicamente información sobre las principales novedades en materia de protección de datos y promover un debate continuado con profesionales y expertos que tiene su manifestación más importante en la celebración de Sesiones Anuales Abiertas organizadas por la Agencia. La IV Sesión Anual, cuya celebración se retrasó al 27 de enero de 2012 para vincularla al Día Europeo de Protección de Datos, contó con la asistencia de más de 800 expertos. El tema central fue el análisis de las implicaciones para la protección de datos personales de la oferta de servicios de "cloud computing". Junto a ello, en la sesión se presentaron las principales resoluciones dictadas por la Agencia a lo largo del año 2011 así como los informes más destacados en ese periodo. Se examinaron las sentencias más relevantes de la Audiencia Nacional y del Tribunal Supremo y se prestó especial atención a la sentencia del Tribunal de Justicia de la Unión Europea que resolvió las cuestiones prejudiciales planteadas por el Tribunal Su-

premo en relación con la interpretación del artículo 7.f) de la Directiva Europea de Protección de Datos. Finalmente, se analizaron las principales novedades en el contexto europeo e internacional, particularmente la propuesta de Reglamento General de protección de datos personales y de una Directiva en el ámbito judicial y policial elaborados por la Comisión Europea en sustitución de la Directiva 95/46/CE.

Por otra parte, la AEPD responde mediante **informes específicos** a las consultas sobre cuestiones de cierta complejidad planteadas por los responsables de tratamientos de datos con la finalidad de resolver dudas y facilitar la aplicación de la LOPD. En el año 2011, se atendieron un total de 484, de las cuales 246 (57%) fueron planteadas por las Administraciones Públicas y 238 (43%) por el sector privado.

Continúa así apreciándose un menor número de consultas planteadas respecto a las formuladas en los años inmediatamente posteriores a la entrada en vigor del RLOPD y, en particular, a los años 2008 a 2009. Ello es debido a la mitigación del efecto producido como consecuencia de esa entrada en vigor, que hizo incrementarse en gran medida el número de consultas. 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, el mantenimiento de la pauta habitual de similitud en el número, con una muy ligera preponderancia de las procedentes del sector público (en este ejercicio el 57% del total).

En cuanto a las materias objeto de consulta destacan los siguientes aspectos:

- El incremento de las cuestiones relacionadas con las obligaciones del encargado del tratamiento (un 13%) y el cumplimiento del deber de informar (un 15%).

- La relevancia 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.

- El mantenimiento de un número relevante de cuestiones relacionadas con las cesiones de datos (un 38% del total), siendo igualmente relevante el número de cuestiones relacionadas con ficheros de titularidad pública y con la legitimación para el tratamiento (si bien disminuyen, en ambos casos, en un 34%).

- La disminución cuantitativa de cuestiones que resultaron especialmente reiteradas en el año 2010, pese a mantener un importante volumen. Así sucede en relación con las consultas relativas al ejercicio de los derechos de acceso, rectificación, cancelación y oposición y a la implantación de las medidas de seguridad.

- Una disminución sensible, de un 36% (que se suma a la de un 25% en el año 2010), de las cuestiones relacionadas con el tratamiento de datos con fines de videovigilancia.

Atendiendo a la distribución sectorial de las consultas del sector privado, se aprecian las siguientes tendencias:

- El mantenimiento de un reducido peso (sólo un 5% del total) 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 retomar 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 continuidad de la relevancia adquirida por las consultas procedentes de asociaciones no profesionales y fundaciones, que se consolidan como el primer sector de origen de las consultas, incrementando en un 23% sus cifras respecto del ejercicio anterior.

- El notable incremento de las consultas procedentes de los sectores de las comunicaciones electrónicas y de la sociedad de la información, así como el de las empresas de servicios informáticos (con incrementos respectivos del 41% y el 77% respecto al 2010).

- La disminución del volumen de consultas procedentes de partidos políticos y sindicatos (cercana al 30%) y del sector financiero (de un 30%, exactamente), así como del sector sanitario (de un 24%).

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

- La normativa aplicable en los supuestos en los que empresas ubicadas en territorio español prestan servicios de encargado del tratamiento para embajadas o consulados de Estados no integrantes del Espacio Económico Europeo

- El análisis de los derechos de los ciudadanos en relación con las informaciones publicadas sobre los mismos en Internet e indexadas a través de motores de búsqueda o en relación con páginas web que replican el contenido de informaciones ya publicadas y las posibilidades de reaccionar a través del ejercicio del derecho de oposición, conocido comúnmente como "derecho al olvido".

- Las incidencias en materia de protección de datos de las reformas operadas en el sector financiero y crediticio como consecuencia de procesos de reestructuración societaria o la creación de sistemas institucionales de protección.

- La conformidad con la legislación de protección de datos de la creación por los sujetos obligados, en virtud de lo dispuesto en la legislación de prevención del blanqueo de capitales, de ficheros comunes para el intercambio de información sobre operaciones que previamente hayan sido objeto de comunicación al Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias.

- Los requisitos exigibles para la transmisión de datos personales a órganos judiciales de los Estados Unidos en la fase del procedimiento conocida como "pre-trial discovery".

- La conformidad con la normativa de protección de datos del establecimiento de instalaciones de videovigilancia en relación con zonas anejas a inmuebles que incluyen instalaciones consideradas como estratégicas por el regulador sectorial correspondiente (arquetas de registro de telecomunicaciones).

- La licitud del establecimiento por operadores de comunicaciones electrónicas de sistemas de

rastreo de comunicaciones por SMS, a fin de prevenir el fraude y la suplantación de identidad en las comunicaciones dirigidas por las entidades financieras a sus clientes, sujeto a la garantía de preservación del anonimato del destinatario de los mensajes si no fuera cliente de tales entidades.

- La inexistencia de habilitación en las normas de protección de datos para que entidades privadas puedan elaborar ficheros en que se contengan las notificaciones de resoluciones sancionadoras publicadas en diarios oficiales o tablones edictales electrónicos, al resultar tal práctica proscrita por el artículo 7.5 de la LOPD.

- La licitud del acceso por los inspectores del Instituto Nacional de Seguridad Social a los datos contenidos en las historias clínicas relacionadas con los episodios que impliquen una situación de incapacidad temporal.

- El análisis de los requisitos necesarios para la conformidad con lo dispuesto en la legislación de protección de datos de los sistemas integrales de verificación y seguimiento de recetas médicas electrónicas, puestos en funcionamiento por determinadas Comunidades Autónomas.

- La necesaria aplicación del principio de proporcionalidad para que resulte conforme a la LOPD el tratamiento de datos identificativos de los trabajadores, como su DNI, fotografía o huella digital para el control de presencia en las instalaciones de la empresa.

- Los requisitos necesarios para la licitud de los sistemas de denuncia interna o *whistleblowing,* así como la legislación nacional aplicable en cada caso teniendo en cuenta la estructura del grupo empresarial y la ubicación del sistema.

- La licitud de las comunicaciones de datos por parte de las Administraciones Públicas a comisiones de investigación creadas por las Cortes Generales o los Parlamentos de las Comunidades Autónomas, en los términos establecidos en sus propios Reglamentos.

- Los criterios para determinar la licitud del acceso a los datos contenidos en expedientes administrativos por quienes tuvieran la condición de interesados.

- Los requisitos exigibles para la cesión de datos que obren en ficheros de los que sean responsables las Administraciones Públicas a los gobiernos de otros Estados en virtud de solicitudes efectuadas al efecto por los correspondientes órganos consulares.

- La limitación del posible acceso por la Administración a datos en poder de otros órganos con fines de verificación, respecto del que se exige el consentimiento del afectado, como consecuencia de la anulación por la STS de 15 de julio de 2010 del artículo 11 del Reglamento de desarrollo de la LOPD.

- El análisis del papel de los distintos intervinientes y los requerimientos de legitimación y proporcionalidad exigibles en distintos supuestos de realización de campañas publicitarias, con intervención de diversas entidades en distintos roles.

- Los requisitos legalmente exigibles para la creación de ficheros o la difusión pública en Internet

de datos personales referidos a las víctimas de la Guerra Civil y represaliados de Franquismo.

La **inscripción de ficheros** en el Registro General de Protección de Datos ha sido tradicionalmente uno de los indicadores significativos para evaluar el nivel de conocimiento y cumplimiento de la LOPD.

A 31 de diciembre de 2011 se encontraban inscritos en el RGPD 2.609.471 ficheros (el 95,5% de titularidad privada y el 4,5% de titularidad pública) lo que supone un incremento del 22% respecto al 2010, si bien disminuyó ligeramente el ritmo de crecimiento respecto al año anterior (464.599 inscripciones de nuevos ficheros en 2011 frente a las 497.116 en 2010).

El menor número de altas en el total de operaciones es probablemente debido a la evolución negativa de la tasa neta de creación de empresas, en valores negativos desde el inicio de la crisis económica en 2008. No obstante, el creciente grado de concienciación y responsabilidad sobre el cumplimiento de la normativa de protección de datos personales en el ámbito empresarial ha permitido que el número de empresas con ficheros inscritos en el RGPD se haya incrementado un 125% en el periodo 2008-2011.

En relación con el grado de actualización de la información registral, es interesante destacar que de los más de 214.000 ficheros inscritos en 1994, sólo un 20% permanecen activos sin haber sido objeto de modificaciones.

Con el fin de impulsar la actualización de la información registrada a finales de 2011, la AEPD realizó un requerimiento a 103 bancos y cajas de ahorro solicitando la revisión y en su caso actualización de la inscripción de sus respectivos ficheros. El requerimiento fue enviado a aquellas entidades que no habían adecuado la inscripción a lo dispuesto en la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, o que no habían declarado el nivel de medidas de seguridad o los colectivos objeto del tratamiento de datos en algunos de sus ficheros.

Estos últimos casos se referían a ficheros inscritos con anterioridad a la aprobación del reglamento de medidas de seguridad de la LORTAD (RD 994/1999) o de la implantación del formulario electrónico NOTA respectivamente.

Un 87% de las notificaciones fueron presentadas a través de Internet y el 13% restante en formato papel, cifras muy similares a las registradas el año anterior. Es reseñable asimismo el mayor uso de la firma electrónica. Esta forma de presentación supuso ya el 30% de las notificaciones en 2011, frente al 26% del año anterior.

En 2011 los mayores incrementos porcentuales se han producido en los ficheros con finalidades de "Guías/repertorios de servicios de comunicaciones electrónicas", "Videovigilancia" y "Comercio electrónico", con variaciones relativas superiores al 30%. La finalidad de "Gestión de clientes, contable, fiscal y administrativa" continúa siendo la más significativa en términos absolutos: un 63% de los ficheros inscritos tienen declarada esta finalidad. Le siguen las finalidades de "Recursos humanos" y "Gestión de Nóminas", declaradas en un 23% y un 17% de los ficheros, respectivamente.

Por sectores de actividad, el mayor crecimiento relativo se ha producido en las "Actividades políticas, sindicales y religiosas" (38%), "Comercio y servicios electrónicos" (32%) e "Inspección Técnica de Vehículos y otros análisis técnicos" (29%). En términos

absolutos, las actividades más declaradas son "Otras actividades", "Comunidades de Propietarios", "Comercio" y "Sanidad".

El número total de ficheros de titularidad pública inscritos a 31 de diciembre de 2011 era de 117.503, habiéndose producido un incremento neto de 9.214 ficheros respecto al 2010, 5.283 menos que en 2010.

En lo que corresponde a la Administración del Estado, debe reseñarse la actuación del Ministerio de Defensa con la notificación de los ficheros creados en siete Órdenes Ministeriales, publicadas durante el año 2011, que han incrementado en más de un 68% el número de ficheros inscritos, alcanzando un total de 853. De igual forma, debe destacarse la actualización realizada por el Ministerio de Empleo y Seguridad Social con 248 ficheros inscritos, lo que hace un total de 1.496 ficheros de dicho Ministerio.

También son destacables las reorganizaciones de ficheros de datos de carácter personal llevadas a cabo por el Ministerio de Agricultura, Alimentación y Medio Ambiente y el Ministerio del Interior suponiendo, en el primero de ellos, más de 500 notificaciones de ficheros y en el segundo, la realización de 238 notificaciones de actualización, entre las que se incluyen las de la Dirección General de Tráfico.

Por lo que corresponde a las Administraciones autonómicas, se debe destacar el número de ficheros inscritos desde el País Vasco, con un incremento del 36%, así como desde la Xunta de Galicia, con un 35% de incremento, el Principado de Asturias, (un 24%), o la Comunidad Autónoma de Aragón, con un incremento del 20%, respecto a las inscripciones de creación de ficheros realizadas en el año anterior.

Es importante señalar la labor que, al objeto de mantener actualizada la relación de ficheros empleados en estas Administraciones, se ha llevado a cabo por parte de las Comunidades Autónomas de Galicia, Aragón y Canarias, con un relevante número de notificaciones de actualización y supresión de ficheros, que hace que el número total de ficheros inscritos de estas Comunidades Autónomas, a 31 de diciembre de 2011, sea inferior al del año anterior.

En el proceso continuado de mejora de los procedimientos de notificación de ficheros, en abril de 2011 entró en producción el nuevo sistema de información RENO para la tramitación de los expedientes de inscripción de ficheros, copias del contenido de la inscripción y autorización de transferencias internacionales.

El desarrollo de esta nueva aplicación ha venido motivado por la necesidad de mejorar la eficiencia de las operaciones asociadas a la inscripción de ficheros, cuyo volumen se ha venido incrementado de manera significativa en los últimos años. Su implantación se inscribe en el desarrollo de la administración electrónica promovido por la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos y por su normativa de desarrollo.

RENO permite la tramitación desasistida de las notificaciones de ficheros de acuerdo con unas reglas configurables. El nuevo sistema de información incorpora sistemas de firma electrónica individual y de sello electrónico para la emisión de resoluciones, notificaciones y otros escritos. Por otra parte, permite optimizar la gestión de la información del Registro al almacenar en un expediente electrónico único toda la documentación concerniente a la inscripción de un fichero o a otros trámites del Registro General de Protección de Datos.

Asimismo, la puesta en marcha de RENO ha posibilitado que junto con la resolución de inscripción de un fichero se notifique al responsable o a su representante un informe resumido de la relación de ficheros activos que figuran a su nombre, de forma que con cada operación de inscripción tenga información actualizada de la situación de sus ficheros.

Un instrumento complementario para facilitar el cumplimiento de la LOPD son los **Códigos tipo**, como fórmulas de autorregulación que adaptan la norma a las características de un sector de actividad.

En 2011 se han dictado tres resoluciones relativas a la inscripción de códigos tipo, dos acordando la inscripción en el RGPD y una denegando la inscripción:

- Con fecha 5 de septiembre de 2011, se acordó la inscripción del "CÓDIGO TIPO DEL FICHERO DE AUTOMÓVILES DE PÉRDIDA TOTAL, ROBO E INCENDIOS" (CT/0002/2011), promovido por la Unión Española de Entidades Aseguradoras y Reaseguradoras (UNESPA), cuyo objeto es establecer la regulación del Fichero de automóviles de pérdida total, robo e incendio y el uso de la información en él contenida, que podrá ser realizado por las entidades asociadas al código.

- Con fecha 11 de noviembre de 2011, se acordó la inscripción del "CODIGO TIPO DE TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL PARA ESTABLECIMIENTOS SANITARIOS PRIVADOS DE LA PROVINCIA DE SEVILLA", promovido por el Colegio Oficial de Farmacéuticos de Sevilla (CT/0002/2010), cuyo objeto es regular los tratamientos de los datos de carácter personal que habitualmente se recogen en las oficinas de farmacia y demás establecimientos sanitarios privados localizados en la provincia de Sevilla, cuyo titular sea un licenciado en farmacia que esté colegiado en el mencionado Colegio Oficial.

- Con fecha 8 de septiembre de 2011, se denegó la inscripción del CODIGO TIPO DE FARMACEUTICOS EMPRESARIOS CON FARMACIA ADHERIDA AL CÓDIGO" –CODIGO TIPO FEFAC-VERITAS" (CT/0001/2011), promovido por la Federació D´Associacions De Farmácies de Catalunya, al no cumplir los requisitos establecidos en el Reglamento de desarrollo de la Ley Orgánica 15/1999, en particular en su Título VII.

Es asimismo reseñable el incremento en el interés por la elaboración de códigos tipo, de manera que, al margen de las consultas telefónicas demandando información al respecto, durante 2011 se han mantenido diversas reuniones para debatir otros proyectos promovidos por distintos sectores: Colegio de Farmacéuticos de Barcelona (cuya tramitación se hace en colaboración con la Autoridad Catalana de Protección de Datos), Asociación AEDCI (aplicación de la LOPD en relación con destrucción segura de documentos por parte de las empresas) y propuesta de modificación del Código tipo de la UNIÓN CATALANA DE HOSPITALES, modificado para su adecuación al RLOPD con fecha 16 de noviembre de 2009.

Por último, en el año 2011 se han recibido las memorias anuales correspondientes al año 2010 de siete promotores de códigos tipo inscritos en el RGPD, que resumen las actividades realizadas para difundir y promover la adhesión al código tipo correspondiente y dan cumplimiento a la obligación prevista en el artículo 78.b) del RLOPD. A los promotores que no han remitido las memorias se les han realizado los correspondientes requerimientos para que efectúen la remisión de la memoria anual.

B. UNA RESPUESTA ACTIVA A LAS DEMANDAS CRECIENTES DE LOS CIUDADANOS

En el año 2011 se ha producido una importante novedad al modificarse el régimen sancionador de la LOPD por la Ley 2/2011, de 4 de marzo, de Economía Sostenible. La reforma del régimen sancionador de la LOPD tiene por objeto alcanzar mayores niveles de seguridad jurídica así como posibilitar una aplicación más flexible de las sanciones económicas previstas en la Ley.

El objetivo de lograr mayor seguridad jurídica se articula a través de una más adecuada tipificación de las conductas infractoras, la supresión de tipos que se han demostrado técnicamente inadecuados y la recalificación de algunas infracciones atendiendo a los bienes jurídicos que protegen. Asimismo se redefine, manteniendo su núcleo básico, la potestad de inmovilización de ficheros.

La posibilidad de flexibilizar las sanciones económicas presenta un triple vertiente: la ampliación de los criterios de modulación dentro de cada escala de infracciones leves, graves o muy graves; la reformulación de los criterios que permiten su atenuación aplicando la escala inferior en grado a la infracción declarada y la incorporación de la novedosa figura del apercibimiento como alternativa a la sanción económica.

Los nuevos criterios de modulación y atenuación de las sanciones y la posibilidad de apercibir al responsable del tratamiento permiten discriminar en la imposición de las sanciones, especialmente cuando afecten a grandes, pequeñas o medianas empresas, profesionales, personas físicas o entidades sin ánimo de lucro.

Junto a ello el régimen sancionador ha modificado los mínimos de las sanciones aplicables a infracciones leves y graves incrementando a 9.000 euros en el primer caso y reduciéndolo a 40.000 euros en el segundo.

Entre las modificaciones del régimen sancionador de la LOPD, una de las novedades más significativas, ha sido, sin duda, la incorporación de la figura del apercibimiento como alternativa a la sanción.

Esta nueva fórmula resulta de aplicación en el caso de primeros infractores (no apercibidos o sancionados previamente) por hechos constitutivos de infracción leve o grave, y siempre que concurran de forma significativa determinadas circunstancias, como son una cualificada disminución de la culpabilidad del imputado o de la antijuricidad del hecho atendiendo, entre otros, a criterios como el carácter continuado de la infracción, el volumen del negocio o actividad del infractor, el grado de intencionalidad, o la reincidencia por comisión de infracciones de la misma naturaleza. Asimismo, cabe aplicar la figura del apercibimiento teniendo en cuenta si ha existido una regularización diligente de la situación irregular, la influencia en la infracción de la conducta del afectado, el reconocimiento espontáneo de la culpa o el que la infracción fuese anterior a un proceso de fusión por absorción, no siendo imputable a la entidad absorbente.

La trascendencia cuantitativa del apercibimiento ha sido alta desde la entrada en vigor de la reforma, el 6 de marzo de 2011, hasta el 1 de enero de 2012, como se manifiesta en el elevado porcentaje que representa sobre el total de resoluciones en las que se declara el incumplimiento de la LOPD por parte de responsables de ficheros de titularidad privada. En concreto, de 706 resoluciones de infracción a responsables privados, dictadas desde la entrada en

vigor de la reforma, 312 de ellas han concluido con apercibimiento, lo que supone un 44% del total.

Su relevancia ha sido dispar en función del sector, destacando especialmente los apercibimientos correspondientes al sector de la videovigilancia, que representan el 70% del total.

Conviene, no obstante, señalar que su aplicación no es automática, sino que es necesario resolver en cada caso, atendiendo a las circunstancias concurrentes, sobre la procedencia de dictar un apercibimiento o acordar el inicio de un procedimiento sancionador.

Consecuentemente, en determinados supuestos se ha considerado que no procedía el apercibimiento al no concurrir la disminución cualificada de la culpabilidad y de la antijuridicidad requerida por la norma para que sea aplicable la figura. Así ha ocurrido, por ejemplo, en los casos de una comunidad de propietarios que mantiene la divulgación a terceros de datos de morosos en un tablón cerrado durante meses o que continúan expuestos tras una sentencia absolutoria (PS/00585/2010) o en los supuestos de dolo o mala fe por parte del presunto infractor en casos de suplantación de identidad a través de un perfil en red social (PS/00137/2011) o en tiendas online (PS/00322/2011).

En otros casos, el criterio que se ha tenido en cuenta para descartar el apercibimiento y optar por la sanción, ha sido la sensibilidad de los datos afectados. Por ejemplo, en un caso de abandono de documentación en vía pública de una academia de opositores (PS/00560/2010); el envío de mensajes electrónicos a destinatarios múltiples sin copia oculta, por parte de un local de intercambio de parejas (PS/00445/2011); la difusión pública en el perfil de una cafetería en una red social del parte de baja médica de una empleada (PS/00434/2011), o la publicación en Internet de datos médicos por parte de una clínica, aún debiéndose a un error puntual (PS/00417/2011).

Asimismo, el volumen de negocio del infractor o su vinculación con el tratamiento de datos se ha tenido en cuenta para excluir el apercibimiento en casos como el relativo a un distribuidor de telefonía (PS/00244/2011), a una empresa energética que hace accesible un currículo de un trabajador en Internet (PS/00142/2001), a una asesoría fiscal y legal (PS/00065/2011), a hoteles pertenecientes a grandes corporaciones (PS/00068/2011) o a hospitales.

Por el contrario, la figura del apercibimiento ha sido objeto de aplicación en multitud de supuestos en los que concurrían las circunstancias establecidas por el legislador. Entre ellos, cabe mencionar los siguientes:

- Administrador de fincas que en el portal web a disposición de las comunidades de propietarios permite el acceso de los vecinos a información relativa a las novedades de la finca, actas, etc. Por error, cuelga en dicho entorno una relación de recibos en los que aparecen los números de cuenta bancaria de los miembros de la comunidad (PS/00545/2010).

- Particulares que utilizan Internet (Picasa) para colgar los resultados de las pruebas de baremación que publica una consejería para el acceso a un cuerpo de enseñanza, listas que la consejería publica en los tablones de anuncios de las delegaciones, en la que se incluyen datos personales como nombre, apellidos y DNI (A/00008/2011).

- Hostal que instala un sistema de videovigilancia en las zonas comunes del mismo, sin enfocarlas a vía pública, pero sin cumplir los requisitos necesarios de información a los afectados (A/00024/2011).

- Constructor de un pueblo que, al objeto de dar a conocer a sus clientes la página web de nueva creación, envía un correo a las direcciones personales de sus clientes en abierto y sin utilizar la copia oculta (A/00037/2011).

- Sitio web especializado en viajes que activó un foro para todos los clientes que se habían dado de alta a través de la web para recibir información de viajes. Al modificar la web se produce un error y durante dos días permanecieron en la portada de la misma los nombres de los usuarios de forma clara, además de su dirección electrónica (A/00038/2011).

- Denuncia por parte del Director de un Colegio y tres profesoras del centro educativo en la que se pone de manifiesto que varios alumnos del centro, de entre 7 y 8 años de edad, fueron grabados con una videocámara en el transcurso de una actividad extraescolar. El denunciado publicó las imágenes grabadas de los menores en el muro de su propio perfil en Facebook (A/00275/2011).

- Publicación en internet de la fotografía de una boda, a pesar de que en el contrato de encargo del reportaje fotográfico expresamente se había negado el consentimiento para hacer uso de las fotos con fines publicitarios. Tras el requerimiento de la AEPD, el fotógrafo advirtió el error y la retiró (A/00321/2011).

- Inserción de datos relativos al denunciante -que figuran en su expediente de expulsión como socio- en la Web de la Sociedad, accesible a terceros (A/00349/2011).

Por otra parte, como consecuencia del principio de aplicación retroactiva de la norma más favorable (art. 128.2 LRJPA), la AEPD ha recalificado los procedimientos pendientes de resolución. La Audiencia Nacional ha procedido de idéntico modo respecto de los recursos contencioso-administrativos en tramitación.

El mayor conocimiento del derecho a la protección de datos personales por los ciudadanos ha generado una demanda creciente de las **reclamaciones** presentadas ante la AEPD. En el año 2011 el número de denuncias registradas en la Agencia ha aumentado en un 51,6% respecto a las presentadas en 2010. El mayor número de denuncias ha incidido en las actuaciones previas de investigación, que consolidan el crecimiento de los años anteriores, incrementándose en un 25,26% adicional.

El incremento de las denuncias presentadas en 2011 ha derivado en un crecimiento en el número de **resoluciones declarativas de infracción** del 37,7% (procedimientos sancionadores a responsables privados, procedimientos de infracción de Administraciones Públicas y apercibimientos). No obstante, la aplicación de la figura del apercibimiento ha determinado una disminución del 14,5% en las sanciones económicas declaradas.

El sector en el que se ha producido un mayor incremento de las sanciones (64%) y se han declarado en mayor medida (25,5%) y cuantía, (63%) es el de las telecomunicaciones.

Las resoluciones de archivo y las denuncias inadmitidas crecen un 18%. El incremento, aunque menor al de denuncias presentadas, obedece – junto a los casos en que el denunciante desiste - a las siguientes razones:

a) *Nueva doctrina de las resoluciones jurisprudenciales.*

Los criterios jurídicos recogidos en las sentencias de los Tribunales que requieren modificar los aplicados para la apertura de procedimientos sancionadores, archivando expedientes que antes acabarían en sanción.

b) *Inaplicación de la LOPD.*

La no aplicabilidad de la LOPD puede producirse por varias razones:

- por estar excluido de su ámbito territorial de aplicación.

- por no afectar a datos de personas físicas.

- por realizarse un tratamiento de datos relativos a fallecidos no amparados por la LOPD.

- por tratarse de cuestiones ajenas al ámbito competencial de la AEPD al presentarse reclamaciones sobre cuestiones como facturación o consumo, deficiencias en la prestación del servicio, interpretación sobre cláusulas contractuales o envío de mensajes de tarificación adicional Premium.

c) *Ponderación de otros derechos e intereses legítimos.*

Tal circunstancia puede concurrir, entre otros, en los casos en que prevalecen otros derechos, tales como:

- el derecho a la libertad de información o expresión.

- el derecho a la tutela judicial efectiva como habilitante para el tratamiento de datos.

- el ejercicio de la libertad sindical que legitima el tratamiento de datos, principalmente en el ámbito laboral.

d) *El carácter excepcional del procedimiento sancionador cuando el ordenamiento permite otras formulas para satisfacer las pretensiones de los afectados*.

La LOPD ofrece a los afectados diversas alternativas para reaccionar ante la vulneración de sus derechos. Entre ellas se encuentra el ejercicio y la tutela por parte de la AEPD de los denominados derechos ARCO, entre los que destaca el ejercicio del derecho de cancelación para conseguir el cese en el tratamiento de los datos personales. El ejercicio de los derechos permite, además, una respuesta más rápida que los procedimientos de declaración de infracciones atendiendo a los plazos temporales establecidos en la LOPD.

En consecuencia, la apertura de un procedimiento sancionador ha de considerarse como último recurso para reaccionar ante el incumplimiento de la norma.

Las resoluciones de declaración de infracción de administraciones Públicas han crecido un 30%. El incremento se debe principalmente a la declaración de 32 infracciones a Registros de la Propiedad (prácticamente la tercera parte del total de las impuestas) por haber desvelado información sin verificar adecuadamente el interés legítimo de los solicitantes. Junto a ellas cabe destacar las siguientes:

- AP/00050/2011. Denuncia por la difusión pública de los nombres de cada uno de los miembros de la colonia española a través de un mensaje electrónico remitido por una Embajada a más de 350 direcciones electrónicas.

- AP/00046/2011. Un Ayuntamiento difunde a

través de su portal informativo en Internet, los datos personales de una menor. Se trata de una noticia relativa a una intervención de la policía que medió en una discusión familiar, entre la madre denunciante y la hija menor de edad. Al informar sobre el suceso se divulgaron los datos personales de la menor.

- AP/00041/2011. Fallo en las medidas de seguridad de un sitio Web de una Consejería de Sanidad que ocasiona el acceso no autorizado a los datos de reclamaciones presentadas a través de dicha Web, incluyendo diagnósticos médicos. El acceso pudo realizarse sustituyendo aleatoriamente el número de la reclamación (4 cifras) en la URL.

- AP/00032/2011. Una empleada de un Ayuntamiento denuncia que durante una Incapacidad Temporal el Ayuntamiento ha abierto el sobre con su parte de baja, dirigido al servicio médico del INSS con el diagnóstico, registrándolo y manteniéndolo en sus ficheros, ya que se facilitaron a la denunciante cuando ejerció el derecho de acceso. La alcaldía lo devolvió a la denunciante tras comprobar que no debía estar en sus archivos.

La cuantía de las sanciones ha crecido un 12% respecto a 2010, pese a la disminución del 14,5% en las sanciones declaradas, circunstancia que se debe fundamentalmente al incremento de las sanciones declaradas como graves en un porcentaje próximo al 3,5%.

Cabe resaltar que apenas el 14% de las multas se han impuesto sin atenuación, puesto que en el 86% de los casos se ha modulado la sanción, bien al dictarse apercibimientos o bien aplicando los criterios de atenuación que prevé la LOPD en los apartados 4 y 5 del artículo 45.

Las solicitudes de **tutela de derechos**, frente a la disminución del año anterior, han vuelto a incrementarse en un porcentaje importante que asciende al 34,58%, alcanzando la cifra de 2.230 solicitudes.

Entre las resoluciones de tutelas más destacables, cabe citar las siguientes:

- La estimación de una tutela para la cancelación de datos de una antigua reclusa, rechazándose el argumento de que debe mantenerse por razones históricas y estadísticas (TD/781/2011).

- La desestimación del derecho de cancelación por que los datos están amparados en el derecho fundamental a la libertad de información al referirse a una noticia de prensa sobre corrupción en 2011 (TD/765/2011).

- Las múltiples tutelas planteadas frente a buscadores en Internet, entre las que cabe citar, en cuanto a las resoluciones estimatorias, las siguientes:

  - Informaciones ciertas pero ya obsoletas.

    - Sanción impuesta en 1983 por ocultar datos de la renta para obtener una beca universitaria (TD/01768/2011).

    - Indulto en 1991 sobre un delito de robo con fuerza en las cosas cometido en 1988 (TD/01225/2011).

    - Divulgación en varios sitios web de identidades de plazas de interinos en convocatorias de empleo público (TD/00501/2011).

  - Informaciones que no resultaron ciertas.

- Portal informativo que cancela una noticia relativa al archivo de una causa abierta por un crimen con decapitación (TD/00909/2011).

- Condena por una falta de maltrato y absolución posterior (TD/00537/2011).

- Persona implicada en un proceso de corrupción de menores que fue sobreseído (TD/01520/2011).

Respecto a las resoluciones desestimatorias, se pueden destacar los siguientes casos:

- Persona inhabilitada para ser administrador que pide la cancelación en el BOE sin que pase el tiempo de la inhabilitación (TD/00139/2011).

- Personas relacionadas con casos de corrupción, que tienen relevancia pública y son objeto de información no obsoleta (TD/01218/2011 y TD/00413/2012).

Publicación de una noticia de 2007 sobre el gerente de una fundación subvencionada por la Administración imputado por falsificación de documentos (TD/00720/2011).

Solicitud de cancelación ante la Dirección General de la Policía y Guardia civil de datos personales, denegada en aplicación de los artículos 22.4 y 23.1 de la LOPD (TD/1469/2011).

Inaplicación del derecho de acceso previsto en la LOPD en supuestos como el acceso a expedientes de la Fiscalía, que deberá realizarse por los medios previstos en la legislación sectorial (TD/1395/2011), o a un expediente de la Agencia Nacional de Evaluación de Calidad y Acreditación (ANECA), en el que deben ejercerse los derechos previstos en la Ley 30/1992 (TD/179/2011).

En cuanto a las principales **áreas temáticas**, se describen a continuación aquellas en que se ha producido una actuación creciente en inspecciones y resolución de procedimientos.

a) *Morosidad.*

Destacan los casos de fraude o suplantación en la prestación del consentimiento en la contratación. Con frecuencia la morosidad deriva de un supuesto de suplantación del titular de los datos por un tercero. La Agencia, en consonancia con la jurisprudencia de la Audiencia Nacional, valora la diligencia en la obtención de la información. La cuestión a dilucidar consiste en determinar si la empresa contratante empleó o no una diligencia razonable a la hora de identificar a la persona con la que suscribió el contrato.

Así, se ha archivado por acreditar diligencia el supuesto de una empresa de telecomunicaciones que remite una grabación telefónica en la que la denunciante se identifica como tal, aportando su DNI, nombre y apellidos, y presta su consentimiento para la contratación de tres líneas (E/04273/2010).

El incumplimiento de las garantías previstas reglamentariamente para la inclusión de datos del deudor en fichero común de solvencia ha derivado en denuncias y resoluciones respecto de la acreditación del requerimiento de pago previo a la inclusión.

El acreedor en la realización de sus gestiones para hacer efectivo el cobro de la deuda debe salvaguar-

dar el deber de secreto evitando su divulgación a terceros. En 2011 y años anteriores se investigaron a 6 entidades tras más de 280 denuncias por vulneración del deber de secreto en llamadas para el recobro de deudas que han finalizado en 4 declaraciones de infracción (P. ej. PS/00203/2011). Por ello se debe insistir en que las justificadas gestiones para recuperar las deudas por parte de los acreedores debe complementarse con la escrupulosa custodia de sus datos, evitando su divulgación a terceros.

b*) Datos en Internet.*

Las denuncias motivadas por la aparición de datos en internet sin consentimiento permiten diferenciar diversas situaciones en función de que se dirijan contra aquel que inserta el dato, el titular de la página en la que se inserta la información o el prestador de servicios.

A su vez, respecto de quién inserta el dato, es necesario diferenciar varias situaciones a los efectos de iniciar la vía sancionadora u optar por otras fórmulas reparadoras como instar el ejercicio del derecho de cancelación. De ellas destacan las siguientes:

- Publicación de datos personales no sensibles en blogs, foros o vídeos sin consentimiento previo del afectado y sin vulneración del deber de secreto.

- Publicación de datos personales (incluyendo vídeos) sin consentimiento previo del afectado, cuando existen indicios de vulneración del deber de secreto para la obtención de los datos publicados.

- Publicación de datos personales de especial sensibilidad (incluyendo vídeos) sin consentimiento del afectado, por ejemplo, el listado de personas pertenecientes a una congregación religiosa (PS/00337/2011).

En cuanto al titular de la página o prestador de servicios, la posible responsabilidad puede producirse en los siguientes supuestos:

- Páginas cuyo objeto está relacionado con la gestión de datos de especial sensibilidad, circunstancia que requiere del titular una especial diligencia. Entre otros cabe destacar los siguientes casos:

  - página destinada a menores que no realiza comprobación de la edad al obtener los datos (PS/00468/2009).

  - páginas de inserción voluntaria de imágenes de menores (PS/00023/2010).

  - página de contacto gay en la que no se encuentra controlada la identidad de quien inserta anuncios (PS/00280/2010).

- Requerimiento de la Agencia para que retire un contenido que no se ha hecho efectivo.

Debe destacarse que la Agencia no considera aplicable la "excepción empresarial" en la puesta a disposición en páginas de Internet de la identidad de un profesional para que se realicen valoraciones por terceros, estimándose las pretensiones del titular de los datos ejerciendo los derechos de oposición o cancelación (TD/01248/2011).

No obstante, el afectado puede tener la obligación de soportar la inserción de los datos en el caso de que tenga relevancia pública o existan razones justificadas.

c) *Medidas de seguridad.*

En materia de medidas de seguridad durante el año 2011 se han planteado supuestos de divulgación indebida de datos como consecuencia de una vulneración de medidas de seguridad. Las principales categorías detectadas son las siguientes:

- Medidas de identificación y autenticación insuficientes, mal configuradas o mal implementadas como son:
  - Disponer de un código de usuario pero no de una clave para autenticar al usuario que accede al fichero.
  - Errores en la implementación del módulo de identificación y autenticación que permiten el acceso sin utilizar un código de usuario y clave válidos.
  - Utilización de códigos de usuario y claves por defecto (ej: PS/00650/2010).
- Errores en la configuración del servidor web.

Un error en la ubicación de un archivo o en la configuración de esas zonas de privacidad puede hacer que un fichero que debe ser accesible a una aplicación web (p.e. una base de datos) se encuentre accesible al público en general y sea descargado, impreso o indexado por un buscador (ej: PS/00465/2011).

- Acceso a datos del fichero mediante la modificación de los parámetros de una URL.

Un localizador uniforme de recursos, más comúnmente denominado URL (por sus siglas en inglés), es una secuencia de caracteres, de

acuerdo a un formato modélico y estándar, que se usa para nombrar recursos en Internet para su localización o identificación, como por ejemplo documentos textuales, imágenes, vídeos, presentaciones, presentaciones digitales, etc. En el caso de que la aplicación web no imponga ningún tipo de filtro a las solicitudes, puede suceder que un tercero, sin necesidad de haberse autenticado ante el sistema pueda acceder a la información.

En algunos casos la aplicación web filtra las solicitudes descartando aquellas que no provienen de un usuario autenticado pero una vez verifica ese extremo, responde a sus solicitudes cualesquiera que estas sean. Para evitarlo es necesaria la implementación de un segundo filtro que descarte las solicitudes de información que proporcionen datos ajenos al perfil del usuario autenticado. (ej: PS/00459/2008).

- Hacking.

En este tipo de ataques el responsable del fichero es exonerado de responsabilidad únicamente en los supuestos en que, a pesar de la existencia de medidas de seguridad adecuadas, el intruso, utilizando sus conocimientos sobre las vulnerabilidades potenciales o conocidas de los distintos programas y herramientas específicas de hacking, consigue sortear un conjunto de medidas de seguridad que además de existir, están correctamente configuradas (E/02257/2011).

d) *Bases de datos ilegales*.

La AEPD tiene entre sus principales objetivos evitar la creación y comercialización de bases de datos que no se ajusten a las previsiones de la normativa de protección de datos.

Durante 2011 una empresa ya sancionada ha mantenido el tratamiento de los datos registrados en un fichero que se refiere a 36 millones de españoles cuya inmovilización declaró la AEPD y ha continuado desarrollando su actividad de cesión a terceros con fines lucrativos. Asimismo, ha realizado diversas acciones para que pudiera mantenerse el desarrollo de la actividad de prestación de servicios que constituye su objeto y el acceso al fichero por parte de terceros mediante un enlace habilitado en otra página Web, circunstancia que ha sido objeto de un nuevo procedimiento sancionador del que han derivado importantes sanciones (PS/146/2011).

C. LA SEGURIDAD JURÍDICA COMO OBJETIVO PRIMORDIAL

La AEPD ha continuado trabajando en el objetivo de contribuir a la 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, como es la LOPD, con las regulaciones sectoriales.

En el año 2011 fueron informadas 110 disposiciones de carácter general, lo que supone un máximo en el número de disposiciones sujetas a informe, dado que hasta ahora la cifra máxima correspondía a 2009, con un total de 100 proyectos informados. Entre las disposiciones sobre las que la Agencia ha emitido su parecer cabe hacer referencia a las siguientes:

- El Anteproyecto de Ley por la que se modifica la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

- El Anteproyecto de Ley de Supervisión de los Seguros Privados.

- El Anteproyecto de Ley por la que se modifica la Ley Orgánica 7/2006, de 21 de noviembre, de Protección de la Salud y Lucha contra el Dopaje en el Deporte y el Anteproyecto de Ley Orgánica complementaria de la misma.

- El Anteproyecto de Ley Integral para la igualdad de trato y la no discriminación.

- El Anteproyecto del Ley por la que se modifica la Ley 42/1997, de 14 de noviembre, ordenadora de la Inspección de Trabajo y Seguridad Social.

- El Proyecto de Real Decreto por el que se regula el procedimiento común para el acceso a documentos conservados en archivos de la Administración General del Estado.

- El Proyecto de Real decreto por el que se desarrolla la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.

- El Proyecto de Real Decreto por el que se regula el Reglamento del Registro de Entidades Religiosas y la declaración de notorio arraigo en España.

- El Proyecto de Real Decreto por el que se dispone la formación de los censos de población y viviendas de 2011.

- El Proyecto de Orden por la que se dictan las instrucciones para la formación de los censos de población y viviendas del año 2011.

- El Proyecto de Orden por la que se regula el tablón edictal de la Seguridad Social.

- El Proyecto de Orden por la que se regula el tablón edictal de Resoluciones de Extranjería.

- El Proyecto de Real decreto por el que se aprueba el Reglamento de desarrollo de la Ley 19/1988, de 12 de julio, de Auditoría de Cuentas.

- El Proyecto de Real Decreto por el 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.

- El Proyecto de Real decreto por el que se establece el marco para la implantación de los sistemas de transporte inteligentes en el sector del transporte por carretera y para las interfaces con otros medios de transporte.

- El Proyecto de Real Decreto por el que se establece el procedimiento de aplicación de la escala conjunta de deducciones a la facturación mensual de cada oficina de farmacia.

- El Proyecto de Orden por la que se regula el Registro Electrónico de Apoderamientos.

- Diversas disposiciones de creación de ficheros de la práctica totalidad de los Departamentos Ministeriales, 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 2011 se han dictado 222 sentencias por la Sala de lo contencioso-administrativo de la Audiencia Nacional y 33 por la del Tribunal Supremo.

En cuanto a las **Sentencias de la Audiencia Nacional**:

- 63 fueron desestimatorias de los recursos formulados contra resoluciones de la Agencia (que quedaron plenamente confirmadas) (28%).

- 90 estimaron parcialmente los recursos (41%).

- 52 estimaron íntegramente las pretensiones anulatorias de las resoluciones de la Agencia (23%).

- 17 inadmitieron los recursos interpuestos contra resoluciones de la Agencia (8%).

Es preciso en este punto clarificar que de las 90 sentencias parcialmente estimatorias dictadas en el año 2011, 80 lo han sido como consecuencia de la aplicación retroactiva del nuevo régimen sancionador de la LOPD establecido por la disposición adicional quincuagésima sexta de la Ley 2/2011, de 4 de marzo, de Economía Sostenible.

En efecto, la entrada en vigor de esta reforma ha conducido a que la Audiencia Nacional haya apreciado que concurrían los requisitos legalmente exigidos para que procediera su aplicación retroactiva de conformidad con lo establecido en aplicación del artículo 128.1 de la Ley 30/1992. Ello ha implicado que, si bien la Sala de la Audiencia Nacional ha considerado que las resoluciones de la Agencia son conformes a derecho en lo que se refiere al fondo del asunto, procedía rebajar la sanción impuesta en aplicación de dichos criterios.

Así, por ejemplo, en 61 sentencias, la estimación parcial consistió en rebajar el importe de la sanción impuesta desde 60.000 a 40.000 euros, como consecuencia de la rebaja de la cuantía inferior de las sanciones correspondientes a la comisión de infracciones graves establecida en la Ley 2/2011. Del mismo modo, las restantes sentencias suponen la aplicación retroactiva de los criterios de atenuación contenidos en el nuevo artículo 45.5 de la LOPD, la rebaja derivada del hecho de la tipificación de la cesión de datos no especialmente protegidos como infracción grave (frente a su carácter muy grave en el régimen anterior), la rebaja proporcional de las cuantías de la sanción como consecuencia de la modificación de los límites mínimo y máximo establecidos en la Ley o la apreciación de los criterios para reemplazar la sanción impuesta por el apercibimiento al que se refiere el nuevo artículo 45.6 de la LOPD.

En resumen, si bien de las cifras anteriormente señaladas pudiera parecer desprenderse que los criterios de las resoluciones de la Agencia no han sido mantenidos en sede jurisdiccional en un gran número de casos, lo cierto es que la confirmación de los criterios de la Agencia en cuanto al fondo del asunto ha sido exactamente la misma que en el año 2010 (ascendiendo a un 72% el total de las sentencias de inadmisión, desestimatorias, y estimatorias parciales causadas por a la aplicación retroactiva de la reforma operada por la Ley de Economía Sostenible).

En relación con los sectores de actividad a los que afectan las sentencias dictadas adquiere especial peso el sector de las telecomunicaciones, al que se refieren 64 de ellas (un 29%, con un incremento del 31% respecto a 2009), siendo también muy notable el peso de los recursos interpuestos por particulares (un incremento del 39%), bien contra resoluciones desestimatorias de tutelas planteadas ante la Agencia, bien contra resoluciones de archivo de actuaciones, si bien en este caso la Audiencia Nacional suele declarar la inadmisibilidad del recurso.

Por su parte, disminuye el número de recursos relativos al sector financiero (en más de un 55%, para representar ahora sólo un 13% del total) y se mantiene el peso de los recursos interpuestos por entidades del sector energético y de suministro de agua y por sindicatos y asociaciones profesionales.

Al propio tiempo, 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), así como los de entidades dedicadas a la publicidad y prospección comercial.

En cuanto a las materias, son significativas las referidas a la inclusión de datos inexactos en ficheros de solvencia patrimonial y crédito o relacionadas 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 analizadas en las sentencias de la Audiencia Nacional cabe destacar las siguientes cuestiones:

- En lo que respecta al ámbito de aplicación de las normas de protección de datos, la SAN de 25 de marzo de 2011 considera sujetos a dicha normativa y a las potestades de la Agencia los tratamientos llevados a cabo por el Ministerio Fiscal.

- Por su parte, la SAN de 9 de junio de 2011, referida al ejercicio por el consejero delegado de una entidad del derecho de oposición en relación con información publicada en Internet sobre la empresa, pone de manifiesto la inaplicación de la LOPD a las personas jurídicas.

- En cuanto al concepto de dato de carácter personal, la SAN de 15 de enero de 2011 considera como tales las direcciones de correo electrónico. Por su parte, la SAN de 1 de septiembre, a la que se hará referencia en otros lugares, considera dato de carácter personal la dirección IP.

- Son especialmente relevantes las sentencias que analizan la colisión del derecho a la protección de datos personales con otros derechos fundamentales.

- Así, en cuanto a la libertad de información, debe hacerse especial mención de la SAN de 29 de septiembre, en que la Audiencia, apartándose del criterio previamente mantenido en este mismo caso, considera conforme a la LOPD la publicación en prensa de fotografías referidas a una víctima de los atentados del 11 de marzo de 2004, al considerar tal información relevante a los efectos de la información facilitada. Por otra parte, la SAN de 24 de febrero de 2011 considera que no procede la aplicación de las normas de protección de datos cuando la información se refiere a meros rumores y se hace constar esta circunstancia.

- También se ha considerado prevalente el derecho a la libertad sindical sobre el derecho a la protección de datos en los supuestos de publicación de información relevante para los trabajadores y limitada al propio ámbito laboral en la

SAN de 20 de octubre de 2011, referida a la publicación de ayudas de acción social.

- En relación con el principio de conservación vinculada a la finalidad, la SAN de 17 de marzo de 2011 señala que los datos del tomador de un seguro deben ser objeto de bloqueo al resolverse el contrato y no utilizarse en el futuro.

- En el marco de la legitimación para el tratamiento, la Audiencia Nacional ha considerado conformes a la LOPD la cesión por un promotor inmobiliario a una compañía de comercialización eléctrica de los datos de un comprador a fin de que por la misma se proceda al suministro (SAN de 3 de marzo de 2011), o la cesión de datos a las Fuerzas y Cuerpos de Seguridad de la información de las mismas sin autorización judicial, al amparo del deber de colaboración previsto en la Ley Orgánica de Fuerzas y Cuerpos de Seguridad (SAN de 17 de noviembre de 2011).

- Por el contrario, se ha considerado que no existe legitimación para el tratamiento consistente en el envío a un trabajador de un correo electrónico por una central sindical, constando previamente su oposición a recibir estos envíos (SAN de 16 de diciembre de 2011), la recogida de datos de los buzones de correo existentes en una finca con fines de realizar campañas publicitarias, al no ser esta la finalidad por la que se identifica al vecino en los mismos (SAN de 16 de diciembre de 2011) o la apertura a favor de un menor de una cuenta de ahorro por parte del centro de educación infantil en que se encuentra matriculado (SAN de 17 de febrero de 2011).

- Igualmente son cesiones contrarias a la LOPD la transmisión de créditos cuya existencia no

consta probada (SAN de 27 de diciembre de 2011), sin que resulte relevante que esta circunstancia no se dé en todos los supuestos que se habían indicado en la resolución recurrida (SAN de 2 de febrero de 2011).

- En este punto, resultan particularmente relevantes la SAN de 1 de septiembre de 2011, que considera contrario a la LOPD el rastreo de direcciones IP de los usuarios que comparten contenidos a través de redes "peer to peer", teniendo en cuenta la doctrina sentada en este punto por el TJUE, y la SAN de 20 de octubre de 2011, por la que se sanciona a un particular que puso a disposición de terceros en una plataforma de intercambio de videos un vídeo de contenido ofensivo hacia el denunciante, considerando lícito el hecho de que el proveedor de servicios de Internet facilitase a la Agencia los datos identificativos del titular de la dirección IP en el momento en que el vídeo fue subido a Internet.

- En cuanto al tratamiento de los datos relacionados con la salud, la SAN de 17 de noviembre de 2011 considera lícita la cesión por un determinado facultativo a una compañía aseguradora de los datos de salud referidos a enfermedades preexistentes a la celebración del contrato, de las que tenía conocimiento como anterior facultativo del asegurado. Asimismo, se ha considerado lícita la cesión de datos a la Seguridad Social por parte de un servicio de prevención a fin de que se resuelva la concurrencia o no de invalidez en el interesado (SAN de 6 de junio de 2011) o la aportación de la historia clínica del afectado en un juicio en que el mismo demanda al facultativo por una supuesta mala praxis (SAN de 16 de junio de 2011).

Por contra, se ha entendido que infringe la LOPD el acceso por el servicio de prevención de la matriz de un grupo a los datos de la historia clínica laboral de los trabajadores de una filial que tiene concertado otro servicio de prevención distinto (SAN de 6 de octubre de 2011).

- Como viene sucediendo en los últimos años, el mayor número de supuestos relacionados con la legitimación para el tratamiento se refiere a casos en los que una entidad ha procedido al tratamiento como consecuencia de un contrato cuya existencia es negada por el afectado. En relación con este punto son múltiples las sentencias de la Audiencia Nacional, pudiendo hacerse referencia a las siguientes:

- Partiendo del principio de que en estos casos la carga de la prueba recae sobre el responsable del fichero (SAN de 23 de diciembre de 2011), la SAN de 10 de diciembre de 2011 ha entendido que existían indicios suficientes de la existencia de un contrato en un supuesto de falsificación del Documento Nacional de Identidad cuya aparente veracidad ha sido comprobada, constando una cuenta corriente abierta por el suplantador a su nombre y con ese documento.

- Asimismo, la Audiencia Nacional ha apreciado la existencia de indicios a favor del contrato en los supuestos en los que el afectado ha procedido al pago de varias facturas (SAN de 3 de marzo de 2011), incluso durante un largo período de tiempo, aun cuando en el contrato no constaba su documento nacional de identidad (SAN de 4 de noviembre de 2011).

- Igualmente se ha considerado lícito el tratamiento al que se refiere la SAN de 10 de febrero de 2011, en que se aportó prueba testifical acre-

ditativa de que un determinado trabajador se encontraba presente y no se opuso a que sus datos fueran facilitados a una entidad de crédito para la apertura de una cuenta.

- Por contra, la Audiencia Nacional ha apreciado la inexistencia de legitimación para el tratamiento en supuestos de suplantación de personalidad en que no se solicitó por el responsable el Documento Nacional de Identidad y la firma plasmada en el contrato no coincide con la del denunciante (tres SSAN de 27 de enero de 2011 y SAN de 24 de febrero de 2011) o los supuestos en que una vez celebrado el contrato telefónicamente no se verifican su existencia (SAN de 6 de octubre de 2011, en que los datos fueron facilitados por un familiar del afectado) o se intentó una sola vez la verificación del mismo pero a falta de respuesta se entendió celebrado el contrato igualmente (SAN de 1 de abril de 2011), considerando expresamente que en materia de contratación telefónica deberá aplicarse lo dispuesto en la Ley 7/1998, de 13 de abril, sobre Condiciones Generales de Contratación (SAN de 3 de marzo de 2011).

- Tampoco existen indicios suficientes de la existencia de contrato cuando no consta consumo ni facturación en un período prolongado de tiempo anterior a la denuncia (SAN de 17 de febrero de 2011) o se solicitó inmediatamente la retirada del servicio una vez comenzado (SAN de 24 de febrero de 2011). Incluso se entiende que no existen indicios de contrato cuando se procedió al pago de los primeros recibos, procediéndose inmediatamente a reclamar la inexistencia del contrato (SAN de 11 de noviembre de 2011).

- Por último, la SAN de 23 de junio de 2011 establece el principio de que si el responsable alega la existencia de un engaño deberá acreditar que ha desarrollado una conducta suficientemente diligente, indicando a su vez la SAN de 1 de abril de 2011 que la responsabilidad en los supuestos que se vienen analizando puede recaer en el agente contratado por el responsable del fichero.

- En lo que afecta al ejercicio de los derechos, y con carácter general, la SAN de 16 de diciembre de 2011 señala que la AEPD no está obligada a la apertura de un procedimiento sancionador en caso de que no sean atendidos por el responsable, pudiendo tramitar el procedimiento de tutela de derecho. Además, cabe entender atendido ejercicio en caso de que el responsable aporte indicios de que así se ha producido (SAN de 30 de junio de 2011, en que el responsable aportaba el acuse de recibo de una comunicación al afectado, aun cuando no quedase lógicamente acreditado su contenido).

- En cuanto al derecho de acceso, las SSAN de 16 de junio y 30 de junio de 2011 consideran que el derecho no se extiende a los posibles usuarios que acceden a los datos (en el segundo de los supuestos, evaluadores de una ANECA).

- Por lo que respecta al derecho de cancelación, la SAN de 29 de abril de 2011 impone la cancelación de los datos relacionados con la ejecución de un contrato en el momento de su resolución, en que sólo podrán emplearse para el cumplimiento de obligaciones derivadas del propio contrato, tales como el abono de recibos pendientes, pudiendo además la cancelación no referirse directamente a datos concretos sino a su uso para determinadas finalidades -como por ejemplo las de remisión de publicidad- (SAN de 8 de abril de 2011).

■ En relación con el derecho de oposición, la SAN de 16 de junio de 2011 señala que no procede su ejercicio en relación con las actas de plenos municipales.

■ En el ámbito del cumplimiento del deber de seguridad, la SAN de 14 de noviembre de 2011 ha indicado que para que proceda por la AEPD la imputación del incumplimiento deberá especificarse la medida infringida.

■ En cuanto a la vulneración del deber de secreto, la SAN de 12 de diciembre de 2011 entiende que se produce la infracción cuando una entidad realiza llamadas insistentes y reiteradas a familiares y compañeros de trabajo de su deudor para indicar la existencia y cuantía de la deuda.

■ Sin embargo, la Audiencia Nacional considera que no se ha vulnerado el deber de secreto cuando una entidad revela a sus empleados la información referente al cumplimiento de objetivos por parte de cada uno de ellos (SAN de 8 de julio de 2011) o cuando se aportan a un interesado en un procedimiento administrativo datos que habían sido a su vez aportados por otro interesado al efectuar alegaciones (SAN de 29 de julio de 2011).

■ En relación con los ficheros de solvencia patrimonial y crédito han sido muy numerosas las sentencias dictadas a lo largo de 2011, debiendo hacer referencia en primer lugar a las relativas al cumplimiento de los requisitos que deben darse para la inclusión de una determinada deuda en el fichero:

■ En este punto, la SAN de 10 de marzo de 2011 considera que es posible la inclusión de deudas respecto de las que existe una reclamación promovida por el acreedor. Igualmente, la SAN de 16 de diciembre de 2011considera que es posible mantener en el fichero una deuda sobre la que existía un laudo arbitral referido a su existencia, constando que el acreedor no tenía conocimiento del mismo en el momento de la denuncia.

■ Por el contrario, no deberá mantenerse en el fichero una deuda contra cuya existencia existe una sentencia judicial (SSAN de 17 de febrero y 8 de abril de 2011), señalando la última de las sentencias citadas que el requisito de que la deuda sea cierta sigue siendo exigible tras la STS de 15 de julio de 2010.

■ En todo caso, la SAN de 28 de noviembre de 2011 señala que la deuda incluida en el fichero debe corresponderse con la pendiente de pago, no siendo posible la inclusión de una deuda distinta, ya pagada, pero de menor cuantía que una efectivamente pendiente de pago, siendo irrelevante cuál sea la cuantía para apreciar la existencia de una infracción (en la SAN de 2 de diciembre de 2011 se analiza un supuesto en que la cuantía era de un céntimo de euro).

■ Han sido también varios los supuestos en los que se ha indicado que no resultaba imputable la entidad acreedora cuando facilitó a la responsable del fichero común el dato del número de pasaporte de la deudora y aquella entidad lo asocio con un NIF al añadirle una letra (SSAN de 4 y 25 de noviembre de 2011). No obstante, la acreedora responde en los supuestos en que omitió involuntariamente la letra del NIF o NIE del deudor (SAN de 19 de mayo de 2011).

■ Han sido muy numerosas las sentencias relacionadas con el requisito de requerimiento de

pago al deudor. En este sentido, la SAN de 11 de noviembre de 2011 reitera que corresponderá al acreedor la carga de la prueba de la realización del requerimiento de pago. Así, la Audiencia Nacional ha considerado que no resulta suficiente la referencia a llamadas efectuadas al deudor respecto de las que no hay prueba de su realización, la alegación de que se han remitido cartas de las que no consta siquiera su envío (SAN de 15 de septiembre de 2011), la mera referencia a que la carta se ha enviado según el sistema interno de información del acreedor (SAN de 30 de septiembre de 2011) o la mera referencia a la existencia de facturas impagadas (SAN de 4 de marzo de 2011). Por el contrario, sí se ha considerado suficiente indicio del requerimiento el hecho de que el deudor en fecha inmediatamente posterior a aquélla en que se supone realizado el envío, se puso en contacto con el acreedor para regularizar su situación (SAN de 28 de octubre de 2011).

- También en relación con el requerimiento debe hacerse referencia a la SAN de 3 de junio de 2011, que señala como razonamiento obiter dictum que podría no ser contrario a la LOPD el requerimiento remitido dentro de los diez días siguientes al pago de la obligación por el deudor, dado que éste es el plazo legalmente previsto para la cancelación de los datos. También deben tenerse en cuenta las SSAN de 10 de marzo y 27 de octubre de 2011, que entienden que será necesario únicamente un requerimiento por el primer incumplimiento en caso de deudas de vencimiento periódico.

- También son numerosas las sentencias de la Audiencia Nacional relacionadas con la videovigilancia, indicándose, en primer lugar, que se encuentran sometidos a la LOPD los dispositivos que únicamente reproducen las imágenes en tiempo real (SAN de 2 de marzo de 2011). Además, si la finalidad es de videovigilancia no cabrá alegar que no se recaban datos personales sobre la base de que la imagen no es suficientemente nítida (SAN de 17 de noviembre de 2011). Asimismo, no resulta admisible la alegación de que el dispositivo no se ha puesto en funcionamiento si existen indicios de que pudiera estarlo en cualquier momento (SAN de 18 de marzo de 2011).

- En cuanto a los supuestos más habituales, la Audiencia se refiere a la vigilancia en comunidades de propietarios, considerando necesario que exista un acuerdo de la Junta (SAN de 18 de febrero de 2011) y que un vecino no podrá por sí solo instalar los dispositivos incluso sobre la base de desavenencias con otros vecinos que pudieran afectar a la integridad de su inmueble (SAN de 17 de junio de 2011), estando prohibida la grabación de zonas privativas por parte de la comunidad (SAN de 18 de febrero de 2011). No obstante, es posible la grabación por un vecino de su propia plaza de garaje si no se invaden las restante y se enmascaran las imágenes de los particulares (SAN de 11 de marzo de 2011).

- Se han declarado contrarios a la LOPD los supuestos de grabación de calles de una urbanización, al tratarse de vía pública (SAN de 20 de mayo de 2011), o la grabación mediante cámaras "DOMO" que permiten un movimiento de 360º en caso de que no se adopten medidas para impedir esa grabación (SAN de 12 de febrero de 2011).

- En el ámbito del marketing, la SAN de 14 de abril de 2011 considera cometida la infracción (en este caso del deber de información del origen de los datos) a la empresa que contrató la campaña y fijó los parámetros identificativos de sus destinatarios.

Por su parte, la SAN de 17 de enero de 2011 confirmó la sanción de la Agencia en un supuesto en que se había insertado el envío publicitario en la factura de un servicio habiendo previamente el interesado manifestado su oposición expresa a la recepción de publicidad.

- En lo referente a la remisión de comunicaciones comerciales no solicitadas si se trata de direcciones corporativas referidas a una persona física cuyo legal representante ha otorgado el consentimiento, la SAN de 27 de diciembre de 2011 entiende que los envíos serán lícitos en tanto no se revoque el consentimiento por un legítimo representante de la entidad.

- Por otra parte, la SAN de 16 de junio de 2011 otorga validez a la información facilitada por el remitente en relación con lo exigido por el artículo 22.1 de la LSSI si se efectúa una remisión a su web, en que se contienen las bases contractuales. Por su parte, la SAN de 15 de julio de 2011 no considera masivo el envío de tres comunicaciones en un plazo muy breve incluyendo en todas ellas la posibilidad del interesado de manifestar su voluntad de no recibir más comunicaciones, al generarse una suerte de apariencia de aceptación de la recepción de estos mensajes.

Por su parte, el Tribunal Supremo dictó un total de 33 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.

En relación con estos recursos, el **Tribunal Supremo**:

- Declaró en 14 sentencias no haber lugar a los recursos interpuestos contra sentencias que con-

firmaban las resoluciones de la Agencia, que quedaron así confirmadas.

- Declaró en 5 sentencias haber lugar a los recursos interpuestos contra sentencias que confirmaban las resoluciones de la Agencia, que quedaron así anuladas.

- Declaró en 12 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.

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

- En relación con el ámbito de aplicación y la competencia de la AEPD, resulta especialmente relevante la STS de 2 de diciembre de 2011, referida a los ficheros de los que son responsables los órganos judiciales (tanto de carácter gubernativo o administrativo como jurisdiccionales), indicando que los mismos se encuentran sometidos a lo dispuesto en la LOPD. No obstante, se señala que respecto de estos ficheros, y en virtud del principio de independencia del Poder Judicial, el órgano al que corresponderán las competencias de supervisión y control será el Consejo General del Poder Judicial.

- Por otra parte, la STS de 1 de julio de 2011 señala que no pueden considerarse sometidos a lo dispuesto en la LOPD los datos meramente valorativos que han sido incluidos en el cuerpo de una resolución administrativa (en este caso de un recurso contra la calificación de un registrador).

- En lo que respecta a los supuestos de conflicto de derechos, la STS de 18 de octubre de 2011 declara la prevalencia del derecho fundamental a la libertad de información en el supuesto de publicación por un medio de comunicación de los datos relativos a la sanción impuesta por un Ayuntamiento a un policía local.

- En cuanto a la titularidad pública o privada de los ficheros, la STS de 1 de marzo de 2011 indica que los ficheros de los colegios profesionales únicamente serán de titularidad pública cuando se encuentre directamente vinculados al ejercicio de potestades de derecho público, no siéndolo los restantes (en este caso el relativo a datos aparecidos en una revista del Colegio).

- En relación con los principios de calidad de datos han sido varias las sentencias que han analizado los requisitos exigibles para que proceda imponer al responsable una sanción por recogida fraudulenta de datos, delimitando el alcance del tipo sancionador, que implica una recogida de datos (STS de 27 de mayo de 2011) y los requisitos necesarios para que pueda apreciarse el carácter fraudulento de dicha recogida a través de la prueba indiciaria (STS de 25 de octubre de 2011). En este sentido, la STS de 2 de marzo de 2011 sí entiende que existe una recogida fraudulenta en un caso en que las firmas que aparecen en el contrato son manifiestamente distintas de las incluidas en los Documentos Nacionales de Identidad de los interesados.

- Por lo que respecta al tratamiento de datos de salud, la SAN de 23 de febrero de 2011 delimita los supuestos de responsabilidad en los casos de consultas privadas prestadas dentro de un establecimiento sanitario. Se trataba de un supuesto de documentación aparecida en la vía pública,

entendiéndose que sería el facultativo el responsable de la comisión de la infracción.

- También en relación con este tipo de datos, la STS de 11 de marzo de 2011 se refiere a un supuesto de ejercicio del derecho de acceso a los datos de un facultativo que reconoció al interesado para determinar la cuantía de la indemnización cuyo pago correspondía a una compañía de seguros, entendiendo el Tribunal que dicho derecho no incluye los datos relacionados con la aplicación por el facultativo de los baremos aplicados para determinar la cuantía de la indemnización.

- Por lo que respecta a los supuestos en que existe un encargado del tratamiento, la STS de 3 de junio de 2011 entiende que no se da esa relación en un supuesto en que un operador de telecomunicaciones facilitó, previo contrato a una agencia de seguros los datos de sus clientes para que dicha agencia, identificándose en nombre del operador, se limitase a ofrecer los productos de la entidad aseguradora de la que es agente, facilitando a la misma los datos de los clientes interesados en la firma de la póliza.

- En cuanto a otros supuestos de legitimación para las cesiones de datos de carácter personal, la STS de 5 de diciembre de 2011 ratifica el criterio sostenido por la AEPD y posteriormente incluido en la Ley 26/2006, de 17 de julio, de mediación de seguros y reaseguros privados, en cuya virtud es preciso el consentimiento del interesado para que un corredor de seguros pueda usar sus datos para suscribir una nueva póliza en la que aquél sea tomador.

- En relación con las cesiones deben traerse también a colación dos cuestiones relevantes analizadas por el Tribunal Supremo: por una parte, entiende el Tribunal en STS de 29 de marzo de 2011 que en caso de transmisión de un dato inexacto que, sin embargo, hubiera estado amparada por alguno de los supuestos establecidos en el artículo 11 si el dato hubiera sido exacto, la única vulneración producida será la del principio de calidad de datos. Por otra parte, entiende la STS de 4 de mayo de 2011 que la infracción en caso de comunicación ilícita de datos se entenderá producida en el mismo momento en que la cesión tenga lugar, por lo que la solicitud por el cesionario del consentimiento del afectado con posterioridad a la cesión resulta irrelevante a los efectos de valorar la existencia de la infracción.

- En lo que atañe al ejercicio del derecho de acceso, deben tenerse en cuenta las SSTS de 2 y 18 de febrero de 2011, 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 on-line a sus datos personales, entendiendo que la reclamación del afectado constituye un abuso del derecho.

- En cuanto a la aplicación de los criterios del artículo 45.5 de la LOPD, la STS de 27 de junio de 2011 recuerda que la aplicación de los criterios debe tomar en consideración los precedentes contenidos en resoluciones anteriores de la AEPD y sentencias de la propia Audiencia Nacional.

- Por último, la STS de 6 de mayo de 2011 reitera la licitud y validez de las pruebas recabadas por la AEPD en la fase de actuaciones previas.

Debe, por último, en este punto hacerse referencia a la importante sentencia dictada por el **Tribunal de Justicia de la Unión Europea**, de 24 de noviembre de 2011, por la que se resuelven las cuestiones prejudiciales planteadas por el Tribunal Supremo en el marco de los recursos interpuestos contra el Reglamento de desarrollo de la LOPD. La Sentencia da respuesta a las dos cuestiones planteadas en el siguiente sentido:

- El artículo 7, letra f), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, debe interpretarse en el sentido de que se opone a una normativa nacional que, para permitir el tratamiento de datos personales necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, exige, en el caso de que no exista consentimiento del interesado, no sólo que se respeten los derechos y libertades fundamentales de éste, sino además que dichos datos figuren en fuentes accesibles al público, excluyendo así forma categórica y generalizada todo tratamiento de datos que no figuren en tales fuentes.

- El artículo 7, letra f), de la Directiva 95/46 tiene efecto directo.

El artículo 7 f) de la Directiva establece que los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse, entre otros supuestos, si "es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva".

El Tribunal clarifica la interpretación aplicable de dicho artículo, considerando que será necesario realizar en cada caso concreto una ponderación para determinar si debe prevalecer el derecho del interesado o el interés legítimo de quien trata sus datos.

De este modo la sentencia precisa que el artículo 7 f) de la Directiva "establece dos requisitos acumulativos para que un tratamiento de datos personales sea lícito, a saber, por una parte, que ese tratamiento de datos personales sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, y, por otra parte, que no prevalezcan los derechos y libertades fundamentales del interesado", de forma que no es suficiente la mera existencia de un interés legítimo, sino que habrá de llevarse a cabo la ponderación de los derechos e intereses concurrentes en cada caso. En relación con la citada ponderación recuerda que "dependerá, en principio, de las circunstancias concretas del caso particular de que se trate y en cuyo marco la persona o institución que efectúe la ponderación deberá tener en cuenta la importancia de los derechos que los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea confieren al interesado".

Como consecuencia de la STJUE será necesario innovar en la metodología para decidir los casos en los que el interés legítimo del responsable legitime el tratamiento o la cesión de los datos personales sin necesidad de consentimiento del interesado. En efecto, la sentencia exige que, en cada caso concreto en que se alegue el citado interés legítimo, se lleve a cabo una ponderación específica de dicho interés u del interés o los derechos fundamentales del

propio afectado para determinar cuál resultará prevalente.

En dicha ponderación habrán de tenerse en cuenta, además, los principios de la normativa de protección de datos personales y, en particular, los de información a los afectados, calidad de los datos y proporcionalidad, como instrumentos básicos a la hora de inclinar la balanza a favor del responsable del tratamiento o del interesado.

De este modo, la necesaria ponderación de intereses y derechos excluirá las opciones que tiendan al automatismo en la aplicación de la LOPD.

Aún no correspondiendo al período analizado en esta Memoria, debe indicarse que el Tribunal Supremo, en sendas sentencias de 8 de febrero de 2012 por las que se resuelven los recursos en cuyo seno se plantearon las cuestiones prejudiciales resueltas por la anterior sentencia, ha declarado la nulidad del artículo 10.2 b) del RLOPD, confirmando la conformidad a derecho del artículo 10.2 a) del mismo.

Como novedad a destacar respecto de la **conservación de archivos históricos** en el año 2011 se autorizó la conservación íntegra de los datos relacionados con afiliados y representantes sindicales, con fines históricos, solicitada por la Confederación Sindical de La Unión General de Trabajadores de España, al cumplirse los requisitos legalmente establecidos (artículo 4.5 de la LOPD, artículo 9.2 del RLOPD, artículo 157 del RLOPD y artículos 49 y 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español).

Con carácter general, la LOPD establece que los datos personales deben ser cancelados cuando dejan de ser necesarios o pertinentes para la finalidad para la que fueron recabados. La normativa de protección de datos prevé, como excepción, el mantenimiento íntegro de determinados datos si se justifica la existencia de valores históricos, estadísticos o científicos de acuerdo con la legislación específica.

La Agencia Española de Protección de Datos ha considerado suficientemente motivadas las causas que justifican la declaración de concurrencia de valores históricos en el tratamiento de datos solicitada por esta organización sindical fundada en 1888, entendiendo asimismo adecuadas las medidas de seguridad que la Confederación ha implantado para garantizar el derecho de los afectados.

A. MEJORAR LA CONFIANZA CIUDADANA EN LA SEGURIDAD Y PRIVACIDAD EN INTERNET

Internet se ha convertido en una herramienta imprescindible en todos los ámbitos de la sociedad actual, pero se hace necesaria la adopción de medidas que permitan conciliar su expansión y funcionamiento cotidiano con el respeto a los derechos y a las normas de privacidad que rijan en ámbito europeo y, al mismo tiempo, disminuir los riesgos para la privacidad y la seguridad de la información que se manifiestan en la Red.

La expansión de Internet requiere la implantación de garantías eficaces para los ciudadanos que disminuyan la desconfianza existente en la seguridad y en la privacidad de Internet. Los datos de la encuesta del CIS sobre privacidad y protección de datos realizada a finales de 2009, reflejaban una alta desconfianza de los ciudadanos sobre la seguridad y privacidad de Internet. Entre otros indicadores, esta encuesta destacaba que un 56,6% de los ciudadanos españoles consideraban que Internet ofrece una seguridad y privacidad de los datos baja, y más del 70% cree que su uso favorece la intromisión en la vida privada.

La inquietud ciudadana sobre la seguridad en Internet se ha visto confirmada por la publicación en medios de comunicación de algunos casos relevantes de brechas y vulnerabilidades de la seguridad o el robo de identidades de usuarios. Entre ellos han destacado los casos de importantes corporaciones multinacionales o instituciones sobre las que la AEPD ha iniciado actuaciones previas de inspección.

Con motivo del Día Mundial de Internet, la Agencia hizo un llamamiento a las empresas y organizaciones que prestan servicios a través de Internet para que extremen la diligencia en la adopción de medidas de seguridad en la Red.

Esta iniciativa se ha complementado con la inclusión en la Web de la AEPD de un espacio específico con información práctica sobre el rastro de los datos personales en Internet, los riesgos asociados a los servicios en la Red, guías, recomendaciones y videos. En este apartado se explica el rastro que dejan los usuarios en Internet, contemplando los datos que se aportan voluntariamente al darse de alta en los servicios (redes sociales, portales de contactos o de compra on-line…), los que genera la navegación en Internet (cookies) o los que pueden publicarse en sitios web sin conocimiento de los usuarios. Por su parte, el capítulo sobre riesgos asociados a Internet abarca, entre otros, el correo web, los buscadores, los chats o la mensajería instantánea y, destacadamente, las redes sociales.

Los riesgos para la seguridad en Internet han abierto una reflexión sobre la conveniencia de que las brechas de seguridad sean notificadas a la autoridad de control y, en su caso, a los propios usuarios afectados. La reforma de la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas ha aportado novedades normativas en este ámbito, si bien limitada su exigencia a los proveedores de servicios de comunicaciones electrónicas disponibles al público. Entre ellas cabe destacar las siguientes:

- La definición de la violación de datos personales como una brecha de seguridad.
- La notificación, sin dilaciones, de la brecha de seguridad a una autoridad nacional competente.
- La notificación a los propios abonados o particulares afectados, sin dilaciones indebidas, cuando la brecha de seguridad pueda afectar

negativamente a su intimidad o a sus datos personales.

- La posibilidad de que la autoridad competente exija al proveedor de servicios que lleva a cabo la citada notificación si no la ha realizado, una vez evaluados sus efectos adversos.

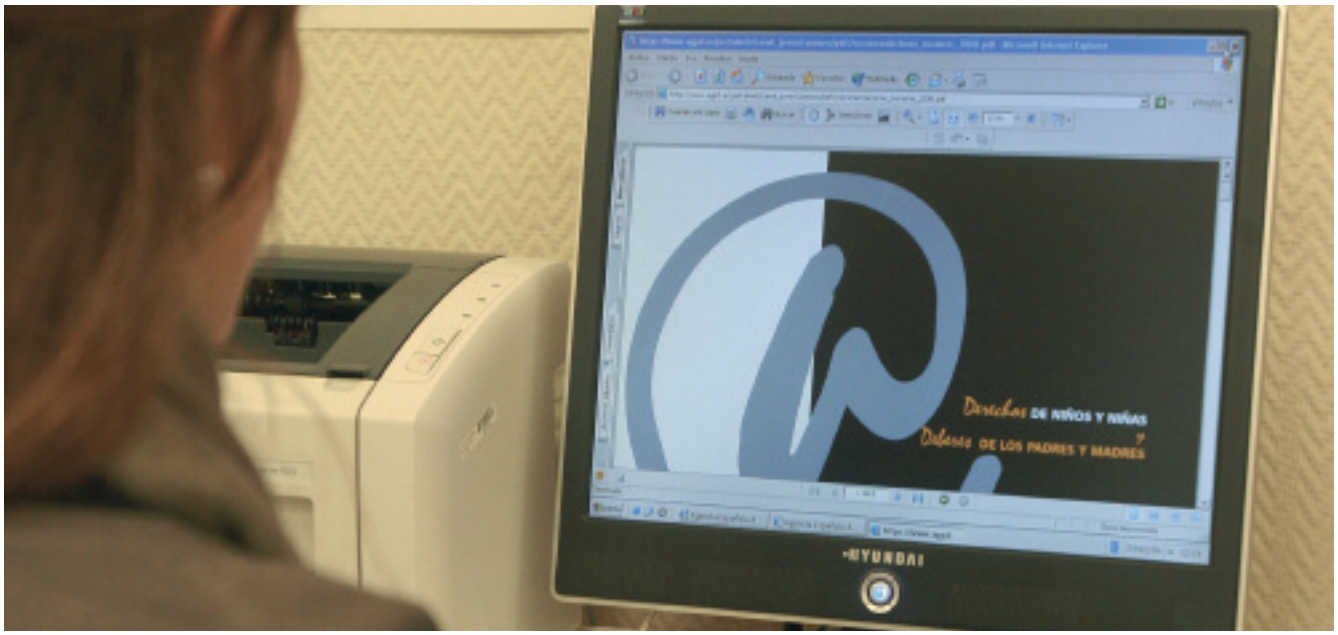
- La notificación a los abonados o particulares se exceptúa en que se haya acreditado la aplicación de medidas de protección tecnológica adecuadas.

- Los abonados o particulares deberán disponer de información sobre la naturaleza de la brecha de seguridad, puntos de contacto donde ampliarlas y recomendaciones para atenuar sus efectos adversos.

La sensibilidad del legislador comunitario sobre la importancia de notificar las brechas de seguridad ha llevado también a la Comisión Europea a incorporarla como una obligación general para los responsables que traten datos personales en la Propuesta de Reglamento General de Protección de Datos Personales cuya tramitación se ha iniciado en 2012.

Los aspectos básicos de la reforma han sido transpuestos en nuestro ordenamiento mediante el Real Decreto-Ley 13/2012, de 30 de marzo, que modifica la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, atribuyendo a la AEPD la competencia para recibir las notificaciones de las violaciones de protección de datos, así como para conocer sus consecuencias y las medidas adoptadas para evitarlas; evaluar la necesidad de notificarlas a los afectados o excepcionar la notificación por haberse adoptado las medidas de protección tecnológica pertinentes.

El Real Decreto-Ley contempla, asimismo, los supuestos en que debe efectuarse una notificación sin dilaciones indebidas a los abonados o particulares



por afectar negativamente la violación de datos a su intimidad.

De otro lado, el Real Decreto Ley 13/2012 modifica la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico incorporando mayores garantías para la privacidad respecto de la utilización de dispositivos de almacenamiento y recuperación de datos (cookies,…) en los terminales de los usuarios, modificando el sistema anteriormente vigente basado en la información al usuario sobre su utilización y el derecho de este a oponerse a ella (opt-out) a un nuevo régimen en el que se exige un consentimiento previo e informado del usuario (opt-in) que podría obtenerse, entre otras opciones, mediante una acción expresa en la configuración del navegador. Tales modificaciones inciden principalmente en las actividades publicitarias basadas en los hábitos de navegación de los usuarios de Internet.

B. EL "DERECHO AL OLVIDO" EN INTERNET: UNA NECESIDAD DE NUESTRO TIEMPO

Actualmente, la acción combinada de la informática y de las tecnologías de la comunicación han arrumbado las dos barreras que tradicionalmente contribuían a proteger la privacidad: la barrera del espacio y la barrera del tiempo.

Hoy en día es posible obtener información personal en cualquier momento, con independencia de la fecha en la que se haya generado o publicado el dato (no hay barreras temporales que protejan la privacidad) y es posible obtenerla desde cualquier lugar, con independencia de la mayor o menor lejanía geográfica (no hay barreras espaciales).

Además, el abaratamiento de los soportes de almacenamiento y de los costes de transmisión hace que tampoco sea un obstáculo el volumen de la información, ni el hecho de que se refiera a un gran número de individuos.

Los motores de búsqueda se han convertido en herramienta esencial en la vida diaria de todos los usuarios de Internet. Sin ellos, sería enormemente difícil acceder a la información existente en la red. Pero, al mismo tiempo, su potencial resulta cada vez más problemático, por cuanto permiten localizar instantáneamente, salvando cualquier barrera de tiempo y espacio, información de todo tipo relativa a una persona. Las capacidades de recuperación y agregación de los motores de búsqueda pueden ocasionar considerables perjuicios a los individuos, tanto en su vida personal como en sus relaciones sociales.

Una de las cuestiones más importantes del debate actual sobre la privacidad en la red es el relacionado con lo que se ha dado en llamar el "derecho al olvido". Estamos ante una de las cuestiones más relevantes del impacto de las nuevas tecnologías sobre la vida personal.

En la historia de la humanidad lo normal ha sido siempre que las cosas se olviden y lo excepcional que se recuerden. Guardar la información y transmitirla siempre ha sido caro y, por tanto, algo limitado. Pero en la era digital esa relación se ha invertido: grabar, guardar, almacenar información es muy barato y, por contra, borrar información exige dedicación, tiempo y dinero.

Hoy, la información personal se almacena masivamente y es fácilmente accesible para cualquiera con sólo tener una terminal de acceso a Internet. Datos o informaciones recientes o lejanas, procedentes de

las fuentes más diversas, están al alcance de cualquiera y para cualquier finalidad.

El debate está abierto y la solución exige la participación de todos los implicados.

En primer lugar, los ciudadanos, en cuanto usuarios de la red deben tomar decisiones conscientes y responsables sobre la información y los datos personales que incorpora a la Red, teniendo en cuenta las dificultades prácticas para ejercer un control efectivo sobre esa información.

En segundo lugar, los administradores de las páginas web deben también tomar decisiones responsables sobre qué información permiten que sea rastreada e indexada por los motores de búsqueda y qué información quieren que sea accesible sólo directamente desde la web, pero resulte opaca para los buscadores.

Es preciso, por otra parte, llevar a cabo una reflexión profunda sobre el contenido y alcance del principio de publicidad de los actos y resoluciones administrativas. Clarificar y precisar hasta dónde llega el mandato de publicidad en la era digital.

En esta misma línea, es necesaria una reflexión pausada en el ámbito de los medios escritos de comunicación sobre la configuración de las hemerotecas digitales, sobre si su contenido ha de ser sólo accesible desde la propia página web o si, como ahora sucede en muchas casos, su contenido puede ser íntegramente indexable por los buscadores y, como consecuencia de ello, al introducir el nombre y los apellidos de una persona, traer al presente cualquier noticia publicada hace varios años.

Por último, es obligado que los responsables de las páginas web y de los motores de búsqueda atiendan las demandas de los ciudadanos cuando ejerzan los derechos que les reconoce la LOPD. Sea el derecho a cancelar sus datos personales cuando han sido publicados sin su consentimiento y sin cobertura legal, o bien el derecho de oponerse a que, aún cuando su publicación originaria fuese legal, sean objeto de tratamientos posteriores que comportan una multiplicación de esa publicidad, como sucede con los buscadores.

La demanda de los ciudadanos en el ejercicio de estos derechos se consolida y amplia año a año. De las tres solicitudes iniciales de tutela recibidas en la Agencia en 2007 se ha pasado a las 160 reclamaciones de 2011, que casi duplican las de año anterior.

La AEPD da respuesta a esta demanda ciudadana a través de los derechos de cancelación y oposición. Este último se aplica para evitar la indexación de datos personales por los motores de búsqueda valorando siempre, en cada caso concreto, la incidencia que pueda tener en los derechos del ciudadano, atendiendo a sus circunstancias especificas. Las resoluciones de la Agencia tutelando estos derechos son en general atendidas por los responsables de las páginas Web, pero no por el prestador del servicio de búsqueda mayoritario que las ha impugnado sistemáticamente ante la jurisdicción contencioso-administrativa. Previamente a la resolución de estos recursos la Audiencia Nacional ha planteado una cuestión prejudicial ante el Tribunal de Justicia de la Unión Europea (Auto de 27 de febrero de 2012). En ella se suscitan las cuestiones esenciales sobre la garantía de estos derechos en cuanto a la ley aplicable, la responsabilidad de los buscadores y titulares de sitios web, las competencias de las Autoridades de protección de datos y la posibilidad de evitar la indexación de la información personal.

Entre las cuestiones planteadas ante el TJUE destacan las relativas a que "la Directiva 95/46/CE se dictó en un momento en que los buscadores de Internet, o no existían o eran muy incipientes, por lo que las normas de conflicto no están, en principio, diseñadas para afrontar los peligros que han sobrevenido con los cambios tecnológicos. Pero con la aprobación sobrevenida de la Carta Europea de Derechos Fundamentales, que según dispone el art. 6 del TUE tiene el mismo valor jurídico que los Tratados, se reconoce el derecho fundamental a la protección de datos de carácter personal (art. 8 de la Carta), por lo que parece razonable acudir a una interpretación y aplicación de las normas comunitarias que permita una tutela eficaz de este derecho, pues la Carta persigue, según su exposición de motivos, "reforzar la protección de los derechos fundamentales a tenor de la evolución de la sociedad, del progreso social y de los avances científicos y tecnológicos".

Y también se suscita si "sostener que la indexación de datos procedentes de páginas web situadas en España, en relación con una información publicada en España, en base a una norma legal española, que afecta a datos de un ciudadano español y que fundamentalmente puede tener una repercusión negativa, a juicio del afectado, en su entorno personal y social sito en España (centro de intereses), tenga que defender la tutela de su derecho a la protección de datos en EEUU, por ser el lugar que el gestor del buscador ha elegido para ubicar los medios técnicos, colocaría a los afectados en una situación de especial vulnerabilidad e impediría o dificultaría enormemente la tutela eficaz de este derecho que podría resultar incompatible con el espíritu y finalidad que inspira la Directiva y, sobre todo, con una tutela eficaz de un derecho fundamental contenido en la Carta Europea de Derechos Fundamentales".

Finalmente cabe mencionar que el reconocimiento de un derecho frente a la difusión universal y permanente de la información personal en Internet, cuando pueda resultar lesiva para los derechos fundamentales de los ciudadanos, se ha confirmado en la propuesta de Reglamento General de Protección de datos de la Comisión Europea, que ya ha iniciado su tramitación legislativa, bajo la denominación genérica de "derecho al olvido", aunque manteniendo su conexión con los tradicionales derechos de cancelación y oposición.

C. EL "CLOUD COMPUTING": UN NUEVO PARADIGMA

La prestación de servicios de "cloud computing" en sus distintas tipologías de nube (pública, privada, híbrida…) y de modalidades de servicios (Infraestructura como servicio, Plataforma como servicio y Software como servicio) ha venido a modificar las relaciones tradicionales entre los clientes -responsables del tratamiento de los datos- y los encargados del tratamiento -prestadores de servicios de "cloud computing"-.

El cambio de paradigma en aquellas relaciones determinó que la AEPD iniciara un proceso de análisis sobre sus implicaciones y sobre las modulaciones necesarias en la aplicación de la normativa de protección de datos para garantizar los derechos de los ciudadanos.

Con este objetivo la Agencia inició una serie de reuniones con los principales agentes afectados que posteriormente fue ampliada al público en general a través de una consulta pública a fin de conocer

con mayor amplitud las experiencias, opiniones y condicionamientos, desde la perspectiva de la protección de datos, de prestadores y usuarios de servicios de "cloud computing". La consulta comprende una amplia variedad de cuestiones entre los que destacan los relativos a la legislación aplicable, las garantías que deben exigirse en la contratación de los mismos o su impacto en la subcontratación de servicios y en las transferencias internaciones de datos.

Paralelamente la AEPD ha intervenido activamente en la elaboración de una opinión del Grupo de Trabajo del artículo 29 que recoja un criterio armonizado de las Autoridades de protección de datos en la Unión Europea sobre esta modalidad de servicios, consciente de que se trata de un fenómeno que aconseja una respuesta común a nivel europeo.

No obstante, ante las dudas que ha suscitado a los prestadores de estos servicios y a sus clientes actuales o potenciales, la Agencia convocó una Sesión Anual Abierta en 2012 en la que se formuló un avance de sus criterios sobre este tema.

D. LOS RIESGOS DE LA GEOLOCALIZACIÓN

La proliferación de dispositivos móviles inteligentes ha supuesto la aparición de multitud de servicios que permiten localizar a sus titulares, que utilizan sus teléfonos móviles para conocer la previsión meteorológica, encontrar una calle, localizar a amigos o buscar un determinado servicio en un lugar específico. La tecnología utilizada en estos terminales móviles, que están vinculados estrechamente a las personas, permite a los proveedores de servicios de geolocalización disponer de detalles de hábitos y pautas de comportamiento del propietario de estos dispositivos y establecer perfiles exhaustivos, dado que la tecnología de los aparatos permite un control constante de los datos de localización mediante la captación de señales de estaciones de base y de puntos de acceso Wi-Fi.

Ante la necesidad de analizar este fenómeno y aportar criterios para la protección de los datos personales, la AEPD participó, junto a otras entidades europeas en la elaboración, en el seno del GT 29 de un Dictamen sobre los servicios de geolocalización que se aprobó en mayo de 2011 (WP 185). El propósito de este Dictamen es clarificar el marco legal aplicable a los servicios de geolocalización disponibles en, o generados por, dispositivos móviles inteligentes, es decir, dispositivos que pueden conectarse a Internet y disponen de sensores de localización, tales como GPS. El Dictamen no incluye, al considerarse que ampliaba excesivamente el ámbito de análisis, otros sistemas de geolocalización, como pueden ser los conocidos navegadores para automóviles, los sistemas automáticos de pago de peaje o las aplicaciones de geolocalización que se están generalizando en el terreno de las cámaras digitales.

Dicho documento se concentra en los dispositivos móviles inteligentes, y muy en particular en los teléfonos móviles, ante el hecho de que éstos pueden ser asociados de forma casi indisoluble a una persona específica. La mayoría de las personas tiende a llevar siempre encima sus móviles y es poco frecuente que los presten a otras personas. Ello supone que localizar la posición, o los patrones de movimiento, de un dispositivo móvil equivale, en la práctica, a determinar los de su propietario.

El Dictamen describe las diversas tecnologías empleadas y evalúa los correspondientes riesgos para

la privacidad. Sobre esta valoración, establece una serie de conclusiones sobre la aplicación de preceptos legales clave (legitimación, información, conservación de los datos,…) a los diferentes responsables que participan en los procesos de geolocalización.

En este sentido, se distingue el papel que como responsables de tratamiento pueden tener los proveedores de infraestructuras de geolocalización, fabricantes de dispositivos móviles inteligentes y desarrolladores de aplicaciones basadas en la geolocalización y, en concreto, se establece que los distintos responsables del tratamiento de información de geolocalización procedente de dispositivos móviles deben permitir a sus clientes acceder a sus datos de localización en un formato legible y que los usuarios puedan rectificarlos o borrarlos sin recoger datos personales excesivos. Asimismo, también debe facilitarse a los interesados los derechos de acceso, rectificación y borrado de posibles perfiles basados en datos de localización.

Destaca igualmente el Dictamen el papel central que la información al usuario y el consentimiento previo y específico de éste deben tener en el contexto de los servicios de geolocalización, estableciendo que esta información deberá ser clara, completa y comprensible para un público amplio y no técnico y accesible de forma permanente y fácil. Para las autoridades europeas de protección de datos el consentimiento para la activación de este tipo de servicios no puede obtenerse mediante condiciones generales, debiendo por defecto estar desconectados. Los interesados, a los que debería recordárseles la existencia de su consentimiento al menos una vez al año, deben poder retirar su consentimiento de forma sencilla sin consecuencias negativas para el uso del producto.

Finalmente, en cuanto a la geolocalización en el entorno laboral, se establece que los empresarios sólo podrán adoptar esta tecnología cuando sea una necesidad demostrable para un fin legítimo y el mismo objetivo no pueda conseguirse por medios menos intrusivos.

E. AVANCES EN EL RECONOCIMIENTO FACIAL

En los últimos años ha habido un rápido incremento en la disponibilidad y la precisión de la tecnología de reconocimiento facial. Esta tecnología ha sido integrada en servicios online y dispositivos móviles que permiten a los usuarios capturar imágenes y vincularlas en tiempo real a una amplia variedad de servicios online. Como resultado, los usuarios pueden tomar fotografías con su teléfono móvil, etiquetar a personas (que pueden o no estar registrados en el servicio) y compartir las imágenes con otros usuarios.

La popularización de estos servicios, su implantación en redes sociales como Facebook o en servicios de reconocimiento facial y etiquetado de fotografías como "Find my Face" de Google, conlleva una serie de desafíos para la privacidad, como puede ser el tratamiento de imágenes digitales de personas que no utilizan el servicio y no han dado su consentimiento para ello, o la utilización de las imágenes para otras finalidades distintas para las que fueron tomadas. Cabe llegar la posibilidad de buscar personas mediante la introducción de su imagen en un buscador (sacada por ejemplo a través de un teléfono móvil) obteniendo como resultado imágenes coincidentes o el perfil de una red social.

Debido al número de riesgos para la privacidad que esta tecnología suscita, el GT29 comenzó en 2011 a elaborar un dictamen sobre reconocimiento facial en los servicios en línea y móvil. El Dictamen adoptado en 2012 analiza el marco jurídico y aporta una serie de recomendaciones, como es la necesidad de contar con el consentimiento informado de los usuarios.

F. LOS FLUJOS INTERNACIONALES DE DATOS: FLEXIBILIDAD Y GLOBALIZACIÓN

En 2011 las solicitudes de autorización de transferencias internacionales de datos han mantenido la misma tendencia que en el ejercicio de 2010 (202 solicitudes frente a las 197 presentadas en 2010), si bien, se ha producido un aumento en las solicitudes efectivamente autorizadas en 2011 (175 frente a las 155 en 2010).

Por países destinatarios de las transferencias, destacan las transferencias solicitadas a diversos países de Latinoamérica (79), Estados Unidos (40) e India (29), principales países destinatarios de las transferencias, así como las transferencias con destino a China (14).

América Latina se ha convertido, así, en el principal destino de las exportaciones de datos desde España con un total de 299 autorizaciones a las que deben añadirse las realizadas a la República Argentina que no precisan autorización.

En cuanto al tipo de modelo contractual utilizado para las autorizaciones, la gran mayoría (84%) ha utilizado las cláusulas contractuales que regulan la prestación de servicios, es decir, la nueva Decisión 2010/87/CE, que sustituye a la Decisión 2002/16/CE, vigente hasta mayo de 2010.

En cuanto a las autorizaciones para la transferencia internacional de datos en el seno de grupos multinacionales de empresas, cuando dichos grupos hubiesen adoptados normas o reglas internas vinculantes (BCR en sus siglas en inglés), durante 2011 se han realizado las siguientes actuaciones:

- En el marco del procedimiento coordinado establecido por el Grupo del Artículo 29 de la Directiva 95/46/CE, se ha participado en la revisión de 4 solicitudes de aprobación de BCR presentadas en diferentes Autoridades de Control de Protección de Datos. Francia en el caso de las multinacionales Technip y Hermes, Reino Unido para las BCR presentadas por la entidad Cargill e Irlanda en relación con el Grupo multinacional Intel.

- Así mismo, se han tramitado autorizaciones de transferencias internacionales amparadas en las garantías basadas en BCR previamente autorizadas.

LA REVISIÓN DE LOS MARCOS SUPRANACIONALES DE PROTECCIÓN DE DATOS

Durante el año 2011 han seguido desarrollándose procesos ya iniciados en años anteriores dirigidos a la actualización y modernización de algunos de los más importantes textos que ordenan internacionalmente la protección de datos. La AEPD ha participado activamente en esos procesos.

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

Al cumplirse los 30 años de su adopción en 1981, se iniciaron los trabajos preparatorios de la revisión del Convenio 108 del Consejo de Europa, aunque ésta se lanzó formalmente a finales de 2010 con la aprobación por el Comité de Ministros de una "Resolución sobre la Protección de Datos y la Privacidad en el Tercer Milenio".

En 2011, el Consejo de Europa ha publicado una hoja de ruta con los hitos principales en lo relativo al proceso de modernización del Convenio 108. En el mes de noviembre, el Secretariado publicó una primera propuesta de texto articulado, para su presentación y primera discusión general en la reunión plenaria del Comité Consultivo de Protección de Datos (T-PD), que se celebró ese mismo mes de noviembre. A partir de aquí, el Consejo pretende acelerar los plazos para contar con un borrador definitivo antes del verano de 2012.

Es importante tener presente la relación existente entre esta revisión y la de la Directiva 95/46/CE. Existe un consenso unánime sobre la necesidad de que ambos procesos sean coherentes. Pero el hecho de que en 2011 la Comisión Europea no hubiera publicado aún la propuesta de tal instrumento, así como el hecho de que la propia Comisión haya manifestado su intención de negociar el texto del Convenio en ejercicio de las competencias de la UE en la materia (para lo que tendrá que pedir el correspondiente mandato al Consejo de la Unión Europea), parecen indicar que el proceso se verá ralentizado.

Por otra parte, se da también la circunstancia de que el Consejo de Europa no se ha decantado aún por un instrumento de modificación de entre varias opciones posibles (protocolo adicional, protocolo de modificación o convenio revisado), lo que indudablemente influirá en el cumplimiento de los plazos marcados, puesto que tiene una incidencia directa sobre el contenido de la propuesta que se está elaborando.

Estos trabajos se han desarrollado en paralelo con los del Grupo de Trabajo de Seguridad y Privacidad de la OCDE (WPISP), que se han plasmado en la elaboración de unos Términos de Referencia para el examen de las Directrices de Privacidad, con la finalidad de hacer recomendaciones a la OCDE sobre el futuro de las Directrices, entre las que no se descarta la redacción de un nuevo instrumento.

B. HACIA UNA NUEVA NORMATIVA EUROPEA DE PROTECCIÓN DE DATOS

Pese a la importancia que en el ámbito español pueda tener la revisión de los instrumentos anteriores, ya que no hay que olvidar que España es parte del Convenio 108 y de su Protocolo Adicional, la revisión que sin duda tendrá una trascendencia más clara es la

que afecta a la normativa de la Unión Europea sobre Protección de Datos.

Durante el año 2011, la Comisión Europea intensificó el trabajo de preparación de la propuesta del nuevo marco jurídico de protección de datos que vendrá a sustituir a la vigente Directiva 95/46/CE y también a la Decisión Marco de 2008 sobre protección de datos en el ámbito de la cooperación policial y judicial penal (antiguo "tercer pilar").

La AEPD ha tomado parte en diversas actividades desarrolladas por el Grupo de Trabajo del Artículo 29 (GT29) y orientadas a proporcionar a la Comisión opiniones o criterios en diversas materias que serán abordadas en el futuro instrumento normativo.

En primer lugar, la AEPD contribuyó a la Comunicación de la Comisión sobre "un enfoque global de la protección de los datos personales en Europa", mediante un informe en el que se formularon, entre otras, propuestas relativas a cuestiones tales como:

- Ampliación del concepto de dato personal, para dar respuesta a las evoluciones tecnológicas.
- Aumento de la transparencia para los interesados.
- Notificación de las "violaciones de datos personales".
- Desarrollo del llamado "derecho al olvido".
- Establecimiento de un régimen sancionador más uniforme a nivel europeo.
- Clarificación las normas relativas a legislación aplicable.

- Impulso de una más eficaz autorregulación.

- Actualización del régimen de transferencias internacionales de datos.

- Refuerzo del marco institucional de las Agencias y del Grupo del Artículo 29.

Por otra parte, la AEPD participó en la elaboración de tres "documentos de asesoramiento" que el Grupo elaboró en respuesta a tres preguntas de la Comisión sobre:

- Categorías especiales de datos, en el que se proponían alternativas al actual sistema de "datos sensibles" de cara a su posible flexibilización.

- Notificaciones de ficheros a las autoridades de protección de datos, en el que se analizaba la conveniencia de mantener o no los registros, tal y como los conocemos hasta ahora.

- Cooperación entre dichas autoridades entre sí en procedimientos de ámbito trasnacional, donde se destacó la necesidad de armonizar las legislaciones nacionales como presupuesto para una cooperación eficaz.

Estos documentos daban continuidad a algunos de los dictámenes adoptados por el Grupo en 2009 y 2010, como el relativo al "Futuro de la Privacidad" (WP 168), o al principio de "accountability" (WP 173) que tenían como objetivo principal o secundario ofrecer a la Comisión materiales, criterios y análisis en aspectos clave de la reforma.

Además, la AEPD participó en una reunión del Subgrupo de Trabajo sobre "Futuro de la Privacidad" celebrada en el mes de julio y dedicada monográficamente a responder a un cuestionario de contenido fundamentalmente técnico circulado por la Comisión y destinado a recabar la posición de las Autoridades de Protección de Datos sobre una variedad de temas como derechos de los interesados, obligaciones de responsables y encargados, transferencias internacionales o régimen sancionador en materia de protección de datos. La posición de la AEPD fue transmitida también por escrito a la Comisión.

Posteriormente, la AEPD participó, también en el seno del GT29, en la elaboración de la respuesta a una serie de preguntas que la Vicepresidenta Vivianne Reding había formulado al Grupo en relación con algunos aspectos de la futura norma comunitaria.

En enero de 2012, es decir, fuera ya del periodo temporal al que se refiere esta Memoria, la Comisión presentó oficialmente sus propuestas de reforma, consistentes en dos textos, un Reglamento General de Protección de Datos y una Directiva sobre protección de los derechos individuales en relación con el tratamiento de datos personales por parte de las autoridades competentes para la prevención, investigación, detención y persecución de los delitos penales o la ejecución de las penas, así como sobre el libre movimiento de tales datos.

A. LA ACTIVIDAD DEL GRUPO DE TRABAJO DEL ARTÍCULO 29

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 forma parte del mismo desde su constitución en febrero de 1997.

La actividad del GT29 en el año 2011 estuvo orientada en gran medida, como ya se ha apuntado en el apartado anterior, a coordinar y preparar las aportaciones colectivas de las autoridades de protección de datos al proceso de revisión del marco europeo de protección de datos. Ello ha supuesto que la adopción de documentos no directamente relacionados con este proceso no haya alcanzado el volumen de años anteriores.

Pese a ello, el GT29 también se ha pronunciado sobre otras cuestiones, de entre las que, por su interés, cabe destacar las que se mencionan a continuación.

Dictamen 10/2011 relativo a la propuesta de directiva del parlamento europeo y del consejo relativa a la utilización de datos del registro de nombres de los pasajeros para prevención, detección, investigación y enjuiciamiento de los delitos terroristas y delitos graves (WP 181).

Este Dictamen analiza la propuesta de Directiva relativa a la utilización de datos del registro de nombres de los pasajeros para prevención, detección, investigación y enjuiciamiento de los delitos terroristas y delitos graves dada a conocer por la Comisión Europea el 2 de febrero de 2011. Tras hacer un análisis detallado de la propuesta, el Grupo de Trabajo concluye que aún no se ha demostrado de forma fehaciente la necesidad de un sistema de PNR de la UE y que las medidas recogidas en la propuesta no responden al principio de proporcionalidad, sobre todo porque el sistema plantea la recogida y retención de todos los datos de todos los viajeros de todos los vuelos. El Grupo de Trabajo muestra también serias dudas sobre la proporcionalidad de que los datos de todos los pasajeros se analicen sistemáticamente según criterios predeterminados.

El Dictamen recomienda que se evalúen de forma previa los sistemas y métodos de cooperación existentes y el modo en que se ensamblan para detectar lagunas de seguridad. Si las hubiera, señala, el paso siguiente sería analizar el mejor modo de paliarlas, lo que no implica necesariamente la introducción de un sistema nuevo. Los mecanismos actuales podrían seguir explotándose y mejorándose.

Dictamen 14/2011 sobre cuestiones de protección de datos relacionadas con la prevención del blanqueo de capitales y la financiación del terrorismo (WP 186).

Este Dictamen tuvo su origen en una petición de la Comisión que solicitaba del GT29 criterios sobre aplicación del marco de protección de datos en el terreno de la puesta en práctica de las legislaciones nacionales que han traspuesto las sucesivas directivas europeas de prevención del blanqueo de capitales y la financiación del terrorismo.

A lo largo de 2010 el GT29 abrió un proceso de consultas con las partes afectadas, incluidos la propia

Comisión, los supervisores financieros y las FIU -Unidades de Inteligencia Financiera (en España, el SEPLAC)-.

En este proceso se identificaron una serie de problemas centrales desde la perspectiva de la protección de datos. Entre ellos:

- Se trata de un área sensible, ya que alcanza a cuestiones tales como el tratamiento de datos sensibles, transferencias internacionales o la posibilidad de elaboración de perfiles.

- En una valoración global del conjunto de Estados Miembros, se constata que se ha prestado poca atención a la protección de datos tanto en la redacción como en la aplicación de las normas nacionales, posiblemente, y entre otras razones porque las directivas de blanqueo no han incluido previsiones específicas al respecto.

- Hay disparidad de percepciones en las cuestiones de protección de datos en los Estados Miembros.

- Hay dificultades entre los actores implicados a la hora de interpretar y aplicar los principios de protección de datos en el sector.

Partiendo de esta constatación, el Dictamen incluye hasta 44 recomendaciones, dirigidas tanto a las FIU como a los sujetos obligados (principalmente entidades financieras), que intentan clarificar cómo han de entenderse los principios y garantías propios de la legislación de protección de datos en su aplicación al ámbito de la prevención del blanqueo de capitales y la financiación del terrorismo.

En ese sentido, las recomendaciones abordan las cuestiones clásicas de la protección de datos, como son la identificación de los criterios de legitimación de los tratamientos, principio de calidad, principio de finalidad, principio de necesidad, identificación de los posibles responsables del tratamiento, salvaguardas para el tratamiento de datos sensibles, y aspectos relacionados con las transferencias internacionales de datos.

Dictamen 15/2011 sobre la definición del consentimiento (WP 187).

Este Dictamen analiza en detalle el concepto de consentimiento utilizado actualmente en la Directiva de Protección de Datos y en la Directiva sobre Privacidad en las Telecomunicaciones. Es una nueva muestra del trabajo del GT29 para explicar y aclarar algunos de los conceptos clave del régimen de protección de datos establecido por dichas Directivas, que ha sido ya precedido por otros Dictámenes sobre, por ejemplo, ley aplicable o los conceptos de responsable y encargado.

El Dictamen proporciona numerosos ejemplos de consentimiento válido y no válido, concentrándose en los diversos elementos constitutivos de la regulación que de este concepto hace la Directiva, tales como “indicación, “libre”, “específico”, “inequívoco” o “expreso”.

También se destaca cómo el consentimiento es uno de los varios criterios de legitimación previstos por la Directiva que no excluye la posibilidad, dependiendo del contexto, de otros fundamentos legales que pueden llegar a ser más apropiados en determinadas circunstancias.

En la medida en que el Dictamen es en parte respuesta a una petición de la Comisión en el contexto de la revisión de la normativa de la Unión Europea

sobre Protección de Datos, contiene algunas recomendaciones a tomar en consideración en esta revisión. Entre ellas:

- La necesidad de aclarar el significado del término "inequívoco" y de explicar que sólo el consentimiento que se manifiesta a través de manifestaciones o acciones que significan acuerdo constituye un consentimiento válido.

- La necesidad de pedir a los responsables que establezcan mecanismos para demostrar la existencia de consentimiento dentro de la obligación general de "accountability" que se prevé pueda ser incluida en la futura norma.

- La necesidad de añadir un mandato específico relativo a la calidad y accesibilidad de la información sobre la que se basa el consentimiento.

B. ACTUACIONES EN EL AREA DE COOPERACIÓN POLICIAL Y JUDICIAL

Efectos del Tratado de Lisboa

El elemento de mayor relevancia en estos momentos es, sin duda, el impacto generado por el nuevo marco jurídico que emana del Tratado de Lisboa y que pone fin a la división en pilares existente hasta la fecha. De esta importancia son muestra evidente los posicionamientos que sobre la materia han expresado tanto la Comisión Europea como el Consejo.

En el terreno específico de la protección de datos, el Tratado de Lisboa se ha traducido ya en dos iniciativas paralelas como son la decisión del GT29 de crear un subgrupo de trabajo con competencias específicas en todo lo relativo a protección de datos en las materias cubiertas por el antiguo Tercer Pilar y el acuerdo de la Conferencia de Primavera de Autoridades de Protección de Datos de redefinir la labor del Grupo de Trabajo de Policía y Justicia con el fin de limitar progresivamente su actuación a aquellos temas que no puedan ser asumidos por el GT29.

Evaluación del Acuerdo sobre Programa de Seguimiento de la Financiación del Terrorismo (TFTPII)

El primer tercio del año fue testigo de la controversia generada por la revisión del acuerdo TFTP II, en vigor desde agosto de 2010. Este acuerdo, suscrito entre la Unión Europea y los Estados Unidos, define las condiciones en que se podrán transferir datos sobre transacciones financieras desde la Unión Europea a Estados Unidos con la finalidad de identificar fuentes de financiación de actividades terroristas.

Los trabajos realizados tanto por la Autoridad Común de Control de Europol -con participación de la AEPD- como por la Comisión Europea -con participación de representantes del GT29- pusieron de manifiesto, de un lado, aspectos prácticos de implementación que han generado dudas sobre la efectiva aplicación del acuerdo en los términos acordados y, de otro, la dificultad de demostrar que los presupuestos del mismo se atienen al principio de necesidad. Los informes de las dos revisiones están siendo objeto de estudio por parte del Parlamento Europeo.

La AEPD está participando de forma significativa en estas actividades de control del acuerdo TFTP II, particularmente en las que se están llevando a cabo por parte de la Autoridad Común de Control de Europol. Europol tiene asignadas funciones de intermedia-

ción en la remisión de los datos a las autoridades de Estados Unidos. Por ello, la Autoridad de Control ha realizado hasta el momento dos inspecciones sobre el cumplimiento por parte de Europol de las tareas de evaluación de los requerimientos de información realizados por el Departamento del Tesoro Estadounidense en virtud del artículo 4 de dicho acuerdo, así como sobre los procedimientos de envío espontáneo de información -artículo 9- y a requerimiento de las autoridades competentes de los Estados miembros en el marco del procedimiento señalado en el artículo 10 del Acuerdo.

TFTP Europeo

Con fecha 13 de julio de 2011 la Comisión Europea presentó una comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones relativa a las posibles opciones para la creación de un sistema europeo de seguimiento de la financiación del terrorismo (TFTP Europeo), que responde, entre otras razones, al cumplimiento de lo establecido en el artículo 11 del acuerdo TFTPII antes citado. Según sostiene la Comisión Europea, dicho sistema, considerando la efectividad del TFTP estadounidense, debería contribuir significativamente a los esfuerzos para evitar el acceso de los terroristas a financiación y a materiales, así como seguir las transacciones que realicen.

Registro europeo de datos de pasajeros

En febrero de 2011 la Comisión Europea presentó una propuesta de Directiva sobre registro de nombres de pasajeros (PNR europeo). Esta propuesta, que se enmarca dentro de la Estrategia de Seguridad Interior de la Unión Europea aprobada en noviembre de 2010, establece una serie de requisitos y normas comunes para la recopilación y puesta a disposición de estos datos para los estados por parte de los transportistas aéreos. El GT29 adoptó en su reunión de abril de 2011 un primer dictamen al respecto en el que se insiste en la necesidad de ser extremadamente cauto en el desarrollo de este instrumento garantizando que se atiene a los principios de necesidad y proporcionalidad y que contempla salvaguardas específicas que garanticen que los tratamientos se ajustan estrictamente a la finalidad declarada.

Es de interés señalar que, aunque la propuesta inicial de la Comisión Europea limitaba el ámbito de recogida de datos a los vuelos que entraran o salieran de la Unión Europea, por parte del Consejo se ha solicitado que sean también objeto de seguimiento, en grado aún por determinar, los vuelos intraeuropeos.

Evaluación de la Directiva de Retención de Datos

La Comisión Europea presentó el informe de evaluación de la Directiva sobre retención de datos aprobada en el año 2006. En el documento se subraya que la Directiva se ha incorporado a las legislaciones nacionales de manera desigual, provocando que las diferencias que siguen existiendo entre las legislaciones de los distintos Estados miembros generen dificultades a los proveedores de servicios de telecomunicaciones. Por otro lado, señala que hay algunas dudas sobre las garantías de que los datos sean almacenados, recuperados y utilizados respetando plenamente el derecho a la intimidad y a la protección de los datos personales, lo que ha dado lugar a que en algunos Estados miembros los tribunales hayan anulado la legislación que incorporaba la Directiva.

No obstante lo anterior, la Comisión concluye que, dada la, a su juicio, evidente utilidad del instrumento, apuesta por revisar la Directiva con vistas a proponer un marco jurídico mejorado que solvente los problemas detectados y que redunde en una mayor eficiencia y armonización del sistema.

Evaluación Schengen

Como resultado del proceso de evaluación del nivel de cumplimiento del Convenio de Schengen en materia de protección de datos de carácter personal que tuvo lugar en 2010, la Agencia Española de Protección de Datos ha venido llevando a cabo un intenso programa de actividades en diversas áreas –actividades de inspección, mejora en la información proporcionada al usuario, gestión de procedimientos– en colaboración con las unidades competentes del Ministerio del Interior y del Ministerio de Asuntos Exteriores y Cooperación.

A comienzos del mes de noviembre fue presentado el primer informe de seguimiento de las recomendaciones realizadas por el equipo evaluador ante el grupo de Evaluación Schengen del Consejo Europeo que fue aprobado sin observaciones o comentarios. El informe de evaluación definitivo se presentó en abril de 2012.

Atendiendo igualmente al requerimiento del Grupo de Evaluación Schengen del Consejo Europeo, la Agencia Española de Protección de Datos participa de forma directa en el proceso de evaluación de los países nórdicos -Dinamarca, Noruega, Suecia y Finlandia- que comenzó en octubre de este año con la visita del equipo evaluador a dichos países.

C. AVANCES EN LA CONFERENCIA INTERNACIONAL DE COMISIONADOS DE PROTECCIÓN DE DATOS Y PRIVACIDAD

Los días 1 a 4 de noviembre se celebró en la Ciudad de México la 33ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. En ella se adoptaron decisiones relevantes en relación a su organización y a sus actividades futuras. En especial, se acordó la aprobación de un nuevo reglamento interno por el que, con la finalidad de dar continuidad a la labor de la Conferencia a lo largo del año, se crea un Comité Ejecutivo con funciones de representación y dirección. Este Comité Ejecutivo está compuesto por cinco miembros, tres de ellos nombrados por elección y otros dos reservados para las autoridades organizadoras de la última Conferencia celebrada y de la siguiente Conferencia que vaya a tener lugar. Uno de los miembros del Comité es elegido como su Presidente. El Comité asume las funciones de dirección de los trabajos de la Conferencia, así como otras que anteriormente desempeñaban otras instancias que ahora han desaparecido, como sucede con el Comité de Credenciales, encargado de pronunciarse sobre las solicitudes de acceso como miembro a la Conferencia.

De entre las demás resoluciones adoptadas, destacan la que reconoce como nuevos miembros a las autoridades de Marruecos y Bosnia y Herzegovina, y la que defiende una mayor coordinación transfronteriza entre autoridades en materia de aplicación de la ley. De esta última, merece la pena destacar que se ha establecido un Grupo de Trabajo, del cual forma parte la Agencia Española de Protección de Datos, que se encargará de desarrollar el marco de trabajo y los procedimientos necesarios para facilitar esta coordinación. Se ha alcanzado, igualmente, un compromiso para realizar un encuentro anual dedi-

cado en exclusiva a estos temas, que se desarrollará aprovechando la participación de las autoridades en reuniones de otras instituciones, a los efectos de ahorrar tiempo y recursos.

D. LA RED IBEROAMERICA DE PROTECCION DE DATOS. UNA NUEVA ETAPA HACIA LA COOPERACIÓN

Los procesos legislativos para garantizar la protección de los datos personales continúan desarrollándose en Latinoamérica colocando a esta área geográfica en una posición destacada en la tutela de este derecho fundamental.

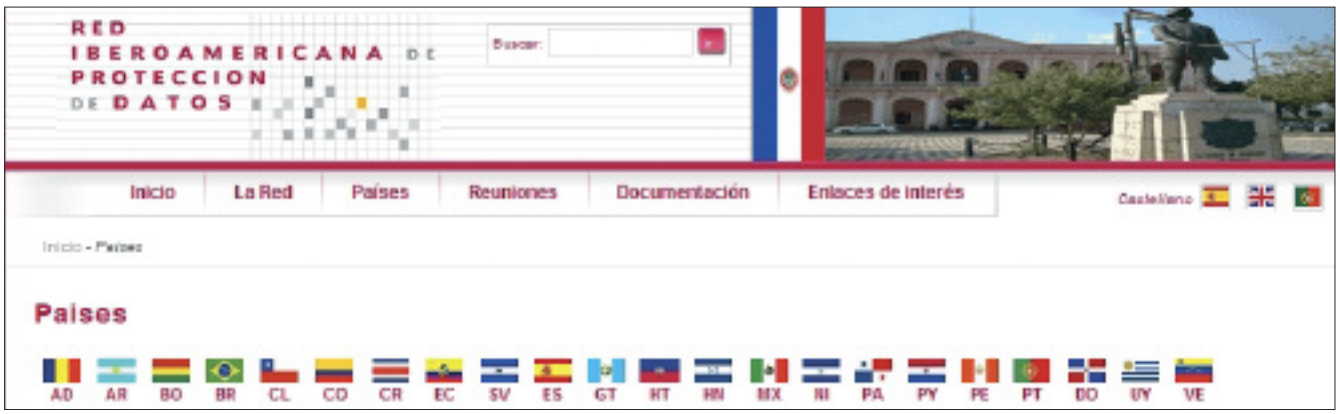
En 2011 se han aprobado dos nuevas leyes. En Costa Rica, la Ley 8968 de Protección de la Persona frente al tratamiento de sus datos personales, de 5 de septiembre de 2011, y en Perú, la Ley nº 29733, de Protección de Datos personales, de 3 de julio de 2011.

Asimismo, la Ley 19.628, de 28 de agosto de 1999, sobre Protección a la Vida Privada, de Chile, se encuentra en proceso de revisión de parte de su articulado. Por último, en Colombia el Proyecto de ley estatutaria No.184 aprobado en 2010 "por el cual se dictan disposiciones generales para la protección de datos personales", está solo pendiente de la sanción presidencial.

El proceso legislativo ha ido acompañado de una consolidación de las autoridades a las que se ha atribuido la competencia para tutelar el derecho a la protección de datos.

Como exponente de esa consolidación, debe destacarse la organización por parte del IFAI de la 33 Conferencia Internacional de Privacidad y Protección de Datos que tuvo lugar en la Ciudad de México los días 2 y 3 de noviembre de 2011, siendo la primera vez que se celebra en un país latinoamericano. Iniciativa que tendrá continuidad en 2012 al haberse designado a la Agencia de gobierno electrónico y sociedad de la información (AGESIC), como organizador de la 34 Conferencia Internacional de la República Oriental del Uruguay.

La creación de Autoridades de protección de datos en América Latina ha incidido en el funcionamiento de la Red Iberoamericana de Protección de Datos



planteando la conveniencia de modificar su reglamento de funcionamiento.

En dicha modificación debe jugar un papel principal la definición de los miembros de la Red y, especialmente, la articulación de nuevos instrumentos de cooperación entre los que ostentan la condición de Autoridades de Control.

Por su parte, la Red ha seguido desarrollando iniciativas para la protección de los datos personales:

- En abril se celebró en el Centro de Formación de la Agencia Española de Cooperación Internacional para el Desarrollo (AECID), en La Antigua (Guatemala), el "Seminario sobre el acceso a la información pública yprotección de datos. La protección de datos en las cédulas y documentos de identificación de los ciudadanos".

  En el seminario se abordaron dos cuestiones claramente diferenciadas: por un lado, el acceso a la información pública y la protección de datos, y por otro, las implicaciones de los documentos oficiales electrónicos de identificación de los ciudadanos en un entorno en el que incide un nuevo elemento como son las exigencias de seguridad asociadas a dichos documentos.

  En este Seminario participaron representantes de la AEPD, del Instituto Federal de Acceso a la Información y Protección de Datos de México, del Consejo de la Unidad Reguladora y de Control de Datos Personales de Uruguay, del Servicio del Registro Civil e Identificación de Chile, la Comisión de Transparencia del Congreso de la República de Guatemala, la Comisión para la Transparencia y Combate a la Corrupción de Guatemala, la Defensoría del Pueblo de Paraguay, la Oficina de Acceso a la Información Pública en la Procuraduría General de la República Dominicana, el Consejo para la Transparencia de Chile, la Corte Suprema de Justicia de El Salvador, del Instituto de Acceso a la Información Pública de Honduras, la Dirección de Derechos Ciudadanos de AGESIC de Uruguay, el Registro Nacional de Personas de Guatemala, y de la Defensoría de los habitantes de Costa Rica. El sector privado estuvo representado por la Comisión Nacional Bancario y de Valores de México, y por Sm4rt Security Services de México.

  El Seminario ha dado continuidad a los trabajos de la Red Iberoamericana de Protección de Datos, potenciando así las iniciativas de intercambio de experiencias entre los países iberoamericanos y estableciendo canales abiertos de diálogo y colaboración en materia de protección de datos personales y transparencia.

- En el mes de junio se celebró en el Centro de Formación de la Agencia Española de Cooperación Internacional para el Desarrollo (AECID), en la ciudad de Cartagena de Indias (Colombia), el Seminario "El impacto de las trasferencias internacionales de datos en América Latina. Las políticas preventivas y la autorregulación en la implantación de la normativa de protección de datos".

  En este seminario se debatió sobre el impacto y regulación de las transferencias internacionales, la deslocalización de actividades económicas en América Latina, las experiencias de los países de la Red en políticas preventivas, autorregulación y aplicación de la legislación de protección de datos, experiencias sectoriales de autorregulación y otros instrumentos preventivos en la aplicación de la normativa de protección de datos.

En la última jornada se celebró una reunión cerrada de la Red, en la que se debatieron propuestas de recopilación de jurisprudencia en materia de protección de Datos, de participación en los trabajos sobre protección de datos de la Organización de Estados Americanos (OEA), y se presentaron las líneas generales de la Conferencia Internacional que se celebrará en México abordándose la celebración del IX Encuentro en dicha Conferencia.

En este seminario participaron representantes de la AEPD, del Instituto Federal de Acceso a la Información y Protección de Datos de México, del Consejo Consultivo de la Unidad Reguladora y de Control de Datos Personales de Uruguay, de la Secretaría de Economía de México, del Registro Nacional de Costa Rica, del Ministerio de Comercio, Industria y Turismo de Colombia, y de la Agencia para el desarrollo del Gobierno Electrónico y la Sociedad de la Información y el Conocimiento de Uruguay. Asimismo, el sector privado estuvo representado por las siguientes empresas: Telefonica, S.A., Comunicaciones Nextel de México S.A., el Grupo BBVA, la Hewlett-Packard Company, Google, Telmex de México, la Corporación de Fomento de la Producción de Chile, la Asociación Nacional de Empresarios Industriales de Colombia, y MetL2,8fe de Estados Unidos.

- En el mes de octubre tuvo lugar el IX Encuentro de la Red en la Ciudad de México, en el marco de la 33 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, con la participación del Consejo de Europa y de la Comisión Federal de Comercio de los Estados Unidos (FTC).

La Resolución aprobada en México recoge los compromisos adoptados, entre los cuales destacan: desarrollar procedimientos transfronterizos de cooperación que contribuyan a garantizar los derechos a los ciudadanos, promover intercambios de información entre las Autoridades de Protección de Datos miembros de la Red Iberoamericana para establecer criterios armonizados en la aplicación de las leyes nacionales, colaborar activamente, partiendo de las experiencias de los distintos países, en la elaboración de una ley modelo sobre la protección de datos en la Organización de Estados Americanos y acentuar las acciones formativas entre los miembros de la Red Iberoamericana de Protección de datos.

Las relaciones bilaterales de la AEPD con miembros de la Red se han traducido en diversas visitas institucionales a la Sede de la Agencia.

- En el mes de febrero se recibió la visita de una delegación del gobierno colombiano, representado por el Embajador de Colombia en España, el Superintendente de Industria y Comercio, el Director de Regulación del Ministerio de Comercio, Industria y Turismo, y la Asesora de Asuntos Internacionales de la Superintendencia de Industria y Comercio.

El principal objetivo de la visita consistió en la presentación del proyecto de Ley Estatutaria nº 46 de 2010 Cámara, "por la cual se dictan Disposiciones Generales para la Protección de Datos Personales proyecto normativo "habeas data" y comentar aspectos sobre la normatividad secundaria. Asimismo, se solicitó información sobre el procedimiento a seguir para solicitar una decisión de adecuación de la Comisión Europea.

En la sesión de tarde, se sumaron a la reunión representantes de MOVISTAR, BBVA Y UNESPA que expusieron la experiencia adquirida en materia de

protección de datos en los sectores de telecomunicaciones, financiero y de la salud.

- En el mes de mayo tuvo lugar la visita de una delegación de la Comisión de Transparencia y Acceso a la Información del Estado de Nuevo León (México) con la finalidad de firmar un convenio de colaboración. Este convenio tiene por objeto establecer una etapa de colaboración y coordinación institucional entre ambos entes con la finalidad de promover la difusión del derecho a la protección de datos, el fomento de estudios e investigaciones, así como el intercambio de de experiencias de mutuo interés.

- En el mismo mes visitó la Agencia una delegación del Consejo para la Transparencia de Chile con la finalidad de firmar un convenio de colaboración. Este convenio tiene por objeto establecer un marco de colaboración y coordinación institucional entre ambos entes con la finalidad de promover la difusión del derecho a la protección de datos, el fomento de estudios e investigaciones, así como el intercambio de experiencias de mutuo interés.

- Por último, en el mes de noviembre la Agencia recibió a una delegación en representación del Instituto Federal de Acceso a la Información y Protección de Datos (IFAI). En ella se realizó un análisis en profundidad del funcionamiento de distintas áreas de la AEPD: la Atención al Ciudadano, el Registro General de Protección de Datos, el Área de Informática, y en especial, la Inspección de datos abarcando tanto la Inspección como la Instrucción y las Tutelas de derechos.

E. EL IMPULSO DE LA PROTECCIÓN DE DATOS EN OTRAS ÁREAS GEOGRÁFICAS

La Agencia Española de Protección de Datos fue el organismo seleccionado, tras el correspondiente concurso convocado y financiado por la Comisión Europea, para desarrollar el Proyecto de Fortalecimiento de las capacidades de la Agencia Croata de Protección de Datos, que viene ejecutándose desde julio de 2010 (Proyecto de Hermanamiento nº 2007-0101-030201,HR/2007/IB/JH/02).

El objetivo primordial del proyecto es contribuir a la efectividad de la protección de datos en Croacia según el acquis communautaire y las buenas prácticas, a través del reforzamiento del papel consultivo y de supervisión de la Agencia croata de Protección de Datos de carácter personal. Los propósitos del contrato son:

- Armonización de la Ley de Protección de Datos Personales con la Directiva 95/46/CE y la implementación de la base de datos standard ISO 27001 para el sistema de seguridad de la información.

- Contribución al acuerdo de estabilización y asociación del programa nacional para la integración de la República de Croacia a la Unión Europea.

Más de 25 expertos de la Agencia, junto a otros expertos internacionales de otras agencias Europeas de Protección de Datos, han participado en el proyecto.

Un funcionario de la Agencia desarrolla las labores de Asesor residente en Zagreb con carácter permanente.

En 2011 se han desarrollado el grueso de las actividades del proyecto, destacando las siguientes:

- Seminarios para analizar la adecuación de la legislación croata a la normativa comunitaria en los siguientes sectores: Administraciones Públicas, Policía, Justicia, Salud, Telecomunicaciones, Internet, Marketing Directo y Protección de datos en el ámbito laboral. Tras la realización de los Seminarios, se han elaborado las correspondientes Guías sectoriales y las oportunas modificaciones legislativas.

- Definición y realización de una Encuesta entre la población croata para conocer su grado de concienciación en materia de protección de datos.

- Fortalecimiento de las facultades inspectoras de la Agencia Croata. A tal efecto, una vez analizadas sus necesidades y teniendo en cuenta las características y formación de sus funcionarios, se ha diseñado un Manual dirigido especialmente a su Departamento de Inspección.

- Planes Sectoriales en Salud, Telecomunicaciones y Marketing Directo.

- Plan de Comunicación para el período 2010-2013.

- Talleres en el Ministerio del Interior para incrementar la concienciación de la Policía sobre el adecuado tratamiento de datos personales.

- Seminarios para la mejora de los sistemas informáticos (IT) y de las medidas de seguridad de la Agencia croata. Están también dirigidos a la formación de sus funcionarios y a la propuesta de modificaciones en la normativa croata sobre IT. Se realizó una visita a la AEPD con el fin de conocer in situ el modelo español en este aspecto. Está previsto que, al concluir este Proyecto, esté implementada una política de seguridad adecuada a los estándares europeos y a la ISO 27001.

Asimismo, la Agencia Española de Protección de Datos ha participado en 2011 en un proyecto de asistencia técnica, financiado por la Unión Europea, en Albania ("Fortalecimiento de la Agencia de Protección de Datos de Albania"). Se trata de un proyecto iniciado en 2010 y gestionado por un consorcio europeo, liderado por la Fundación Internacional y para Iberoamérica de Administración y Políticas Públicas (FIIAPP).

Con el fin de mejorar el funcionamiento de la Agencia Albanesa de Protección de Datos, en el marco del proyecto, se han desarrollado tareas de asesoría, entre otras materias, en técnicas de inspección y protección de datos en sectores tales como Justicia, Sanidad, Estadística y Finanzas/Banca.

Junto a ello, en 2011 una delegación de funcionarios de la Agencia Albanesa de Protección de Datos, visitó la sede de la Agencia Española de Protección de Datos, con el fin de dar conocer de manera cercana y práctica la experiencia española sobre inspección de datos, transferencias internacionales de datos personales, gestión de nuevas tecnologías y tratamiento de datos personales en registros públicos.

El objetivo del proyecto es alinear los procedimientos de la Agencia Albanesa de Protección de Datos (Albanian Data Protection Commissioner Office) con los estándares de la Unión Europea con el fin de garantizar el derecho a la intimidad y la protección de datos personales.

COOPERACIÓN CON LAS AGENCIAS AUTONÓMICAS DE PROTECCIÓN DE DATOS

Los Grupos de Trabajo creados para la coordinación entre las Autoridades de Protección de datos (Registro, Inspección, Asesorías Jurídicas, Secretarías Generales e Internacional) mantuvieron ocho reuniones de trabajo a lo largo de 2011. El 14 de diciembre de 2011, se celebró la reunión de coordinación de los Directores de las cuatro Agencias de Protección de Datos, en la que se abordaron, entre otros, los siguientes temas:

- Las consecuencias derivadas de la STJUE, de 24 de noviembre de 2011, que declaró el efecto directo del artículo 7.f) de la Directiva 95/46/CE.

- El intercambio de criterios sobre la aplicación de la figura del apercibimiento, sus implicaciones procedimentales y las consecuencias derivadas de su incumplimiento.

- El ejercicio de los derechos de cancelación y oposición ante los responsables de los diarios y boletines oficiales y de las tecnologías disponibles para garantizarlo.

- El impulso definitivo a la elaboración de un recurso informativo sobre la protección de los datos de los menores.

- El análisis de la incidencia sobre la protección de datos de la oferta de servicios de Cloud Computing.

- La cooperación entre las Agencias en relación con las iniciativas de la Comisión Europea para aprobar una nueva regulación de la protección de datos en la Unión Europea, sustituyendo a la Directiva 95/46/CE.

Además, los Grupos de Trabajo, en sus respectivas reuniones, intercambiaron criterios sobre otras cuestiones, tales como:

- Las reclamaciones sobre tutela de derechos ejercitadas por uno de los padres separados que tienen atribuida de forma conjunta la patria potestad.

- La promoción de sesiones formativas para el personal de las Autoridades de Protección de Datos.

- La creación de un lista de preguntas más frecuentes (FAQ) comunes a dichas Autoridades.

- La coordinación en la tramitación de Códigos Tipo.

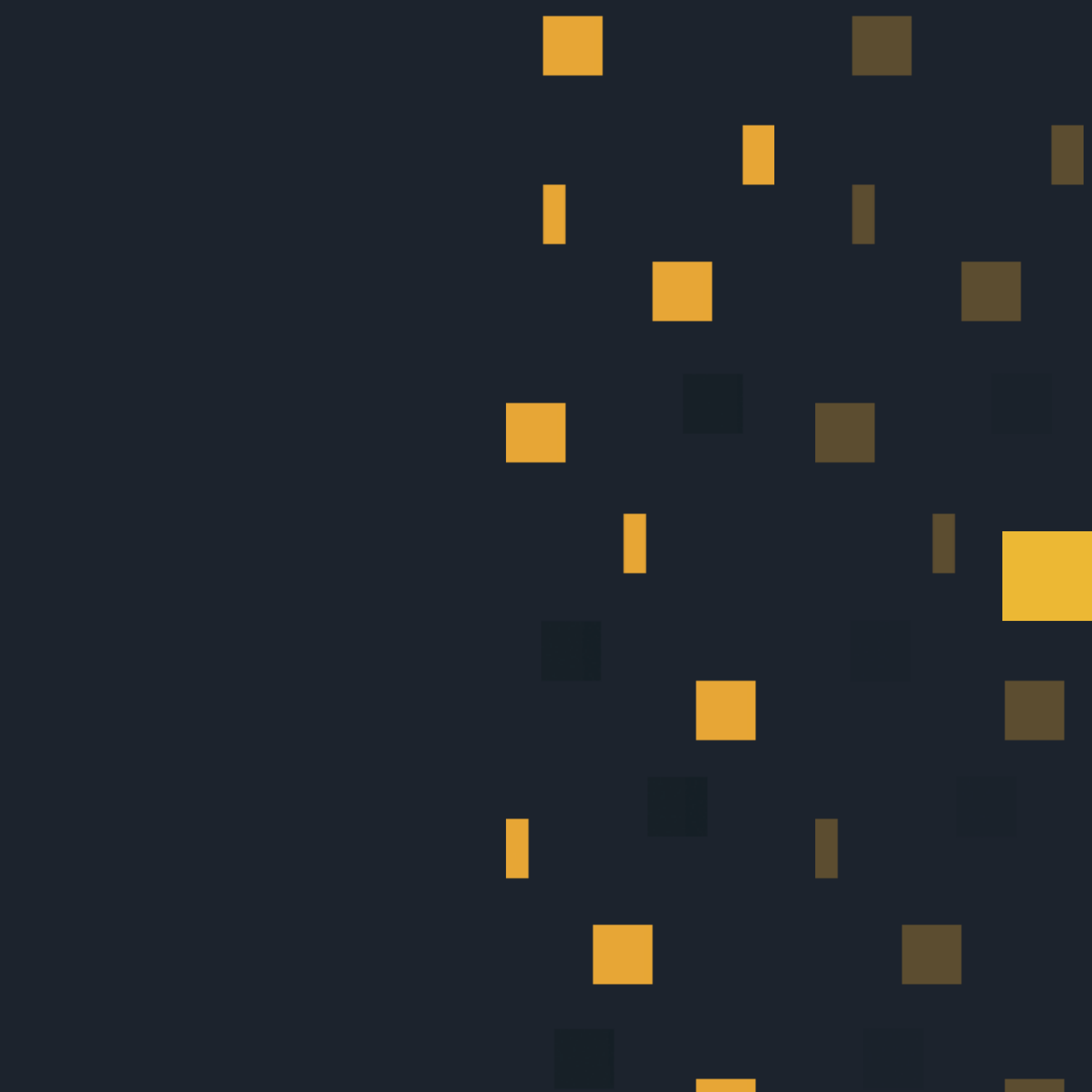
- La coordinación en relación con el nuevo sistema de inscripción en el RGPD (sistema RENO).

- El análisis de las habilitaciones legales para la comunicación por parte de los colegios profesionales de datos relativos a la "habilitación profesional" y a la existencia de posibles expedientes disciplinarios de los colegiados.

- La videovigilancia en comunidades de propietarios.

- La publicación abreviada de los actos administrativos, especialmente, en procedimientos sancionadores y disciplinarios.


AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



MEMORIA 2011

LA AGENCIA EN CIFRAS

DENUNCIAS Y RECLAMACIONES REGISTRADAS

TIPO	2009	2010	2011	% VAR. 2010/11
Escritos de reclamación de tutela	1.832	1.657	**2.230**	34,58
Escritos de denuncia	5.310	5.045	**7.648**	51,60
TOTAL	**7.142**	**6.702**	**9.878**	**47,39**

RESOLUCIONES DICTADAS POR EL DIRECTOR

TIPO	2009	2010	2011	% VAR. 2010/11
Reclamaciones de tutela de derechos resueltas	1.947	1.830	**1.939**	5,96
Denuncias resueltas	4.525	5.122	**5.917**	15,52
TOTAL	**6.472**	**6.952**	**7.856**	**13**

PROCEDIMIENTOS RELATIVOS AL EJERCICIO DE LA POTESTAD SANCIONADORA

SEGÚN TIPO DE PROCEDIMIENTO

TIPO	2009	2010	2011	% VAR. 2010/11
Desistimiento por art. 42 y 71 LRJPAC	222	229	**337**	47,16
Acuerdo de no admisión a trámite	1.967	2.240	**2.993**	33,62
Archivo de actuaciones tras investigación previa	920	1.044	**901**	-13,70
Resolución de procedimientos de apercibimiento	-	-	**290**	-
Resolución de procedimientos sancionadores	709	766	**674**	-12,01
Resolución de procedimientos de infracción de las AAPP	89	76	**99**	30,26
TOTAL RESOLUCIONES	**3.907**	**4.355**	**5.294**	**47,16**

SEGÚN SENTIDO DE LA RESOLUCIÓN

TIPO	2009	2010	2011	% VAR. 2010/11
Archivo de actuaciones	3.109	3.513	**4.231**	20,44
Archivo de procedimiento de apercibimiento	-	-	**7**	-
Archivo de procedimiento sancionador	88	175	**140**	-20,00
Archivo de procedimiento de infracción de las AAPP	18	15	**18**	20,00
TOTAL RESOLUCIONES DE ARCHIVO	**3.215**	**3.703**	**4.396**	**18,71**
Declarativa de infracción con apercibimiento[1]	-	-	**312**	-
Declarativa de infracción con sanción económica	621	591	**505**	-14,55
Declarativa de infracción de las AAPP	71	61	**81**	32,79
TOTAL RESOLUCIONES DECLARATIVAS DE INFRACCIÓN	**692**	**652**	**898**	**37,73**

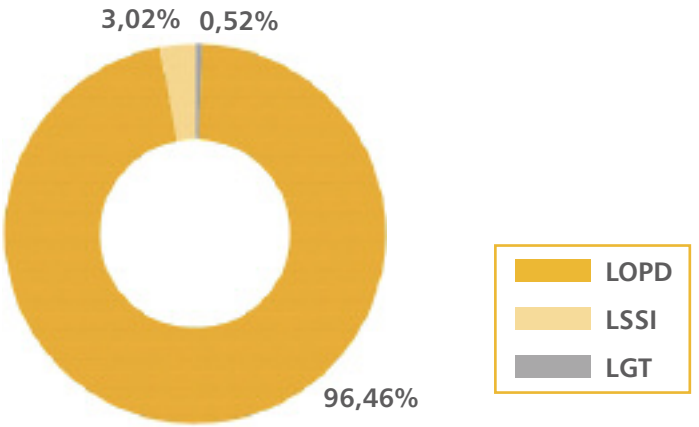
[1] Se incluyen los procedimientos sancionadores que habían sido iniciados antes de 6/3/2011, fecha en que entró en vigor el actual régimen sancionador, a través de las modificaciones introducidas por la Ley 2/2011, de 4 de marzo, de Economía Sostenible, y que se resolvieron con apercibimiento.

SANCIONES IMPUESTAS

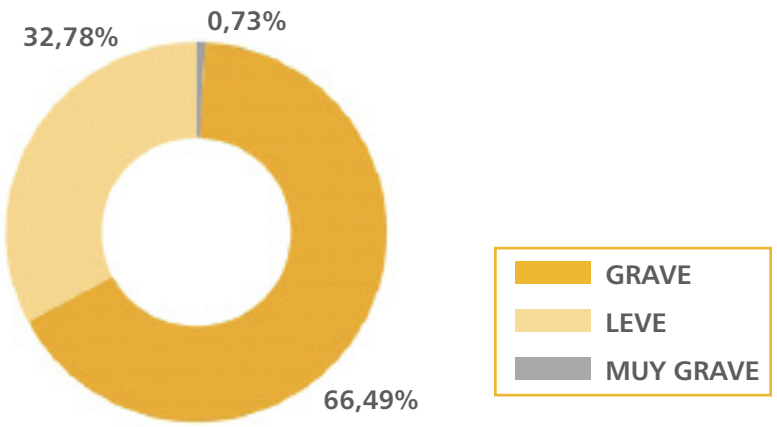
	2009 (€)	2010 (€)	2011 (€)	% VAR. 2010/11
TOTAL SANCIONES	24.872.979,72	17.497.410,02	**19.597.905,97**	12

* La tabla recoge el total de sanciones declaradas.

SANCIONES IMPUESTAS SEGÚN LEY INFRINGIDA 2011



SANCIONES IMPUESTAS SEGÚN GRAVEDAD 2011



GRADUACIÓN DE LA CUANTÍA DE LA MULTA EN TRATAMIENTOS DE TITULARIDAD PRIVADA (LOPD)

ATENUACIÓN DE LA MULTA / APERCIBIMIENTO	2011	% RELATIVO
Apercibimiento por aplicación del art. 45.6	355	38,30
Aplicación del art. 45.5 en sanción económica	145	15,64
Aplicación del art. 45.4 en sanción económica	291	31,39
Sanción económica sin atenuación	136	14,67
	927	**100**

EVOLUCIÓN DE LAS INFRACCIONES CON SANCIÓN ECONÓMICA (LOPD)

2009	2010	2011	% 2010/2011
661	665	572	-13,98

ACTUACIONES PREVIAS INICIADAS

	2009	2010	2011	% VAR. 2010/11
Actuaciones previas	4.136	4.302	**5.389**	25,26

DISTRIBUCIÓN DE LAS ACTUACIONES PREVIAS

ACTIVIDAD	2009	2010	2011	% RELATIVO	% VAR. 2010/11
Telecomunicaciones	908	1.170	**1.378**	25,57	17,78
Videovigilancia	721	819	**871**	16,16	6,35
Entidades financieras	768	691	**841**	15,61	21,71
Servicios de Internet (excepto spam)	156	168	**288**	5,34	71,43
Comunicaci. electrónicas comerciales - spam (LSSI)	180	126	**270**	5,01	114,29
Profesionales, admón. fincas, comunid. de propietarios	160	137	**226**	4,19	64,96
Administración pública	218	194	**206**	3,82	6,19
Recursos humanos, asuntos laborales	120	106	**135**	2,51	27,36
Suministro y comercialización de gas, electricidad y agua	53	74	**122**	2,26	64,86
Sanidad	123	114	**110**	2,04	-3,51
Asociaciones, federaciones, colegios profesionales, clubes, fundaciones, ONG's	119	75	**105**	1,95	40
Comercios, transporte, hostelería	137	68	**105**	1,95	54,41
Publicidad y prospección comercial (excepto spam)	52	91	**98**	1,82	7,69
Medios de comunicación	51	63	**92**	1,71	46,03
Inscripción de ficheros / Información artículo 5	-	75	**90**	1,67	20
Seguros	47	59	**67**	1,24	13,56
Sindicatos	24	48	**57**	1,06	18,75
Procedimientos judiciales	3	9	**51**	0,95	466,67
Partidos políticos	15	19	**46**	0,85	142,11
Enseñanza	34	19	**45**	0,84	136,84
Fuerzas y cuerpos de seguridad	32	54	**39**	0,72	-27,78
Documentación desechada sin destruir o borrar	-	28	**36**	0,67	28,57
Comunicaciones comerciales por fax (LGT)	25	8	**27**	0,50	237,50
Derechos ARCO	-	13	**12**	0,22	-7,69
Seguridad privada	10	5	**8**	0,15	60
Otros	180	69	**64**	1,19	-7,25
TOTAL	**4.136**	**4.302**	**5.389**	**100**	**25,26**

NOTA: Las cifras incluyen las actuaciones de inspección incoadas por denuncia o de oficio (EI), los desistimientos que se producen como consecuencia de no haberse subsanado en plazo las denuncias incompletas (AT) y las denuncias sobre las que se acuerda no incoar actuaciones de inspección y no iniciar procedimiento de infracción/sancionador (IT).

DISTRIBUCIÓN DE LOS PROCEDIMIENTOS SANCIONADORES RESUELTOS

ACTIVIDAD	2009	2010	2011	% RELATIVO	% VAR. 2010/11
Telecomunicaciones	182	169	**249**	36,94	47,34
Videovigilancia	145	262	**122**	18,10	-53,44
Entidades financieras	100	94	**79**	11,72	-15,96
Comunicaciones electrónicas comerciales - spam (LSSI)	46	52	**29**	4,30	-44,23
Servicios de Internet (excepto spam)	17	15	**23**	3,41	53,33
Sanidad	8	11	**23**	3,41	109,09
Recursos humanos, asuntos laborales	18	20	**20**	2,97	0
Suministro y comercialización de gas, electricidad y agua	21	18	**20**	2,97	11,11
Inscripción de ficheros/Información artículo 5	-	10	**20**	2,97	100
Asociaciones, federaciones, colegios profesionales, clubes	24	26	**16**	2,37	-38,46
Publicidad y prospección comercial (excepto spam)	28	14	**15**	2,23	7,14
Profesionales, comunidades de propietarios, admón. fincas	19	17	**11**	1,63	-35,29
Comercio, transporte, hostelería	23	23	**8**	1,19	-65,22
Seguros	10	8	**6**	0,89	-25
Comunicaciones comerciales por fax (LGT)	12	2	**6**	0,89	200
Administración pública	5	2	**2**	0,30	0
Derechos ARCO	-	2	**2**	0,30	0
Partidos políticos	7	3	**1**	0,15	-66,67
Otros	28	19	**22**	3,26	15,79
TOTAL	**709**	**767**	**674**	**100**	**-12,12**

* Se incluyen procedimientos que acaban con archivo o sanción.

DISTRIBUCIÓN DE LAS RESOLUCIONES SANCIONADORAS

ACTIVIDAD	2009	2010	2011	% RELATIVO	% VAR. 2010/11
Videovigilancia	117	176	**281**	34,39	59,66
Telecomunicaciones	170	134	**220**	26,93	64,18
Entidades financieras	89	82	**58**	7,10	-29,27
Servicios de Internet (excepto spam)	16	13	**42**	5,14	223,08
Comunicaciones electrónicas comerciales - spam (LSSI)	39	44	**26**	3,18	-40,91
Inscripción de ficheros / Información artículo 5		8	**25**	3,06	212,5
Recursos humanos, asuntos laborales, sindicatos	21	17	**22**	2,69	29,41
Profesionales, comunidades de propietarios, admón. fincas	15	14	**20**	2,45	42,86
Asociaciones, federaciones, colegios profesionales, clubes	20	22	**19**	2,33	-13,64
Suministro y comercialización de gas, electricidad y agua	21	16	**19**	2,33	18,75
Sanidad	6	7	**18**	2,20	157,14
Publicidad y prospección comercial (excepto spam)	24	12	**16**	1,96	33,33
Comercio, transporte, hostelería	22	16	**10**	1,22	-37,5
Comunicaciones comerciales por fax (LGT)	11	2	**5**	0,61	150
Seguros	8	7	**4**	0,49	-42,86
Enseñanza	5	1	**4**	0,49	300
Administración pública (entidad. Derecho privado)	5	2	**3**	0,37	50
Derechos ARCO		2	**2**	0,24	0
Partidos políticos	5	2	**2**	0,24	0
Medios de comunicación	2	1	**2**	0,24	100
Otros	25	13	**19**	2,33	46,15
TOTAL	**621**	**591**	**817**	**100**	**38,24**

NOTA: En cada resolución de procedimiento PS o A puede haberse declarado más de una infracción.

* Resoluciones que finalizan con imposición de sanción o apercibimiento.

SECTORES CON MAYOR IMPORTE GLOBAL DE SANCIONES

ACTIVIDAD	2010 (€)	2011 (€)	% REL. DEL TOT.	% VAR. 2010/11
Telecomunicaciones	9.185.877,87	12.388.639,80	63,21	34,87
Entidades financieras	3.772.072,00	3.896.612,86	19,88	3,30
Suministro y comercialización de gas, electricidad y agua	949.720,17	1.018.000	5,19	7,19
Videovigilancia	507.327,47	494.711,05	2,52	-2,49
Comunicaciones electrónicas comerciales - spam (LSSI)	621.114,42	305.405	1,56	-50,83
TOTAL 5 PRIMEROS SECTORES	**15.036.111,93**	**18.103.368,71**	**92,37**	**20,40**
Publicidad y prospección comercial (excepto spam)	437.810,28	304.002	1,55	-30,56
Recursos humanos, asuntos laborales	394.013,32	303.002	1,55	-23,10
Sanidad	252.606,86	143.204,02	0,73	-43,31
Servicios de Internet (excepto spam)	170.909,09	115.107,06	0,59	-32,65
Seguros	162.202,42	102.001	0,52	-37,11
TOTAL 10 PRIMEROS SECTORES	**16.453.653,90**	**19.070.684,79**	**97,31**	**15,91**
TOTAL	**17.497.410,02**	**19.597.905,97**	**100**	**12**

PROCEDIMIENTOS DE DECLARACIÓN DE INFRACCIÓN DE LAS ADMINISTRACIONES PÚBLICAS RESUELTOS*

TIPO ADMINISTRACIÓN [1]	2009	2010	2011	% RELATIVO	% VAR. 2010/11
Otras Entidades de Derecho Público [2]	21	3	**43**	43,43	1333,33
Local	22	32	**30**	30,30	-6,25
Autonómica	29	16	**18**	18,18	12,50
Estatal	17	25	**8**	8,08	-68
TOTAL	**89**	**76**	**99**	**100**	**30,26**

[1] En un mismo procedimiento de infracción pueden figurar imputados de distintas administraciones territoriales, computándose tales procedimientos en una sola de las administraciones afectadas.

[2] Se incluyen en este apartado los procedimientos en los que se declara la infracción de 32 Registros de la Propiedad.

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

INFRACCIONES DE LAS ADMINISTRACIONES PÚBLICAS

TIPO ADMINISTRACIÓN	2011	% RELATIVO
Otras Entidades de Derecho Público	40	49,38
Autonómica	21	25,93
Local	14	17,28
Estatal	6	7,41
TOTAL	**81**	**100**

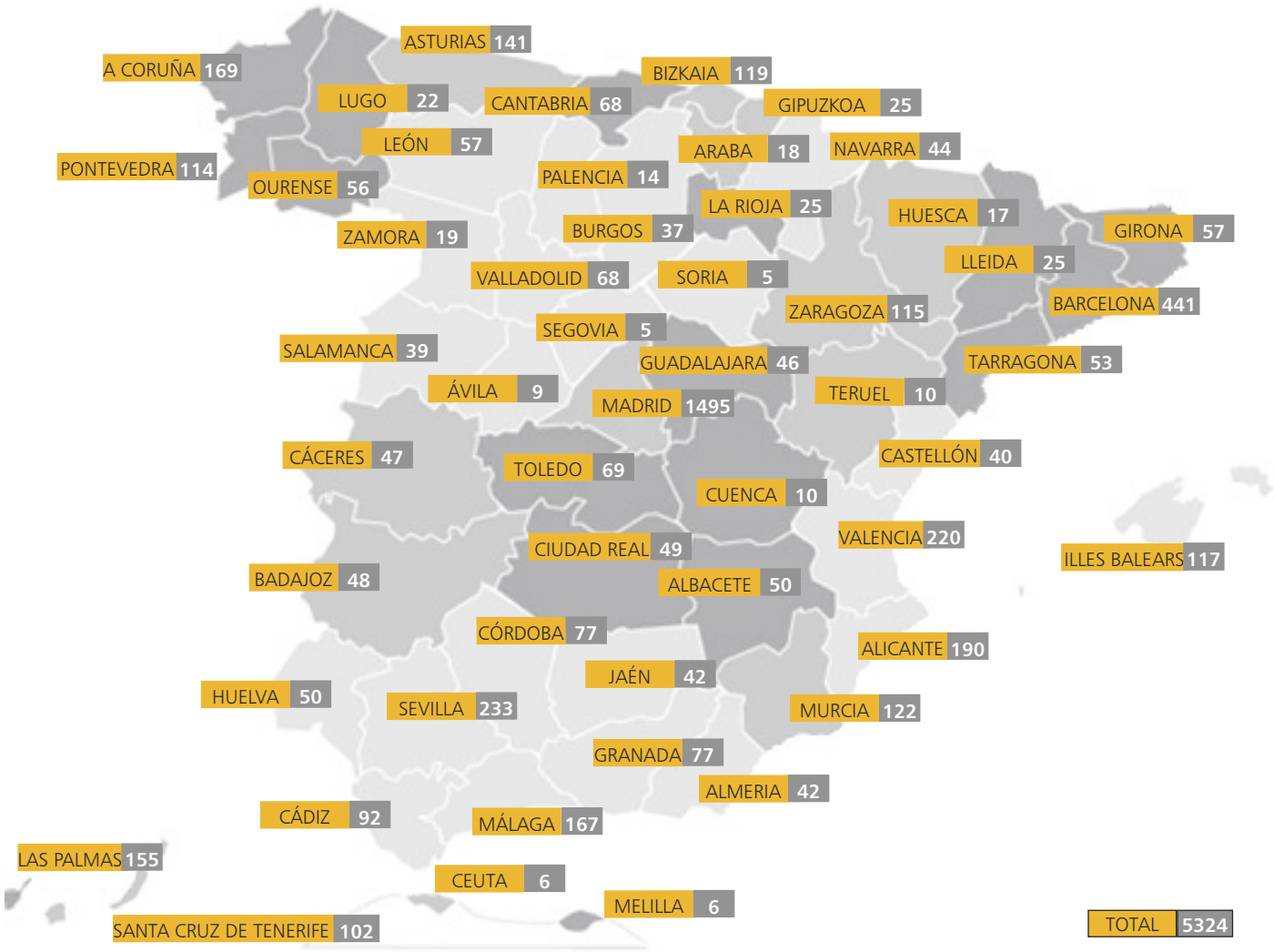
* En una misma resolución puede declararse más de una infracción.

TUTELAS DE DERECHO RESUELTAS

	ESTIMATORIA	ESTIMATORIA FORMAL O PARCIAL	DESESTIMAT.	ARCHIVO POR INADMISIÓN O DESISTIMIENTO	TOTAL
Cancelación	242	158	102	551	1.053
Acceso	176	148	84	219	627
Rectificación	24	27	21	75	147
Oposición	55	28	22	83	188
TOTAL	**497**	**361**	**229**	**928**	**2.015**

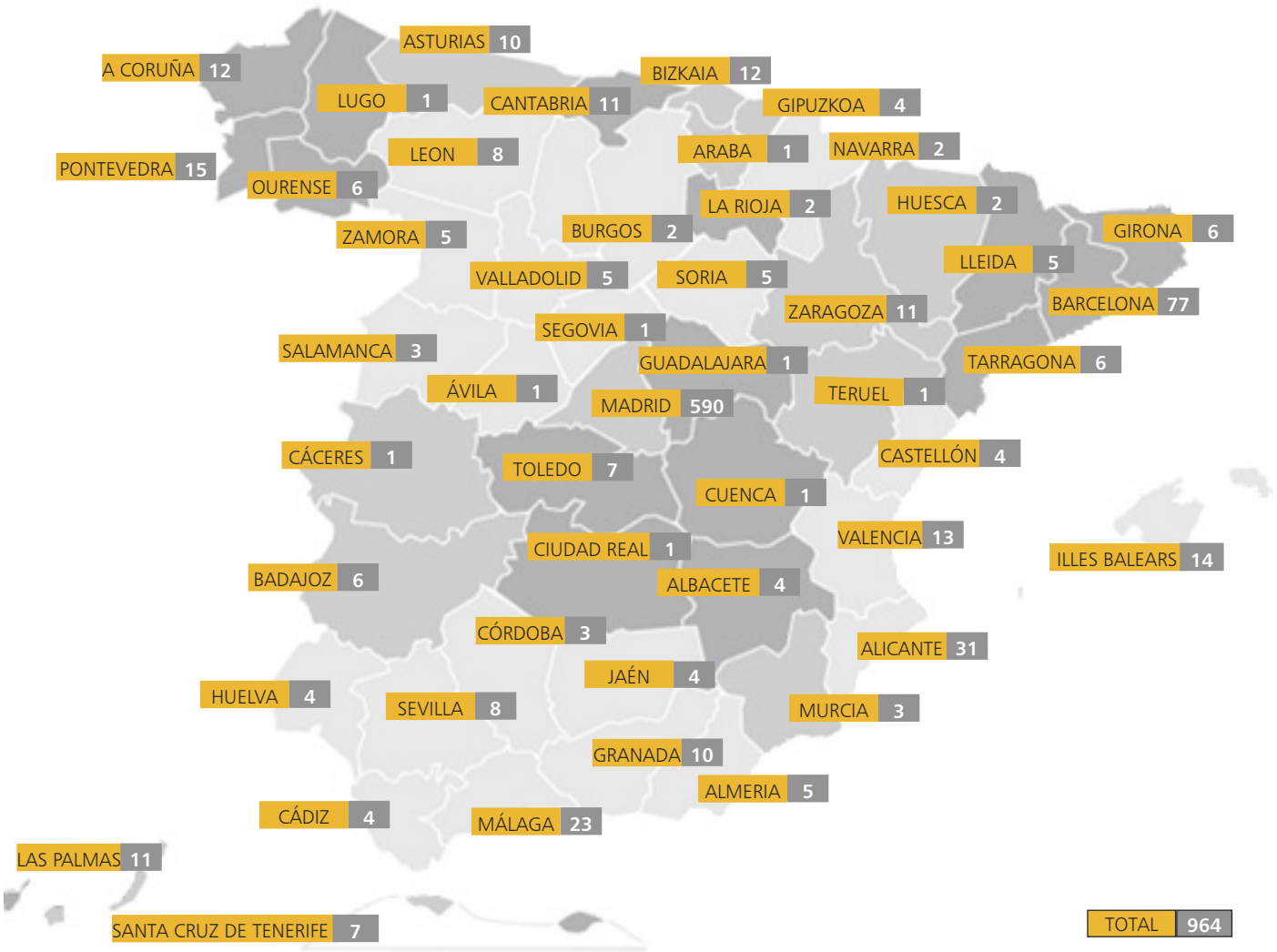
NOTA: En cada procedimiento puede tutelarse más de un derecho ARCO.

DISTRIBUCIÓN GEOGRÁFICA DE LAS DENUNCIAS (PROVINCIA DEL DENUNCIANTE)

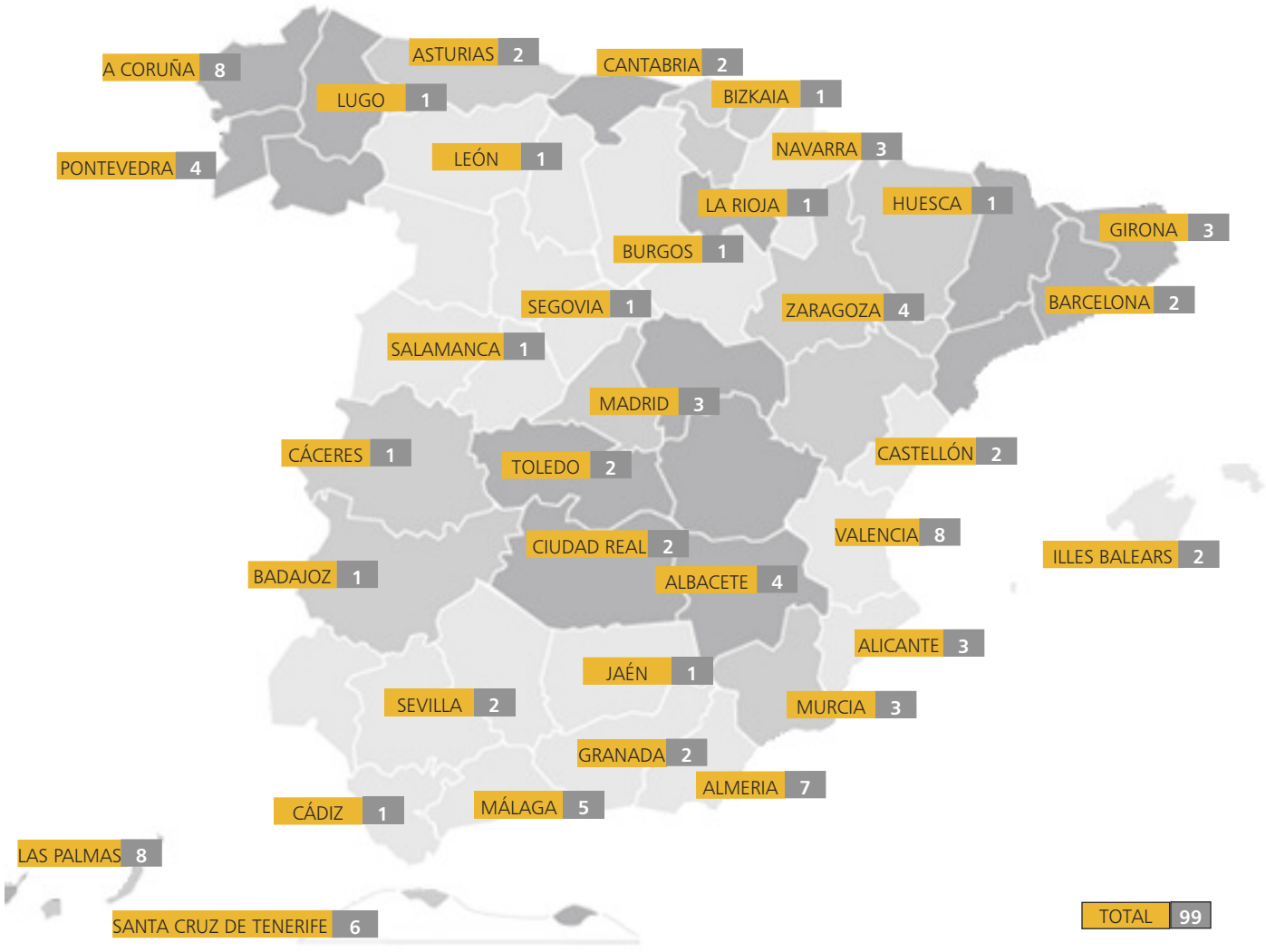


NOTA: No se consideran las actuaciones previas iniciadas de oficio a iniciativa del Director o las iniciadas por solicitud de colaboración de otras autoridades extranjeras de protección de datos.

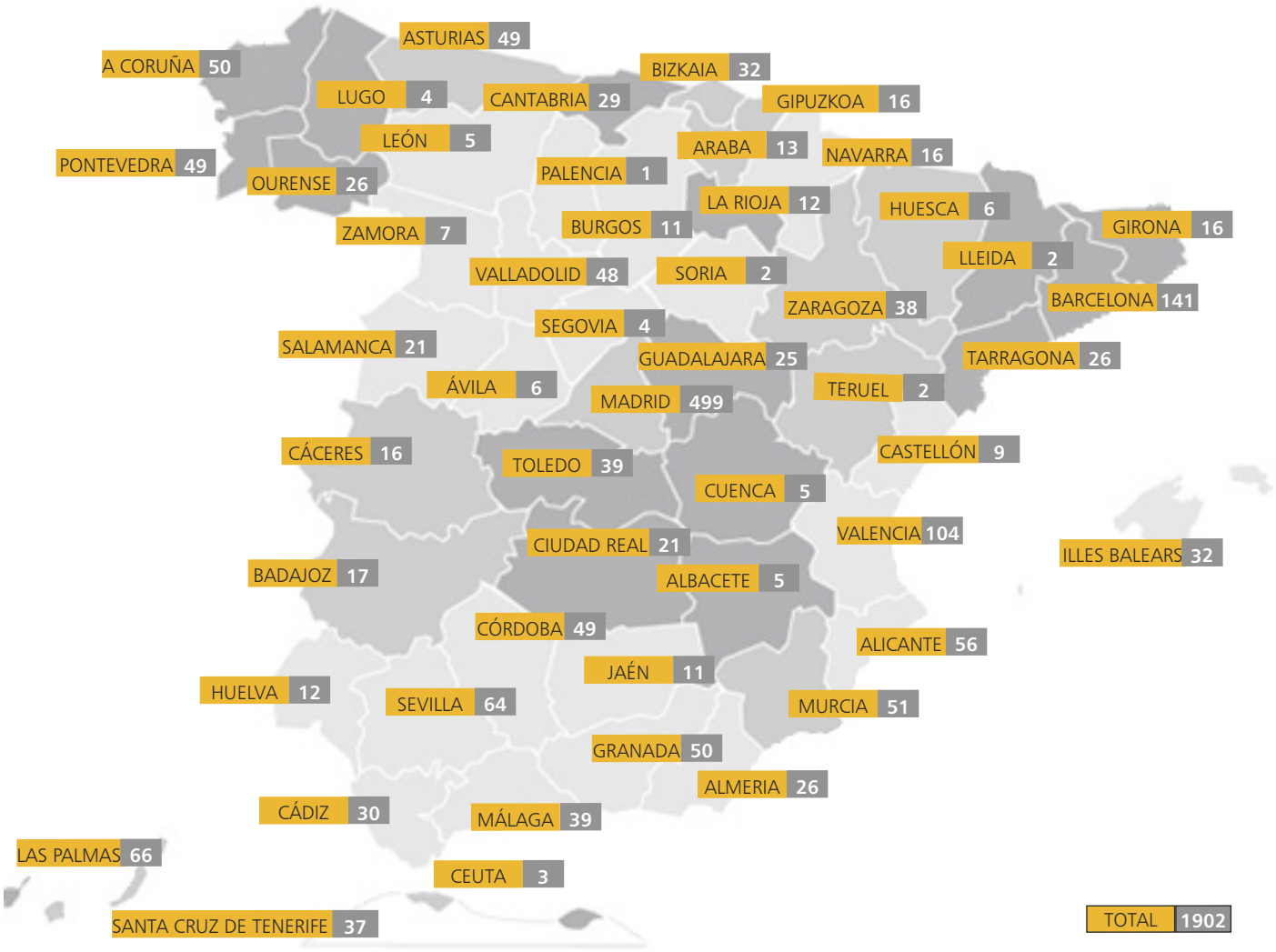
DISTRIBUCIÓN GEOGRÁFICA DE LOS PROCEDIMIENTOS SANCIONADORES



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



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

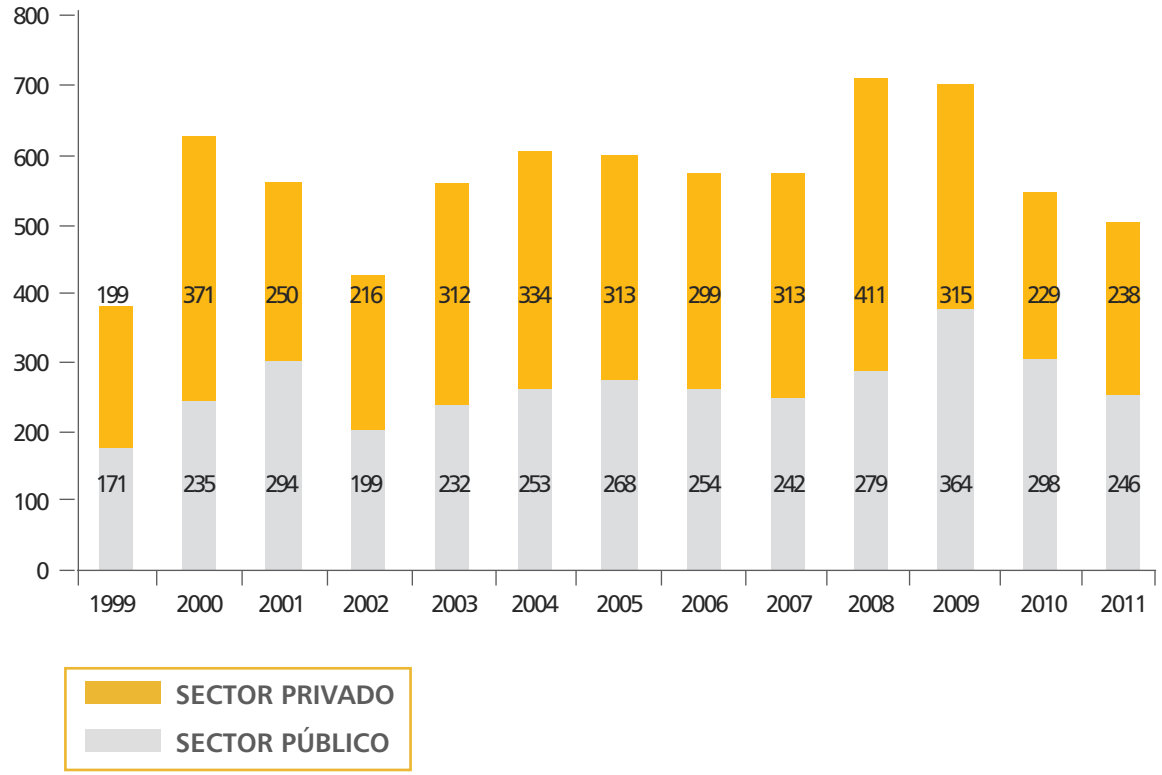


CONSULTAS

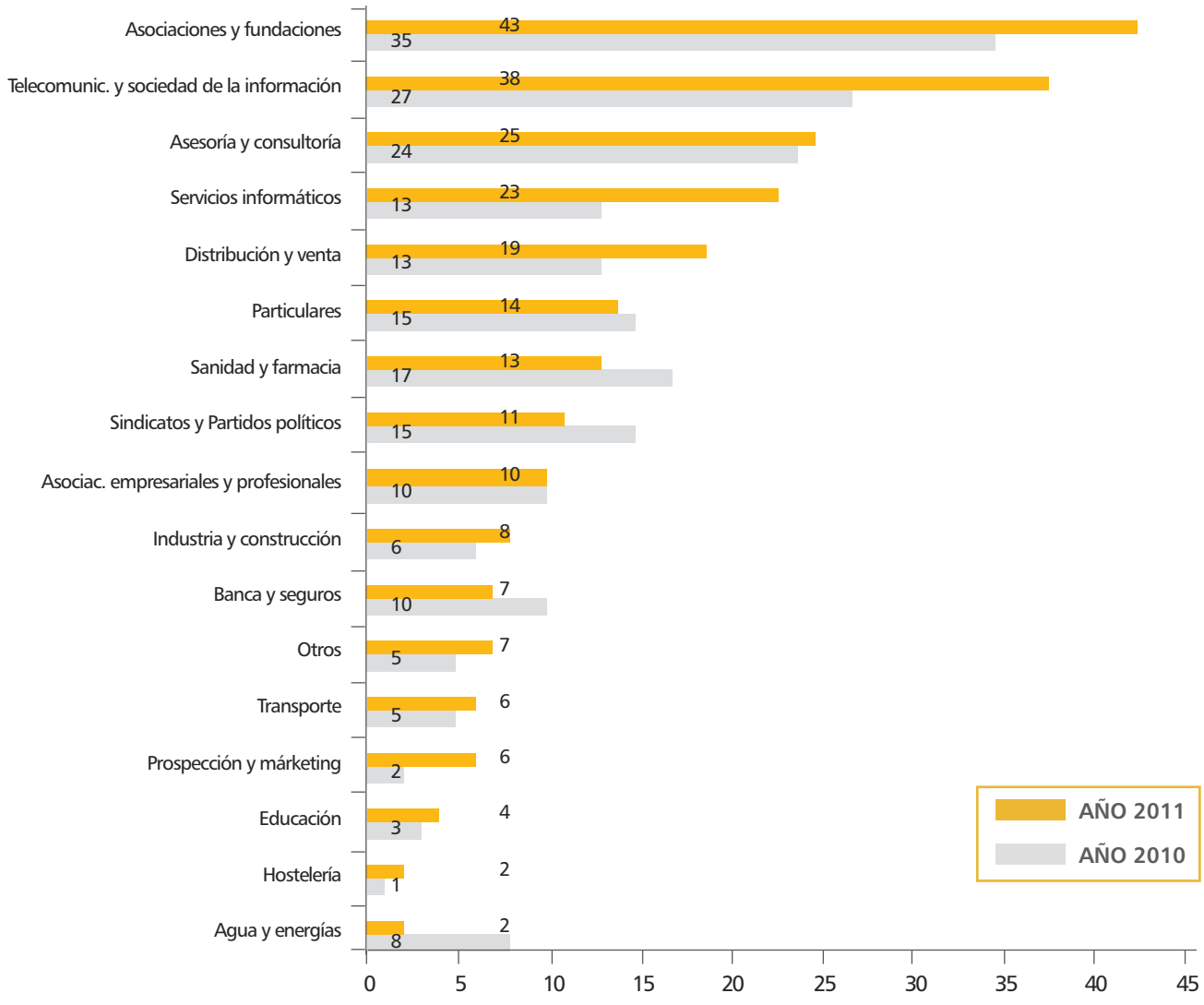
ADMINISTRACIONES PÚBLICAS	246
Administración General del Estado	139
Comunidades Autónomas	44
Entidades Locales	31
Otros Organismos Públicos	32

CONSULTAS PRIVADAS	238
Empresas	166
Particulares	13
Asociaciones / Fundaciones	48
Sindicatos / Partidos políticos	11
Otros	0

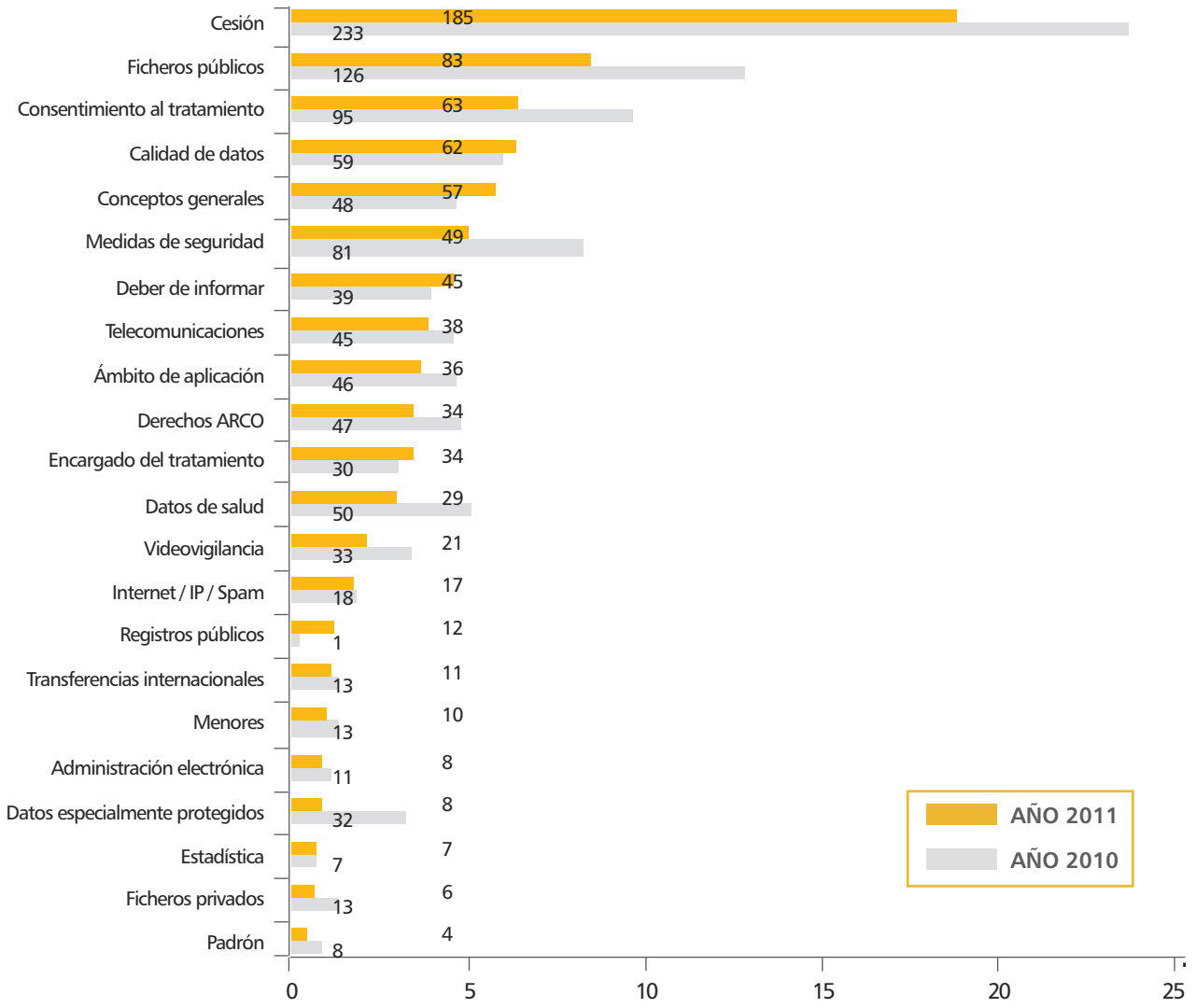
EVOLUCIÓN DE LAS CONSULTAS (1999-2011)



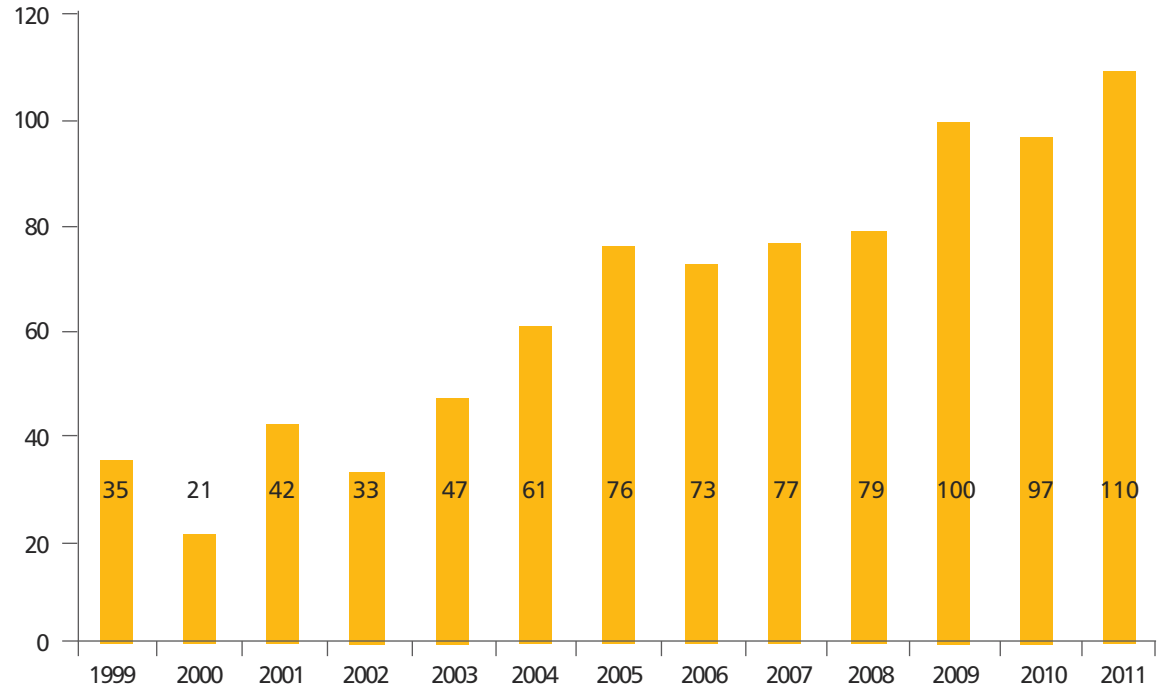
EVOLUCIÓN DE LAS CONSULTAS POR SECTORES (2010-2011)



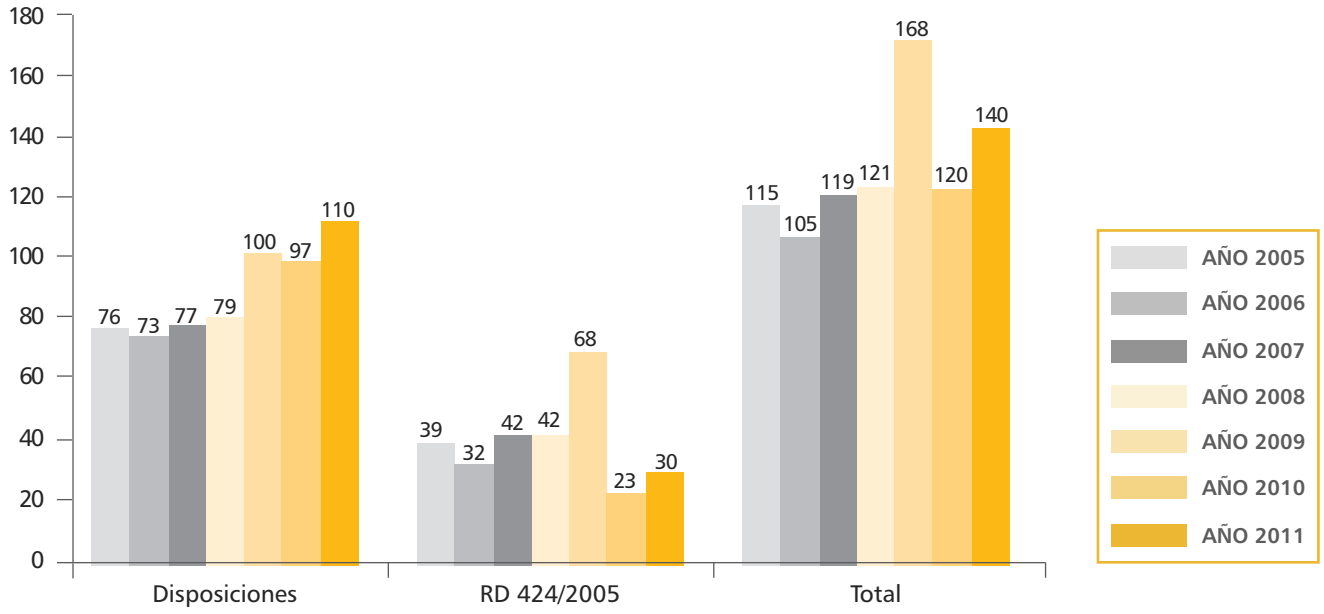
EVOLUCIÓN DE LAS CONSULTAS POR MATERIAS (2010-2011)



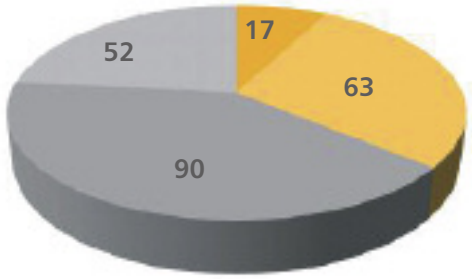
EVOLUCIÓN DE INFORMES PRECEPTIVOS A DISPOSICIONES GENERALES (1999-2011)



INFORMES PRECEPTIVOS (2005-2011)

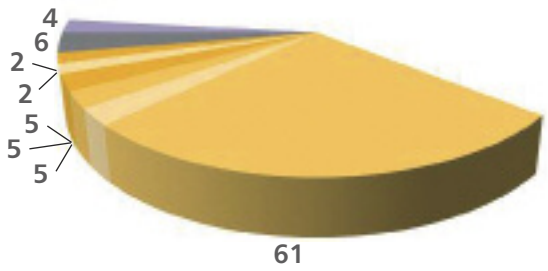


SENTENCIAS DE LA AUDIENCIA NACIONAL EN 2011



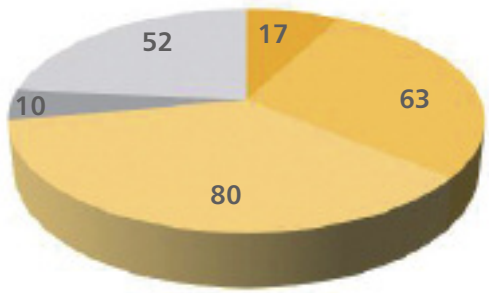
- INADMISIÓN DEL RECURSO
- DESESTIMATORIAS
- PARCIALMENTE ESTIMATORIAS
- ESTIMATORIAS

SENTENCIAS PARCIALMENTE ESTIMATORIAS EN 2011 (FUNDAMENTO)



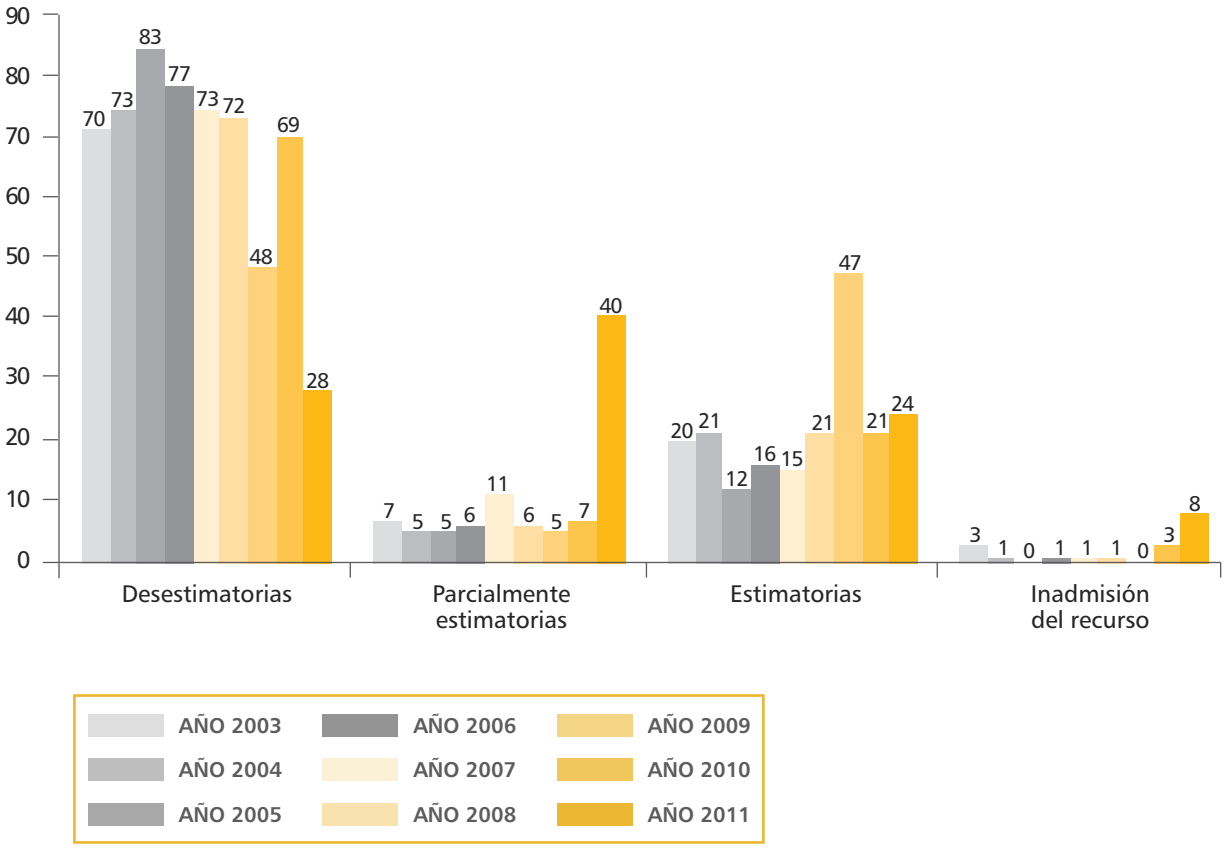
- MÍNIMO GRAVES
- CESIÓN
- REBAJA PROPORCIONAL
- NUEVO 45.5
- REBAJA PROPUESTA POR LA AEPD
- APERCIBIMIENTO
- APLICA 45.5
- OTRAS

SENTENCIAS AN 2011 (CONFIRMACIÓN CRITERIO DE LA AEPD)

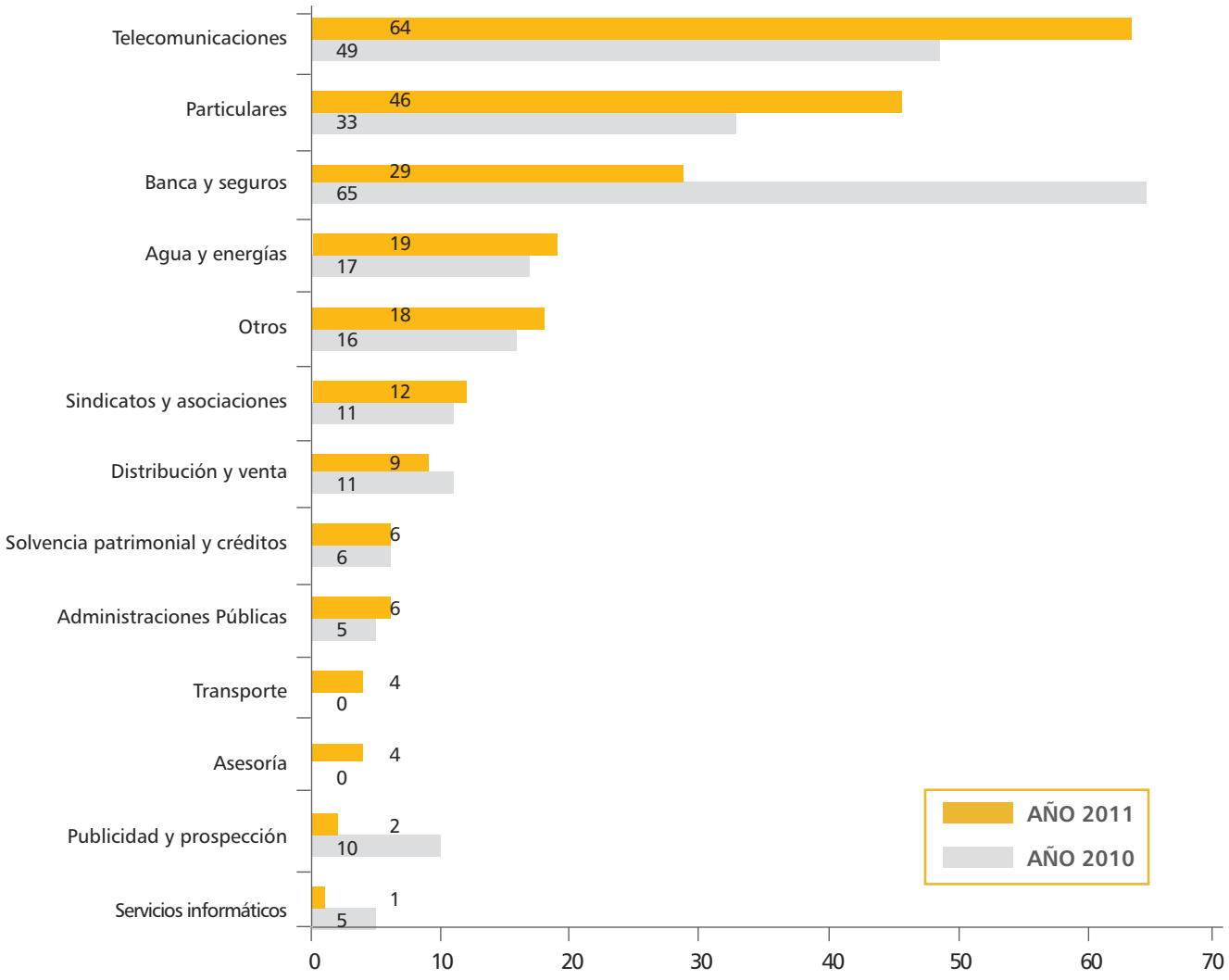


- INADMISIÓN
- DESESTIMATORIAS
- PARCIALMENTE ESTIMATORIAS (APLICACIÓN LES)
- PARCIALMENTE ESTIMATORIAS (ANULACIÓN PARCIAL)
- ESTIMATORIAS

EVOLUCIÓN DE PORCENTAJES EN SENTENCIAS DE LA AUDIENCIA NACIONAL



COMPARATIVA POR SECTOR DEL RECURRENTE (2010-2011)



SENTENCIAS DEL TRIBUNAL SUPREMO EN 2011

CONSULTAS TOTALES PLANTEADAS ANTE EL ÁREA DE ATENCIÓN AL CIUDADANO

	Atención telefónica	Atención presencial	Atención por escrito	Total	% de incremento
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	8,20%
Año 2011	113.579	3.341	17.715(*)	134.635	28,40%

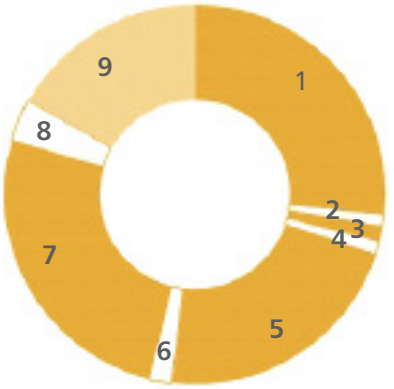
* En el año 2011, **8.999 consultas** escritas se contestaron a través de la página **Web**.

COMPARACIÓN DE ACCESOS A LA PÁGINA WEB CON EL AÑO 2010

AÑO	2010	2011
Accesos Web	2.499.179	2.892.516
Promedio diario	7.619	7.923

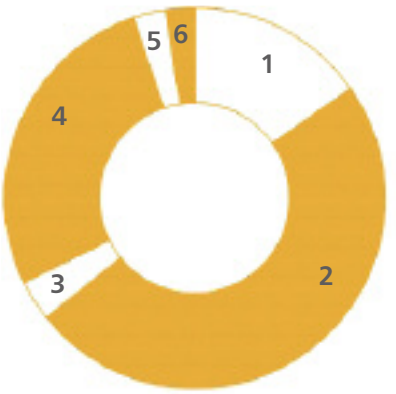
ANÁLISIS DE LAS CONSULTAS POR TEMAS 2011

TEMAS	%
1. Inscripción ficheros	29,86%
2. Nuevo Reglamento	1,21%
3. Comunidades de propietarios	1,36%
4. Internet	1,34%
5. Telecomunicaciones	24,41%
6. Cesión	2,25%
7. Derechos	28,81%
8. Videovigilancia	4,08%
9. Información	18,83%



CONSULTAS SOBRE DERECHOS 2011

TEMAS	%
1. Acceso	15,71%
2. Cancelación	50,35%
3. Rectificación	3,57%
4. Oposición	27,85%
5. Información	2,89%
6. Exclusión de guías	2,50%



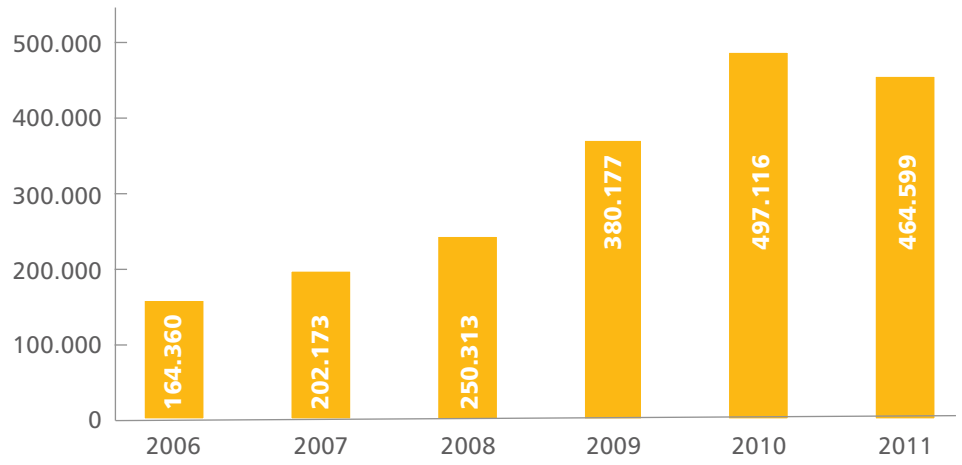
DERECHO DE CONSULTA AL REGISTRO

TITULARIDAD	2010	2011
Privada	2.002.499	2.644.420
Pública	506.351	856.463
TOTAL	**2.508.850**	**3.500.883**

EVOLUCIÓN DE LA INSCRIPCIÓN DE FICHEROS EN EL RGPD

Ficheros inscritos	2006	2007	2008	2009	2010	2011
Titular. Pública	56.138	61.553	85.083	95.696	108.289	117.503
Titular. Privada	758.955	955.713	1.182.496	1.552.060	2.036.583	2.491.968
TOTAL	**815.093**	**1.017.266**	**1.267.579**	**1.647.756**	**2.144.872**	**2.609.471**

INCREMENTO ANUAL TOTAL



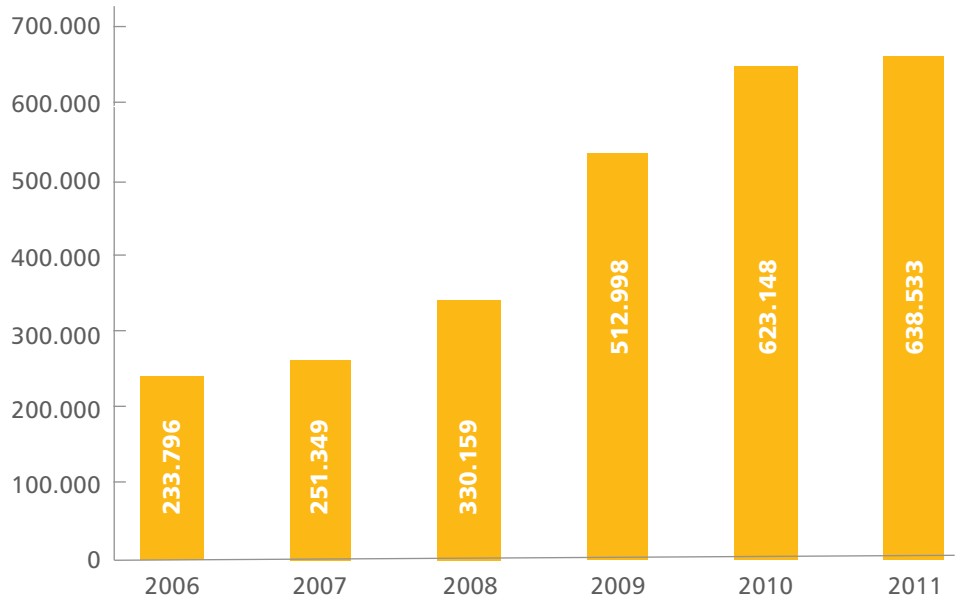
< ÍNDICE >

EVOLUCIÓN DE LA INSCRIPCIÓN EN EL RGPD

DATOS RELACIONADOS CON LA INSCRIPCIÓN

	2010	2011	% Variación 2010-2011	Media diaria en 2010	Media diaria en 2011
Operaciones de Inscripción	623.148	638.533	+ 2	2.596	2.661
Total de ficheros inscritos	2.144.872	2.609.471	+22	2.071	1.936

INCREMENTO ANUAL DE LAS OPERACIONES DE INSCRIPCIÓN



DISTRIBUCIÓN DE FICHEROS

	RESPONSABLES		FICHEROS	
	2011	TOTAL	2011	TOTAL
Comunidad Autónoma de Andalucía	**37.421**	128.254	**92.393**	369.907
Almería	3.394	12.412	8.558	37.294
Cádiz	5.025	15.159	11.823	41.207
Córdoba	3.682	12.168	8.860	34.537
Granada	4.175	17.968	11.056	57.038
Huelva	1.758	5.650	4.288	16.713
Jaén	2.855	10.275	7.717	33.368
Málaga	7.830	28.855	19.905	76.302
Sevilla	8.741	26.395	20.186	73.448
Comunidad Autónoma de Aragón	**6.341**	33.379	**14.984**	81.206
Huesca	1.055	6.521	2.334	15.405
Teruel	724	2.930	1.621	7.505
Zaragoza	4.563	23.977	11.029	58.296
Comunidad Autónoma Principado de Asturias	**5.721**	27.588	**14.126**	83.684
	5.674	19.409	17.262	64.356
Comunidad Autónoma de Canarias	**6.352**	26.502	**17.620**	90.059
Las Palmas	3.061	12.088	8.603	42.276
Santa Cruz de Tenerife	3.295	14.474	9.017	47.783
Comunidad Autónoma de Cantabria	**2.655**	10.359	**6.003**	24.535
Comunidad Autónoma de Castilla y León	**12.759**	45.990	**31.208**	121.410
Ávila	704	2.794	1.526	6.250
Burgos	2.381	8.317	4.971	19.693
León	2.506	8.979	6.163	23.723
Palencia	817	3.629	1.942	9.388
Salamanca	1.468	5.259	4.009	14.241
Segovia	839	3.200	2.222	8.446
Soria	860	2.112	2.052	5.712
Valladolid	2.347	8.951	5.853	24.383
Zamora	847	2.847	2.470	9.574

	RESPONSABLES		FICHEROS	
	2011	TOTAL	2011	TOTAL
Comunidad Autónoma Castilla-La Mancha	**10.636**	32.167	**25.354**	93.813
Albacete	2.208	8.730	5.922	27.750
Ciudad Real	2.750	7.057	6.342	20.707
Cuenca	1.036	3.330	2.661	8.651
Guadalajara	1.185	3.399	2.453	8.647
Toledo	3.461	9.724	7.976	28.058
Comunidad Autónoma de Cataluña	**30.970**	184.472	**78.701**	465.156
Barcelona	22.549	135.789	57.028	336.809
Girona	3.577	22.869	9.801	60.420
Lleida	1.835	9.586	3.809	23.599
Tarragona	3.022	16.560	8.063	44.328
Comunidad de Madrid	**36.969**	150.261	**84.321**	364.769
Comunidad Valenciana	**26.633**	110.148	**64.863**	277.507
Alicante	9.681	37.495	21.228	88.161
Castellón de la Plana	3.338	13.320	8.656	36.281
Valencia	13.628	59.460	34.979	153.065
Comunidad Autónoma de Extremadura	**3.985**	15.173	**11.030**	43.150
Badajoz	2.437	10.024	6.724	27.809
Cáceres	1.551	5.169	4.306	15.341
Comunidad Autónoma de Galicia	**16.353**	65.477	**42.380**	189.961
A Coruña	7.245	28.434	19.228	80.691
Lugo	1.959	8.650	4.388	23.839
Ourense	1.753	7.031	4.592	19.489
Pontevedra	5.407	21.523	14.172	65.942
Comunidad Autónoma de las Illes Balears	**5.674**	19.409	**17.262**	64.356
Comunidad Foral de Navarra	**2.612**	10.590	**6.542**	29.443
Comunidad Autónoma del País Vasco	**9.680**	36.977	**23.148**	95.734
Araba	1.137	4.869	3.060	13.076
Gipuzkoa	3.204	11.225	7.873	29.631
Bizkaia	5.344	20.948	12.215	53.027
Comunidad Autónoma de la Rioja	**1.808**	8.954	**4.360**	22.297
Comunidad Autónoma de Región de Murcia	**7.728**	28.522	**18.034**	71.509
Ciudad Autónoma de Ceuta	**76**	461	**154**	1.015
Ciudad Autónoma de Melilla	**235**	540	**972**	2.354

INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN DE FICHEROS SEGÚN TIPOS DE DATOS	2011	TOTAL
Datos especialmente protegidos (ideología, creencias, religión y afiliación sindical)	**9.430**	70.714
Otros datos especialmente protegidos (origen racial, salud y vida sexual)	**47.213**	321.643
Datos de carácter identificativo	**501.464**	2.491.968
Datos de características personales	**238.261**	1.100.261
Datos de circunstancias sociales	**136.216**	622.321
Datos académicos y profesionales	**142.022**	614.610
Detalles de empleo y carrera administrativa	**160.588**	794.829
Datos de información comercial	**149.312**	681.354
Datos económico-financieros	**285.784**	1.429.792
Datos de transacciones	**229.798**	1.017.929
Otros tipos de datos	**20.821**	98.197

INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN DE FICHEROS SEGÚN SU FINALIDAD	2011	TOTAL	% 2011/TOTAL
Gestión de clientes, contable, fiscal y administrativa	**274.284**	1.562.690	+17,55
Recursos humanos	**114.288**	568.412	+20,11
Gestión de nóminas	**87.794**	430.355	+20,40
Prevención de riesgos laborales	**49.353**	200.501	+24,61
Publicidad y prospección comercial	**38.796**	193.376	+20,06
Videovigilancia	**35.509**	99.593	+35,65
Gestión y control sanitario	**15.243**	110.646	+13,78
Comercio electrónico	**14.472**	41.221	+35,11
Historial clínico	**11.366**	75.833	+14,99
Seguridad y control de acceso a edificios	**8.073**	35.211	+22,93
Fines estadísticos, históricos o científicos	**7.310**	82.857	+8,82
Análisis de perfiles	**7.278**	29.896	+24,34
Educación	**5.390**	33.336	+16,17
Gestión de actividades asociativas, culturales, recreativas, deportivas y sociales	**5.145**	41.186	+12,49
Servicios económicos-financieros y seguros	**4.946**	63.752	+7,76
Cumplimiento/incumplimiento de obligaciones dinerarias	**3.862**	41.357	+9,34
Gestión de asociados o miembros de partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical	**3.827**	13.740	+27,85
Seguridad privada	**3.163**	13.884	+22,78
Guías/repertorios de servicios de comunicaciones electrónicas	**2.908**	6.783	+42,87
Prestación de servicios de comunicaciones electrónicas	**2.648**	12.767	+20,74
Gestión de asistencia social	**2.225**	10.656	+20,88
Prestación de servicios de solvencia patrimonial y crédito	**683**	7.271	+9,39
Investigación epidemiológica y actividades análogas	**681**	8.080	+8,43
Prestación de servicios de certificación electrónica	**326**	2.101	+15,52
Otras finalidades	**87.078**	380.253	+22,90

INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUC. DE FICHEROS SEGÚN EL SECTOR DE ACTIVIDAD	2011	TOTAL	% 2011/TOTAL
Comercio	60.244	285.416	+21,11
Comunidades de propietarios	59.888	322.959	+18,54
Sanidad	29.116	186.782	+15,59
Turismo y hostelería	27.586	107.518	+25,66
Construcción	17.666	101.350	+17,43
Contabilidad, auditoría y asesoría fiscal	15.551	125.808	+12,36
Actividades inmobiliarias	12.580	87.763	+14,33
Educación	11.762	61.540	+19,11
Transporte	10.213	54.501	+18,74
Actividades jurídicas, notarios y registradores	9.157	64.693	+14,15
Asociaciones y clubes	8.804	57.248	+15,38
Industria química y farmacéutica	7.994	54.961	+14,54
Activ. relacionadas con los productos alimenticios, bebidas y tabacos	6.436	34.242	+18,80
Servicios informáticos	5.965	38.933	+15,32
Actividades diversas de servicios personales	4.602	24.792	+18,56
Maquinaria y medios de transporte	4.513	37.406	+12,06
Agricultura, ganadería, explotación forestal, caza, pesca	4.466	28.288	+15,79
Actividades de servicios sociales	4.444	22.832	+19,46
Actividades políticas, sindicales o religiosas	4.367	11.613	+37,60
Seguros privados	3.508	27.222	+12,89
Producción de bienes de consumo	3.127	22.450	+13,93
Comercio y servicios electrónicos	2.979	9.369	+31,80
Sector energético	2.770	19.061	+14,53
Servicios de telecomunicaciones	2.054	11.773	+17,45
Activ. de organizaciones empresariales, profesionales y patronales	1.295	12.016	+10,78
Publicidad directa	1.194	9.612	+12,42
Actividades relacionadas con los juegos de azar y apuestas	940	6.235	+15,08
Seguridad	878	6.909	+12,71
Inspección técnica de vehículos y otros análisis técnicos	851	2.935	+28,99
Entidades bancarias y financieras	851	12.865	+6,61
Organización de ferias, exhibiciones, congresos y otras activ. relac.	633	3.162	+20,02
Investigación y desarrollo (I+D)	539	3.703	+14,56
Selección de personal	426	4.252	+10,02
Activ. postales y de correo (oper. Postales, serv. post., transport.	237	2.680	+8,84
Solvencia patrimonial y crédito	84	1.025	+8,20
Mutualidades colaboradoras de los organismos de la seguridad social	45	829	+5,43
Otras actividades	173.656	593.304	+29,27

INSCRIPCIÓN DE TITULARIDAD PÚBLICA

DISTRIBUCIÓN DE FICHEROS POR TIPO DE ADMÓN.	2011	TOTAL
Administración General	**936**	6.213
Administración CC.AA	**1.986**	20.652
Administración Local	**7.771**	65.264
Otras personas jurídico-públicas	**951**	25.374
TOTAL	**11.644**	117.503

DISTRIBUCIÓN DE FICHEROS DE LA ADMINISTRACIÓN GENERAL

	FICHEROS
Presidencia del Gobierno	43
Ministerio de Asuntos Exteriores y de Cooperación	543
Ministerio de Justicia	146
Ministerio de Defensa	853
Ministerio de Economía y Competitividad	381
Ministerio del Interior	219
Ministerio de Fomento	515
Ministerio de Educación, Cultura y Deporte	232
Ministerio de Empleo y Seguridad Social	1.496
Ministerio de la Presidencia	57
Ministerio de Hacienda y Administraciones Públicas	608
Ministerio de Sanidad, Servicios Sociales e Igualdad	536
Ministerio de Agricultura, Alimentación y Medio Ambiente	370
Ministerio de Industria, Energía y Turismo	214
TOTAL	**6.213**

DISTRIBUCIÓN DE FICHEROS DE COMUNIDADES AUTÓNOMAS

	2011	FICHEROS
Comunidad Autónoma de Andalucía	254	1.890
Comunidad Autónoma de Aragón	64	297
Comunidad Autónoma del Principado de Asturias	82	403
Comunidad Autónoma de Canarias	68	374
Comunidad Autónoma de Cantabria	32	204
Comunidad Autónoma de Castilla y León	60	821
Comunidad Autónoma de Castilla-La Mancha	59	667
Comunidad Autónoma de Cataluña	362	1.376
Comunidad de Madrid	280	10.416
Comunidad Valenciana	37	740
Comunidad Autónoma de Extremadura	50	418
Comunidad Autónoma de Galicia	162	386
Comunidad Autónoma de las Illes Balears	65	508
Comunidad Foral de Navarra	9	156
Comunidad Autónoma del País Vasco	339	1.238
Comunidad Autónoma de La Rioja	21	269
Comunidad Autónoma de la Región de Murcia	40	394
Ciudad Autónoma de Ceuta	0	23
Ciudad Autónoma de Melilla	2	72
TOTAL	**1.986**	**20.652**

DISTRIBUCIÓN DE FICHEROS DE LA ADMINISTRACIÓN LOCAL

	ENTIDADES	FICHEROS
Comunidad Autónoma de Andalucía	**719**	**8.158**
Almería	97	1.109
Cádiz	43	722
Córdoba	74	743
Granada	170	1.469
Huelva	86	1.183
Jaén	85	565
Málaga	57	859
Sevilla	107	1.508
Comunidad Autónoma de Aragón	**527**	**4.527**
Huesca	186	1.601
Teruel	66	365
Zaragoza	275	2.561
Comunidad Autónoma del Principado de Asturias	**72**	**829**
Comunidad Autónoma de Canarias	**93**	**1.461**
Las Palmas	40	646
Santa Cruz de Tenerife	53	815
Comunidad Autónoma de Cantabria	**55**	**558**
Comunidad Autónoma de Castilla y León	**618**	**3.732**
Ávila	83	933
Burgos	74	283
León	201	1.205
Palencia	23	192
Salamanca	84	399
Segovia	18	105
Soria	10	37
Valladolid	86	397
Zamora	39	181

DISTRIBUCIÓN DE FICHEROS DE LA ADMINISTRACIÓN LOCAL

	ENTIDADES	FICHEROS
Comunidad Autónoma de Castilla-La Mancha	**429**	**6.162**
Albacete	96	3.444
Ciudad Real	109	739
Cuenca	87	742
Guadalajara	19	133
Toledo	118	1.104
Comunidad Autónoma de Cataluña	**1.250**	**9.982**
Barcelona	622	4.695
Girona	253	2.482
Lleida	224	1.555
Tarragona	153	1.250
Comunidad de Madrid	**201**	**2.962**
Comunidad Valenciana	**451**	**5.667**
Alicante	147	1.950
Castellón de la Plana	98	886
Valencia	207	2.831
Comunidad Autónoma de Extremadura	**274**	**3.132**
Badajoz	161	1.607
Cáceres	113	1.525
Comunidad Autónoma de Galicia	**299**	**2.845**
A Coruña	94	965
Lugo	62	495
Ourense	78	733
Pontevedra	65	652
Comunidad Autónoma de las Illes Balears	**75**	**1.381**
Comunidad Foral de Navarra	**146**	**1.495**
Autónoma del País Vasco	**274**	**5.332**
Araba	44	430
Gipuzkoa	101	1.977
Bizkaia	129	2.925
Comunidad Autónoma de la Rioja	**38**	**330**
Comunidad Autónoma de la Región de Murcia	**43**	**877**

< ÍNDICE >

DISTRIBUCIÓN DE FICHEROS DE OTRAS PERSONAS JURÍDICO-PÚBLICAS

	FICHEROS
Cámaras Oficiales de Comercio e Industria	453
Notariado	7.938
Universidades	1.095
Colegios Profesionales	2.192
Otros	13.696
Total	**25.374**

INSCRIPCIÓN DE TITULARIDAD PÚBLICA

DISTRIBUCIÓN DE FICHEROS SEGÚN TIPOS DE DATOS	2011	FICHEROS
Datos especialmente protegidos (ideología, creencias, religión y afiliación sindical)	431	18.292
Otros datos especialmente protegidos (origen racial, salud y vida sexual)	1.897	31.261
Datos relativos a infracciones	1.443	21.479
Datos de carácter identificativo	11.644	117.503
Datos de características personales	4.838	61.985
Datos de circunstancias sociales	2.953	33.607
Datos académicos y profesionales	3.243	36.687
Detalles de empleo y carrera administrativa	2.863	39.550
Datos de información comercial	1.487	15.291
Datos económico-financieros	4.285	53.596
Datos de transacciones	1.467	21.961
Otros tipos de datos	1.272	18.252

INSCRIPCIÓN DE TITULARIDAD PÚBLICA

DISTRIBUCIÓN DE FICHEROS CON DATOS SENSIBLES	2011	FICHEROS
Datos especialmente protegidos	**431**	**18.292**
Ideología	171	9.078
Creencias	63	8.410
Religión	107	8.593
Afiliación Sindical	271	17.252
Otros datos especialmente protegidos	**1.897**	**31.261**
Origen Racial	259	10.926
Salud	1.872	31.117
Vida Sexual	138	9.419
Datos relativos a infracciones	**1.443**	**21.479**
Infracciones Penales	598	15.546
Infracciones Administrativas	1.310	20.746

INSCRIPCIÓN DE TITULARIDAD PÚBLICA

DISTRIBUCIÓN DE FICHEROS SEGÚN SU FINALIDAD	2011	TOTAL	% 2011/TOTAL
Procedimiento administrativo	**3.437**	36.951	+9,30
Gestión contable, fiscal y administrativa	**1.319**	17.941	+7,35
Recursos humanos	**1.284**	20.993	+6,12
Educación y cultura	**998**	10.807	+9,23
Gestión de nómina	**619**	11.130	+5,56
Hacienda pública y gestión de administración tributaria	**592**	9.496	+6,23
Fines históricos, estadísticos o científicos	**563**	19.062	+2,95
Servicios sociales	**547**	8.394	+6,52
Gestión sancionadora	**484**	4.736	+10,22
Previsión de riesgos laborales	**422**	2.110	+20,00
Padrón de habitantes	**418**	6.042	+6,92
Seguridad y control de acceso a edificios	**412**	3.116	+13,22
Videovigilancia	**382**	1.456	+26,24
Trabajo y gestión de empleo	**373**	5.209	+7,16
Función estadística pública	**363**	12.230	+2,97
Gestión económica-financiera pública	**351**	6.468	+5,43
Seguridad pública y defensa	**308**	3.815	+8,07
Gestión y control sanitario	**304**	4.740	+6,41
Gestión de censo promocional	**159**	624	+25,48
Publicaciones	**152**	1.604	+9,48
Historial clínico	**149**	2.944	+5,06
Actuaciones de fuerzas y cuerpos de seguridad con fines policiales	**132**	2.663	+4,96
Justicia	**131**	10.404	+1,26
Prestación de servicios de certificación electrónica	**85**	1.495	+5,69
Investigación epidemiológica y actividades análogas	**74**	2.268	+3,26
Otras finalidades	**4.344**	25.399	+17,10

RESOLUCIONES DE AUTORIZACIÓN

	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	Total Auto.
EEUU	1	9	2	6	40	9	16	10	31	28	25	**40**	**217**
Latinoamérica													**299**
Panamá	-	-	-	-	-	2	-	-	-	-	-	-	**2**
Colombia	-	-	-	-	-	1	4	9	4	12	22	**23**	**75**
Chile	-	-	-	-	-	1	7	9	1	8	9	**7**	**42**
Uruguay	-	-	-	-	-	1	1	1	4	3	13	-	**23**
Perú	-	-	-	-	-	-	4	5	4	19	20	**30**	**82**
Guatemala	-	-	-	-	-	-	1	-	1	1	-	-	**3**
Paraguay	-	-	-	-	-	-	1	1	4	4	1	**4**	**15**
Brasil	-	-	-	-	-	-	-	1	3	-	1	**2**	**7**
El Salvador	-	-	-	-	-	-	-	1	-	-	-	-	**1**
Costa Rica	-	-	-	-	-	-	-	1	1	-	1	**1**	**4**
Nicaragua	-	-	-	-	-	-	-	1	-	-	-	-	**1**
México	-	-	-	-	-	-	-	-	3	8	20	**12**	**43**
Ecuador	-	-	-	-	-	-	-	-	-	-	1	-	**1**
India	-	-	-	-	4	-	3	2	30	28	14	**29**	**110**
Otros países													**138**
Marruecos	1	-	-	-	2	2	2	1	3	8	7	**4**	**30**
Singapur	-	-	-	-	1	-	1	2	-	-	1	**2**	**7**
Japón	-	-	-	-	-	1	-	1	-	1	1	**3**	**7**
Malasia	-	-	-	-	-	1	1	1	-	3	-	-	**6**
Tailandia	-	-	-	-	-	1	-	1	-	-	-	-	**2**
Filipinas	-	-	-	-	-	-	3	1	5	4	3	**5**	**21**
China	-	-	-	-	-	-	1	1	3	3	1	**14**	**23**
Hong Kong	-	-	-	-	-	-	1	-	-	1	1	-	**3**
Egipto	-	-	-	-	-	-	-	1	-	-	-	-	**1**
Nigeria	-	-	-	-	-	-	-	1	-	-	-	-	**1**
Túnez	-	-	-	-	-	-	-	1	-	-	2	-	**3**
Sudáfrica	-	-	-	-	-	-	-	-	3	-	-	-	**3**
Australia	-	-	-	-	-	-	-	1	-	7	-	-	**8**
Canadá	-	-	-	-	-	-	-	1	-	-	-	-	**1**
Rep. Bielorrusa	-	-	-	-	-	-	-	-	3		-	-	**3**
Mónaco	-	-	-	-	-	-	-	-	-	1	-	-	**1**
Israel	-	-	-	-	-	-	-	-	-	1	6	2	**9**
Vietnam	-	-	-	-	-	-	-	-	-	-	3	-	**3**
Barbados	-	-	-	-	-	-	-	-	-	-	3	-	**3**
Bermuda	-	-	-	-	-	-	-	-	-	-	1	-	**1**
Andorra	-	-	-	-	-	-	-	-	-	-	1	-	**1**
Mauricio	-	-	-	-	-	-	-	-	-	-	-	1	**1**
Internacional	-	-	-	-	-	-	-	-	-	-	3	1	**4**
Solic. presentadas	2	9	2	19	56	45	54	127	137	166	197	202	**1016**
Archivadas	-	-	-	13	6	16	17	68	42	24	39	22	**247**
Total Autorizac.	**2**	**9**	**2**	**6**	**47**	**19**	**46**	**43**	**103**	**128**	**155**	**175**	**735**

FICHEROS DE VIDEOVIGILANCIA

Año de Inscripción	Titularidad Privada	Titularidad Pública	Total
1994 - 2006	1.004	15	1.019
2007	4.637	86	4.723
2008	8.974	171	9.145
2009	21.403	275	21.678
2010	31.716	791	32.507
2011	36.308	495	36.803
TOTAL	**104.042**	**1.833**	**105.875**

FICHEROS DE VIDEOVIGILANCIA DE TITULARIDAD PRIVADA

ACTIVIDAD PRINCIPAL	2010	2011	% VARIAC.
Comercio	15.181	**23.915**	+57,53
Turismo y hostelería	8.536	**12.741**	+49,26
Comunidades de propietarios	5.277	**7.838**	+48,53
Sanidad	3.766	**5.432**	+44,24
Construcción	1.809	**2.486**	+37,42
Activ. relacionadas con los productos alimenticios, bebidas y tabacos	1.675	**2.456**	+46,63
Industria química y farmacéutica	1.773	**2.322**	+30,96
Transporte	1.384	**1.967**	+42,12
Actividades inmobiliarias	1.073	**1.485**	+38,40
Educación	969	**1.428**	+47,37
Servicios informáticos	971	**1.314**	+35,32
Maquinaria y medios de transporte	925	**1.262**	+36,43
Seguridad	987	**1.199**	+21,48
Sector energético	846	**1.129**	+33,45
Asociaciones y clubes	656	**954**	+45,43
Contabilidad, auditoría y asesoría fiscal	631	**945**	+49,76
Producción de bienes de consumo	624	**868**	+39,10
Agricultura, ganadería, explotación forestal, caza, pesca	501	**823**	+64,27
Actividades relacionadas con los juegos de azar y apuestas	650	**822**	+26,46
Servicios de telecomunicaciones	548	**743**	+35,58
Actividades diversas de servicios personales	491	**676**	+37,68
Actividades de servicios sociales	436	**637**	+46,10
Comercio y servicios electrónicos	301	**470**	+56,15
Actividades jurídicas, notarios y registradores	301	**448**	+48,84
Entidades bancarias y financieras	269	**311**	+15,61
Seguros privados	181	**271**	+49,72
Act. de organizaciones empresariales, profesionales y patronales	186	**219**	+17,74
Actividades políticas, sindicales o religiosas	87	**173**	+98,85
Inspección técnica de vehículos y otros análisis técnicos	98	**136**	+38,78
Organización de ferias, exhibiciones, congresos y otras act. relac.	78	**122**	+56,41
Investigación y desarrollo (I+D)	81	**113**	+39,51
Publicidad directa	73	**112**	+53,42
Act. postales y de correo (oper. postales, serv. post., transport.)	50	**65**	+30,00
Selección de personal	20	**30**	+50,00
Mutualidades colaboradoras de los organismos de la S. S.	16	**19**	+18,75
Solvencia patrimonial y crédito	8	**9**	+12,50
Otras actividades	17.406	**28.102**	+61,65
TOTAL	**68.864**	**104.042**	**+51,08**

COMISIÓN EUROPEA

SESIONES PLENARIAS GT29 EN BRUSELAS (5):

- 10, 11 Febrero 2011
- 03 – 06 Abril 2011
- 29 – 31 Mayo 2011
- 13, 14 Octubre 2011
- 07, 08 Diciembre 2011

REUNIONES DE SUBGRUPOS EN LA COMISIÓN EUROPEA (BRUSELAS) A LAS QUE ASISTE LA AGPD (25):

- Subgrupo Travellers' data: 24 Marzo; 07 Septiembre.
- Subgrupo Futuro de la Privacidad: 18 - 20 Enero; 23, 24 Febrero; 12,13 Julio; 12 Octubre.
- Subgrupo Medical Data: 10 Mayo; 14 Junio; 13 Septiembre.
- Subgrupo Health Data: 28, 29 Marzo.
- Subgrupo Asuntos Financieros- Swift: 11, 12 Abril; 13 Septiembre.
- Subgrupo de Tecnología: 18 Enero; 14 Marzo; 14 Abril; 13 Septiembre; 20 Septiembre; 09 Noviembre.
- Subgrupo Datos Biométricos+ e-Government: 09 – 11 Marzo; 19 Mayo; 12 Julio; 27 Octubre.
- Subgrupo BTLE: 22 Noviembre
- Subgrupo Key Provisions: 25 Enero; 17 Marzo.

REUNIONES DE GRUPOS DE EXPERTOS EN LA COMISIÓN EUROPEA (BRUSELAS) A LAS QUE ASISTE LA AGPD (10):

- Grupo Data Retention: 17 Mayo; 22 Junio; 27- 30 Septiembre.
- Grupo Internet of Things: 7, 8 Febrero; 18, 19 Abril; 30 Junio; 04 Julio; 16 Septiembre.
- Grupo ENISA: 11 Mayo; 20, 21 Octubre.

OTRAS REUNIONES (3):

- 05 Septiembre, Zurich
- DPA'S + V. Reading, 09 Septiembre
- OBA + Estrategia WP29, 14 Septiembre.

CONSEJO DE EUROPA (4):

- 21 - 24 Marzo, Estrasburgo.
- 27 - 30 Junio, Estrasburgo.
- 09 -12 Octubre, Estrasburgo.
- 28 Noviembre – 02 Diciembre, Estrasburgo.

AUTORIDADES DE CONTROL COMÚN (22):

- ACC del Convenio de Schenguen: 28 Febrero – 3 Marzo; 05 - 07 Junio, 27 -30 Septiembre.
- ACC del Convenio de Europol: 28 Febrero – 3 Marzo; 05 – 07 Junio, 27 -30 Septiembre.
- ACC Sistema de Información Aduanero: 28 Febrero – 3 Marzo; 05 – 07 Junio, 27 -30 Septiembre.
- ACC Eurodac: 28 Febrero – 3 Marzo; 05 – 07 Junio, 27 -30 Septiembre.
- Grupo de Trabajo de Policía y Justicia: 2 Febrero; 05 – 07 Junio, 27 -30 Septiembre.
- Comsejo. Informe Resolución Schengen: 16, 17 Noviembre Bruselas.
- Europol Inspección: 14 – 18 Marzo; 29, 30 Marzo.
- Europol Inspección TFTP: 14, 15 Noviembre.
- Inspección Schengen Países Nórdicos: 02 – 12 Octubre.
- Data Retention: 27 – 30 Septiembre.
- Europol Reunión: 16 Febrero.

OCDE (3):

- 09, 10 Junio, París.
- 01 Noviembre, México.
- 01, 02 Diciembre, París.

GRUPOS DE TRABAJO SECTORIALES:

- Grupo de telecomunicaciones de Berlín: (2)
  - 02 – 06 Abril, Montreal (CANADÁ)
  - 06, 07 Septiembre Berlín.
- Taller de reclamaciones (1).
  - 03 – 05 Octubre Varsovia.

CONFERENCIAS INTERNACIONALES (6):

- Data Protection Conference 2011, 23, 24 Febrero - Edimburgo
- IAPP Washington 2011, 7 – 11 Marzo – Washington.
- Mini Spring Conference, 4 Abril – Bruselas.
- Conferencia Internacional, 16 – 17 Junio Budapest.
- RIPD, 30 Octubre México.
- 33ª Conferencia Internacional de Autoridades de Protección de Datos, 01 – 04 Noviembre, México.

OTRAS REUNIONES (6):

- Data Protection and Data Transfer to third Countries, 15 – 17 Mayo Skopje.
- European Data Protection Day, 17 Mayo, Berlin.
- BCR, 15 Junio, Varsovia.
- Seminario OEA 09 – 12 Junio, Santo Domingo.
- Privacy Laws, 11 – 13 Julio, Cambridge.
- Conferencia Ethical Issues in Security Research, 29 Septiembre Bruselas.

IBEROAMÉRICA

SEMINARIOS Y ENCUENTROS

- **5 al 7 de abril:** Celebración en el Centro de Formación de la Agencia Española de Cooperación Internacional para el Desarrollo (AECID) en La Antigua (Guatemala) del "Seminario sobre el acceso a la información pública y protección de datos. La protección de datos en las cédulas y documentos de identificación de los ciudadanos".

- **14 al 16 de junio:** Celebración en el Centro de Formación de la Agencia Española de Cooperación Internacional para el Desarrollo (AECID) en la ciudad de Cartagena de Indias (Colombia), el Seminario "El impacto de las trasferencias internacionales de datos en América Latina. Las políticas preventivas y la autorregulación en la implantación de la normativa de protección de datos".

- **31 de octubre:** Celebración del IX Encuentro de la Red en la ciudad de México, en el marco de la 33 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad.

VISITAS INSTITUCIONALES

- **16 de febrero:** Visita de una delegación del gobierno colombiano para presentar el proyecto de Ley Estatutaria nº 46 de 2010 Cámara, por la cual se dictan Disposiciones Generales para la Protección de Datos Personales, proyecto normativo "habeas data", y comentar aspectos sobre la normatividad secundaria.

- **6 de mayo:** Visita de una delegación de la Comisión de Transparencia y Acceso a la Información del Estado de Nuevo León (México) con la finalidad de firmar un convenio de colaboración para promover la difusión del derecho a la protección de datos, el fomento de estudios e investigaciones, así como el intercambio de experiencias de mutuo interés.

- **26 de mayo:** Visita de una delegación del consejo para la Transparencia de Chile con la finalidad de firmar un convenio de colaboración con el objeto de establecer un marco de colaboración y coordinación institucional entre ambos entes con la finalidad de promover la difusión del derecho a la protección de datos, el fomento de estudios e investigaciones, así como el intercambio de de experiencias de mutuo interés.

- **22 de noviembre a 25 de noviembre:** Visita de una delegación en representación del IFAI para realizar un análisis en profundidad del funcionamiento de distintas áreas de la AEPD.

GESTIÓN DE RECURSOS HUMANOS

PUESTOS DE TRABAJO	DOTACIÓN	EFECTIVOS
	Funcionarios **157**	154
	Laborales **7**	2
	Alto cargo **1**	1

NIVEL	30	29	28	26	24	22	20	18	17	16	15	14
Efectivos 2011	6	3	22	44	3	15	3	12	2	7	12	25

GRUPO	A1	A2	B	C1	C2
Efectivos 2011	31	47	0	24	52

GRUPO	TOTAL
Mujeres	91
Hombres	69

EVOLUCIÓN DEL PRESUPUESTO DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS DURANTE LOS EJERCICIOS 2008 A 2011

	CRÉDITO EJERCICIO 2008 (euros)	CRÉDITO EJERCICIO 2009 (euros)	CRÉDITO EJERCICIO 2010 (euros)	CRÉDITO EJERCICIO 2011 (euros)
CAPITULO I	5.292.866,85	6.692.929,00	6.747.004,93	6.283.509,00
CAPITULO II	6.189.248,11	6.701.771,00	6.620.095,07	5.805.060,00
CAPITULO III	47.555,34	12.290,00	127.290,00	697.841,00
CAPITULO VI	1.900.770,00	1.900,770,00	1.900.770,00	1.625.160,00
CAPITULO VIII	10.000,00	10.000,00	30.000,00	26.400,00
TOTAL	**13.440.440,30**	**15.317.760,00**	**15.425.160,00**	**14.437.970,00**

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

MEMORIA AEPD2011

www.agpd.es

ISSN 2254-691X