



MEMORIA

AEPD

2015

ISSN 2254-691X
Depósito Legal: M-12773-2016

© Agencia Española de Protección de Datos

Realiza: Imprenta Nacional
Agencia Estatal Boletín Oficial del Estado



MEMORIA AEPD 2015

P RÓLOGO

Es un honor presentar por primera vez como Directora de la Agencia Española de Protección de Datos la Memoria de esta institución. Recojo así el testigo del anterior Director, José Luis Rodríguez Álvarez, al que corresponde la gestión e iniciativas desarrolladas en la mitad del año recogido en esta Memoria. El texto incluye de forma detallada, entre otras líneas principales, el reflejo del funcionamiento y las actividades realizadas durante 2015; el análisis de las tendencias legislativas, jurisprudenciales y doctrinales; el estudio y la valoración de los retos a los que se enfrenta la protección de datos; y la planificación y decisiones adoptadas por este organismo para afrontar los desafíos más relevantes que van a producirse a corto plazo.

La protección de datos se enfrenta a unos retos cada vez más importantes y decisivos para salvaguardar este derecho fundamental de los ciudadanos, un ámbito en el que va a ser más necesaria la prevención y la actitud proactiva en el cumplimiento de las obligaciones. El Plan Estratégico 2015-2019 que aparece recogido en esta Memoria y que puede ser consultado de forma íntegra en la web de la Agencia, recoge las líneas prioritarias que nos hemos establecido para dar una respuesta eficaz a las múltiples líneas de trabajo que se plantean en un mundo hiperconectado y globalizado. Para hacerlo, nos hemos propuesto contar con la participación de todos los implicados, fomentando una institución colaboradora y transparente que considera la prevención como una herramienta imprescindible. Esa prevención debe ser difundida entre todos los actores, tanto entre los ciudadanos para que sean conscientes de los derechos que les asisten y cómo ejercerlos como entre aquellos que tratan datos, para que abandonen la idea de considerar la protección de datos como un freno al desarrollo y la tengan presente de forma imprescindible en el desarrollo de sus productos y servicios, fomentando un clima de confianza y una ventaja empresarial. La intención de la Agencia es que la protección de datos sirva para construir un modelo basado en la confianza que evite

la sospecha e incluso el rechazo a las nuevas tecnologías por parte de las personas.

Mucho han cambiado las circunstancias desde que en 2007 este organismo recibió las tres primeras reclamaciones de ciudadanos que solicitaban ayuda a la Agencia para ejercitar el denominado derecho al olvido, para evitar que Google mostrase determinadas páginas cuando se realizaba una búsqueda a través de sus nombres. La sentencia del Tribunal de Justicia de la Unión Europea de 2014 clarificó definitivamente el régimen de responsabilidades y respaldó los planteamientos de la Agencia, que en la actualidad se aplican en toda Europa. En la línea de seguir trabajando para otorgar al ciudadano un mayor control sobre su información personal hay que mencionar también los avances realizados a instancias de la Agencia en la política de privacidad que Google ofrece a nivel mundial a sus usuarios. Tras declarar tres infracciones graves y requerir a la compañía para que adoptase medidas para ajustar su política de privacidad a la normativa, la Agencia ha constatado que, tal y como se le solicitaba, Google ha introducido modificaciones significativas en diferentes áreas, adoptando además el compromiso de mantener un diálogo constante con la AEPD.

La Agencia ha trabajado y va a seguir trabajando en informar a los ciudadanos de sus derechos a través de diferentes vías. Las consultas atendidas en 2015 por el servicio de Atención al ciudadano se han incrementado más del 10% respecto al año anterior. Además, vamos a lanzar en 2016 varias iniciativas, tanto en solitario como en colaboración con otras organizaciones, con las que intentaremos ampliar la concienciación de la ciudadanía sobre la importancia de proteger adecuadamente su información personal. De hecho, el Plan Estratégico prevé entre otras actuaciones la elaboración o actualización de más de una veintena de guías y más de 100 actuaciones que pretendemos poner en marcha en diferentes ámbitos. Dentro de estas actuaciones, la prevención y sensibilización a los menores en el uso responsable de las nuevas tecnologías constituye

MEMORIA 2015

una de las prioridades de este organismo. En el año 2015 pusimos en funcionamiento un teléfono y un servicio de whatsapp especializado en atención a las familias, los centros educativos y los jóvenes, y elaboramos un material didáctico con orientaciones básicas en esta materia.

En cuanto a denuncias y reclamaciones planteadas por los ciudadanos ante este organismo por una posible vulneración de sus derechos o para solicitar la tutela de esta Agencia, el año 2015 supone la consolidación de las cifras registradas en 2013 tras el repunte de 2014. A este respecto hay que destacar el esfuerzo realizado por el personal de la Agencia para su tramitación, ya que en 2015 se resolvieron un 15,70% más que en el año anterior. En este sentido hay que mencionar que a finales de año esta institución puso en marcha una Unidad de admisión a trámite de las reclamaciones de los ciudadanos, encargada específicamente de analizar las denuncias recibidas para permitir, en un breve lapso temporal desde su presentación, indicar las evidencias en las que la colaboración del reclamante es necesaria para fundar la reclamación, ofreciendo información sobre cómo pueden obtenerlas. Creemos que esta Unidad será de gran utilidad para profundizar en una respuesta eficaz y adaptada a las demandas de los ciudadanos.

En cuanto a las resoluciones de apercibimiento, estas se han incrementado de forma importante respecto a 2014 (26%). La utilización de esta figura tiene como objetivo salvaguardar los intereses de las personas o entidades sin merma de las garantías y obligaciones contenidas en la LOPD, teniendo en cuenta entre otros aspectos la entidad y el carácter del denunciado (particulares o pequeñas empresas).

Me he referido en este texto con anterioridad al esfuerzo realizado por el personal de la Agencia para afrontar la creciente carga de trabajo experimentada en los últimos años, no sólo en un plano cuantitativo sino también cualitativo, una labor que merece el reconocimiento y agradecimiento desde estas líneas.

Ese salto cualitativo en las materias tratadas es algo que también se observa en las consultas de mayor complejidad, siendo más singulares las características de las situaciones y tratamientos a los que las cuestiones se refieren.

El Reglamento europeo de protección de datos, que se recoge en diferentes apartados de esta Memoria, va a suponer modificaciones en la legislación y la práctica de protección de datos en el conjunto de la Unión, en los Estados miembros y en la forma de trabajar de las Autoridades. En lo que respecta al funcionamiento de la Agencia, la nueva normativa va a consolidar el carácter especializado e independiente de las Autoridades de protección de datos y a llevar a un nuevo plano las labores de coordinación entre ellas –una cooperación de la que la Agencia ya ha formado parte en múltiples ocasiones– lo que previsiblemente va a suponer una adaptación de los procesos internos. La puesta en marcha de este marco legal va a constituir una nueva estructura que trata de responder a los desafíos incorporando muchas de las ideas sobre las que hemos venido trabajando en la Agencia en los últimos años. Conceptos como la rendición de cuentas por parte del responsable, con elementos como la privacidad desde el diseño, la figura del delegado de protección de datos o la notificación de quejas de seguridad van a contribuir a que los responsables realicen una gestión de la protección de datos más efectiva y ajustada al riesgo, a la vez que más respetuosa con los derechos de los ciudadanos. El objetivo final es ofrecer las herramientas necesarias para que aquellos obligados al cumplimiento de la legislación demuestren, de forma transparente, que tienen un compromiso efectivo con la protección de los datos de los ciudadanos. En esa misión, los ciudadanos, los responsables y los profesionales de la privacidad nos encontrarán siempre a su lado.

Mar España Martí
DIRECTORA DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

ÍNDICE

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

2 PRÓLOGO

1

8 CIUDADANOS MEJOR INFORMADOS: NUEVOS CANALES DE COMUNICACIÓN

2

22 GARANTIZAR LOS DERECHOS DE LOS CIUDADANOS

- 22 A-HERRAMIENTAS PARA FACILITAR EL CUMPLIMIENTO DE LA LOPD
- 34 B-UNA RESPUESTA INTEGRAL PARA GARANTIZAR LOS DERECHOS DE LOS CIUDADANOS
- 52 C-LA SEGURIDAD JURÍDICA COMO OBJETIVO PRIMORDIAL

3

64 LA PROTECCIÓN DE LOS MENORES: UNA APUESTA ESTRATÉGICA PARA EL PRESENTES Y FUTURO DE LA PRIVACIDAD

4

69 EL PLAN ESTRATÉGICO 2015-2019. UNA HERRAMIENTA PARA DAR RESPUESTA A LAS NECESIDADES DE LOS CIUDADANOS, LOS RESPONSABLES Y LOS PROFESIONALES DE LA PROTECCIÓN DE DATOS

5

73 DESAFÍOS PARA LA PRIVACIDAD: PRESENTES Y FUTURO

- 73 A-ACTUALIZACIÓN DEL MARCO JURÍDICO DE LA UNIÓN EUROPEA EN MATERIA DE PROTECCIÓN DE DATOS
- 81 B-ACTUACIÓN COORDINADA EN RELACIÓN CON LA NUEVA POLÍTICA DE PRIVACIDAD DE GOOGLE
- 83 C-LA STJUE DE 6 DE OCTUBRE SOBRE LA DECISIÓN DE PUERTO SEGURO (DECISIÓN 2000/520/CE)
- 86 D-INSPECCIÓN CONJUNTA SOBRE EL USO DE COOKIES - COOKIE SWEEP
- 88 E-LA INSPECCIÓN DE LOS SERVICIOS DE CLOUD COMPUTING EN EL SECTOR EDUCATIVO

MEMORIA 2015

6	
91 MARCOS SUPRANACIONALES DE PROTECCIÓN DE DATOS	
91 A-ACTUALIZACIÓN DEL CONVENIO 108 DEL CONSEJO DE EUROPA	100 E-CONFERENCIA INTERNACIONAL DE COMISIONADOS DE PROTECCIÓN DE DATOS Y PRIVACIDAD
91 B-LA ACTIVIDAD DEL GRUPO DE TRABAJO DEL ARTÍCULO 29	101 F-LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS
95 C-ÁREA DE COOPERACIÓN POLICIAL Y JUDICIAL	
99 D-CONFERENCIA DE PRIMAVERA DE AUTORIDADES EUROPEAS DE PROTECCIÓN DE DATOS	
7	
	105 COLABORACIÓN INSTITUCIONAL CON EL DEFENSOR DEL PUEBLO
8	
	107 COOPERACIÓN CON LAS AUTORIDADES AUTONÓMICAS

– LA AGENCIA EN CIFRAS

1	
110 INSPECCIÓN DE DATOS	5
2	
124 GABINETE JURÍDICO	164 PRESENCIA INTERNACIONAL DE LA AEPD
3	
135 ATENCIÓN AL CIUDADANO	6
4	
141 REGISTRO GENERAL DE PROTECCIÓN DE DATOS	167 SECRETARÍA GENERAL







MEMORIA 2015

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

CIUDADANOS MEJOR INFORMADOS: NUEVOS CANALES DE COMUNICACIÓN

La Agencia Española de Protección de Datos tiene encomendadas entre sus funciones la tarea de fomentar una cultura de protección de los datos personales que incluya la asistencia y tutela al ciudadano en el ejercicio de sus derechos y a los responsables de ficheros en el cumplimiento de sus obligaciones legales.

La protección de datos vive un momento decisivo debido en gran medida a los continuos cambios tecnológicos. La digitalización de la información ha ampliado enormemente las posibilidades de recogida, almacenamiento y, sobre todo, procesado de la información, a la vez que ha crecido de forma exponencial en los últimos años la cantidad y variedad de datos personales que recogen y tratan tanto actores públicos como privados. En este sentido, hay que destacar que en España hay 22,2 millones de usuarios intensivos de internet que se conectan todos los días, que el 88,3% de los usuarios acceden a internet a través del móvil y que los españoles se descargaron durante 2015 3,8 millones de apps cada día¹. Este uso intensivo de internet y sus posibilidades no implica que a los usuarios no les preocupe la privacidad y la protección de datos. De hecho, este mismo estudio pone de manifiesto que más del 82% de los usuarios considera este tema de gran importancia y más de la mitad (el 56,3) lo valora con la máxima puntuación. Casi un 84% declara, además, que le preocupa mucho que sus datos personales escapen a su control.

El servicio de Atención al ciudadano es el primer punto de encuentro entre la Agencia Española de Protección de Datos (AEPD) y quienes quieren obtener más información o resolver cualquier duda acerca del derecho fundamental a la protección de datos personales. Ofrece fórmulas de contacto presencial,

telefónica, postal y electrónica y, a través de este servicio, el número total de consultas de ciudadanos atendidas en 2015 ha ascendido a 218.335, lo que ha supuesto un incremento del 10,62% respecto al año anterior. De ellas, el 36% (78.557) corresponde a las consultas planteadas a través de los canales tradicionales, frente al 64% que ha utilizado los canales electrónicos (132.704 consultas automáticas al catálogo de preguntas más frecuentes y 7.054 a través de la Sede electrónica).

Mientras que el volumen de consultas a través de los canales tradicionales ha experimentado una disminución del 16,25% con respecto a 2014, las realizadas a través de la Sede electrónica han aumentado un 19,16%, manteniéndose estable el volumen de las realizadas a través del catálogo de preguntas frecuentes. Estos datos ponen de manifiesto la aceptación creciente de los ciudadanos para mantenerse en contacto con la Administración utilizando los servicios electrónicos.

En relación con la temática de las consultas atendidas por vía telefónica (74.260), las más frecuentes han estado relacionadas con la inscripción de ficheros (22.331) y videovigilancia (3.942). De las planteadas por escrito (7.604), tanto a través de medios convencionales (550) como a través de la Sede electrónica (7.054), destacan las relativas a los derechos amparados por la Ley Orgánica de Protección de Datos (911), la cesión de datos (837), el ámbito de aplicación de la LOPD (829) y la inclusión en los ficheros de morosidad (678).

En cuanto a las consultas planteadas para recabar información sobre el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición –ARCO– (5.522), 3.202 corresponden al derecho de cancelación, 1.450 al derecho de acceso, 717 al derecho de oposición y 128 al derecho de rectificación. El incremento de las consultas sobre los

¹ Informe La Sociedad de la Información en España 2015, Fundación Telefónica.



derechos de cancelación (6%) y acceso (5,88%) ratifican que la principal inquietud de los ciudadanos es conocer qué informaciones personales son objeto de tratamiento y cómo evitarlo.

Asimismo, de las 132.704 cuestiones que se han planteado a través del catálogo de preguntas frecuentes, 16.059 han estado relacionadas con los ficheros de morosos y recobro de deudas, 13.442 con la inscripción de ficheros y 12.874 con el ámbito de aplicación de la LOPD.

En cuanto al nivel de satisfacción expresado con respecto al servicio de Atención al ciudadano

las encuestas realizadas permiten concluir que el 97,83% de los encuestados se ha encontrado satisfecho con la información recibida; el 96,47% consideró que la persona que les atendió poseía un conocimiento suficiente sobre protección de datos; y el 99,45% estimó que el trato recibido fue correcto.

La evolución de este servicio en los últimos años permite apreciar que es un canal de información utilizado no sólo por los ciudadanos sino también por responsables de tratamiento, profesionales de la protección de datos, consultores y diversos grupos y sectores interesados en la materia.

Esta circunstancia pone de manifiesto la necesidad de ofrecer canales informativos especializados para los distintos colectivos afectados. Por ello, en el Plan Estratégico de la Agencia 2015-2019 se prevén las siguientes actuaciones:

- Ofrecer un teléfono de información dirigido a centros educativos, docentes, padres y menores, al que se añade un canal de comunicación a través de WhatsApp, puesto en marcha en octubre que se suma al correo electrónico específico ya existente (canaljoven@agpd.es).
- Diversificar los canales de comunicación dirigidos específicamente a responsables del tratamiento, profesionales de la privacidad y pymes.

Respecto a los accesos a la página web, en 2015 se han aproximado a los cinco millones (4.952.945), con un promedio de 6.766 visitas diarias y unas herramientas para los ciudadanos que han visto incrementadas sus descargas. En concreto, el documento dirigido específicamente a promover los derechos de los ciudadanos, la Guía del ciudadano: el derecho fundamental a la protección de datos, sigue siendo una de las más consultadas. El número total de descargas de esta Guía en 2015 ascendió a 242.140.

Por otro lado, la Agencia ha seguido trabajando en la renovación de su página web, una transformación iniciada en 2014 y que se ha utilizado como base para establecer nuevos canales de comunicación web con los ciudadanos. La sección Bienvenida es uno de los nuevos módulos más visibles para aquellos que visitan la página de la Agencia. Creada en un momento en el que la versión borrador del Plan estratégico se estaba sometiendo a consulta pública, ha servido para presentar este proyecto y fomentar la participación de aquellas entidades, organismos o ciudadanos que han querido enviar sus sugerencias o comentarios antes de la confección de la versión definitiva del documento. Una de las prin-

cipales prioridades de la Agencia es llegar a ser un organismo abierto y cercano que refuerce y amplíe las vías de comunicación con todos los implicados. La sección Bienvenida está acompañada del apartado Sugerencias, un buzón que pueden utilizar tanto ciudadanos como responsables para hacer llegar a la institución comentarios sobre la misma, así como mejoras que consideren podrían ponerse en marcha.

The screenshot shows the official website of the Spanish Agency for Data Protection (Agencia Española de Protección de Datos). The top navigation bar includes links for 'TRANSPARENCIA Y RACIONALIZACIÓN', 'CANAL DEL CIUDADANO', 'CANAL DEL RESPONSABLE', 'REQUERIMIENTOS Y DOCUMENTOS', 'FICHIEROS INSUMETICIÓN', 'INTERNACIONAL', and 'CARTELERA DE COMUNICACIÓN'. Below the navigation is a search bar. The main content area features a large image of a smartphone displaying a video. To the left, there's a section titled 'Cómo solicitar la eliminación de fotos o vídeos publicados en Internet' with a small image of a person. To the right, there are several boxes for 'Ciudadanos', 'Profesionales', and 'Notificaciones y Alertas'. A prominent orange banner at the bottom left says 'Plan Estratégico' and 'EVA-DUA'. The central part of the page has a 'Destacados' section with several news items, each with a small image and a brief summary. At the bottom, there are sections for 'Áreas de interés' (Denuncias presentadas, Ejercicio de derechos, Consultas ciudadanas, Estadísticas de inscripción de ficheros en el RGPD (abril 2016)) and a 'Contacta con nosotros' section with icons for 'Oficina y presenciales', 'Indicaciones preventivas', 'Dudas frecuentes', and 'Sugestiones'.

MEMORIA 2015

Las secciones En qué podemos ayudarte y en qué no y Cómo ejercer el derecho al olvido son una prueba de la orientación práctica de los nuevos contenidos de la web de la Agencia. En septiembre de 2015 este organismo publicó la sección En qué podemos ayudarte y en qué no, que trata de orientar tanto a ciudadanos como a responsables sobre las funciones que desempeña la Agencia indicando en qué casos y de qué forma la AEPD puede ayudar a estos colectivos a reclamar y a cumplir, respectivamente, con la normativa de protección de datos. La sección también recoge en qué casos la Agencia no puede tramitar determinadas reclamaciones por tratarse de asuntos competencia de otros organismos o que deben resolverse por vía judicial. Por su parte, la sección Cómo ejercer el derecho al olvido, recoge algunas de las dudas más frecuentes en relación a las solicitudes presentadas ante los buscadores de internet. El microsite, estructurado en torno a cinco preguntas básicas, responde a algunas de las cuestiones más frecuentes que los ciudadanos han planteado ante la Agencia, incorporando enlaces a los formularios habilitados por los propios buscadores para ejercerlo. La página recoge también algunos ejemplos de procedimientos tramitados por la Agencia a modo de orientación (con resoluciones tanto estimatorias como desestimatorias), así como las sentencias más relevantes relacionadas con el «derecho al olvido».

La Agencia también remodeló en septiembre la sección Actualidad de su portada, que pasó a denominarse Áreas de interés para incluir de un modo destacado los temas recurrentes que más interesan a los ciudadanos. En la nueva sección se pueden consultar de forma directa, entre otros temas, la cifra de las reclamaciones y denuncias presentadas en el año anterior, qué se necesita para presentar un escrito ante la Agencia y cómo hacerlo telemáticamente. La sección Áreas de interés también in-

cluye un acceso a la herramienta Evalúa, con el que las empresas y administraciones puede autoevaluar su grado de cumplimiento de la LOPD.

Por su parte, el apartado de la web Resoluciones y Documentos consta también de dos nuevas secciones dedicadas a la publicación de Informes preceptivos y Criterios de aplicación del artículo 15 de la Ley 19/2013, apartado este último donde se publican los informes adoptados conjuntamente por el Consejo de Transparencia y Buen Gobierno y la Agencia Española de Protección de Datos.

En cumplimiento de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno se creó en diciembre de 2014 en la página web de la Agencia un canal de transparencia denominado «Transparencia: la Agencia», que tiene como objetivo presentar al ciudadano de una forma clara y ordenada todos los contenidos correspondientes a la publicidad activa que describe la mencionada Ley. El canal de transparencia está dividido en tres grandes grupos, mostrando en cada uno de ellos respectivamente datos de «Información institucional y organizativa», «Gestión económica financiera» y «Recursos humanos».

Además de la publicidad activa, la Agencia resuelve las solicitudes de acceso de transparencia que recibe, tanto las dirigidas directamente a este organismo como las que son presentadas a través del Portal de Transparencia de la Administración General del Estado.

Durante el año 2015 se han recibido 54 solicitudes de acceso de las que 35 han sido concedidas, en dos ha desistido el solicitante, una ha sido inadmitida por aplicación del artículo 18.1.a) –referida a información en curso de elaboración o de publicación general–, nueve han sido inadmitidas por

aplicación del artículo 18.1.e) –manifestamente repetitivas o de carácter abusivo no justificado– y siete han sido inadmitidas por aplicación de la Disposición Adicional Primera –materias con normativa específica.

■ DIFUSIÓN DE ACTIVIDADES Y MEDIOS DE COMUNICACIÓN

Los medios de comunicación son un elemento imprescindible para que ciudadanos y responsables conozcan, respectivamente, los derechos y deberes que les reconoce e impone la legislación de protección de datos. Un año más, la Agencia ha apostado por la atención personalizada a los medios, que durante 2015 formularon más de 400 solicitudes de información. A esta labor de respuesta bajo demanda hay que sumar el ámbito de la comunicación proactiva, que se ha materializado, además de en jornadas o eventos, en más de 100 notas de prensa, convocatorias, posturas oficiales enviadas a medios de comunicación y notas de agenda informativa publicadas en la web. Las más de 40 tribunas y entrevistas concedidas por el personal de la AEPD y los documentos sobre materias y asuntos de especial relevancia completan la labor de divulgación que la Agencia ha realizado junto a los medios de comunicación.

Desde una perspectiva cualitativa, se establece una clara identificación entre los nuevos retos que se plantean en materia de protección de datos –generalmente asociados a la aparición y proliferación de nuevas tecnologías– y las consultas planteadas por los medios, si bien la contratación irregular en diferentes sectores y la inserción indebida en ficheros de morosidad o la videovigilancia son áreas que se mantienen como objeto de consulta.

A continuación, se especifican buena parte de las consultas planteadas con mayor frecuencia, y que

permiten tener una visión global de las áreas de mayor interés mediático:

- Sentencia del Tribunal de Justicia de la Unión Europea sobre el denominado «derecho al olvido». Primeras sentencias de la Audiencia Nacional sobre los casos pendientes tras la sentencia del TJUE. Criterios de ponderación sobre reclamaciones estimadas y desestimadas y confirmación de criterios de la AEPD.
- Tratamientos masivos de información: Big Data, recopilación de datos, evolución cuantitativa y cualitativa de las posibilidades de análisis, elaboración de perfiles para hacer predicciones, riesgos asociados y retos de futuro, y evolución de esta tecnología y posibles repercusiones sobre la privacidad de los ciudadanos.
- Videovigilancia. Datos del Registro General de Protección de Datos y requisitos legales.
- Internet de las Cosas: tecnología vestible, domótica, ciudades inteligentes y comunicación entre máquinas. Obligaciones de los responsables, recomendaciones y ejemplos prácticos.
- Tramitación del Reglamento europeo de protección de datos. Configuración del nuevo marco legal, novedades respecto a la legislación actual y garantías añadidas. Plazos para su aprobación. Últimos cambios ante su aprobación.
- Garantías en la cesión de datos a terceros e inscripción en ficheros de morosidad.
- Legislación en caso de spam; competencias de la AEPD. Tratamiento de datos obtenidos de fuentes accesibles al público: derecho a que los datos de las guías telefónicas no sean tratados con fines publicitarios, Lista Robinson.

MEMORIA 2015

- Resultados del primer análisis coordinado sobre el uso de cookies en Europa, que examinó casi 500 sitios web y revisó tanto las cookies instaladas como la información ofrecida sobre las mismas y los mecanismos establecidos para recabar el consentimiento de los usuarios.
 - Evaluaciones de impacto en la protección de datos personales. Promoción de nuevos enfoques proactivos entre las organizaciones para identificar los riesgos que un producto o servicio puede implicar para la protección de datos antes de que se materialicen.
 - Primer Dictamen conjunto de las Autoridades europeas de protección de datos sobre drones. Riesgos para la privacidad y obligaciones que deben cumplirse.
 - Cifras y tendencias recogidas en las memorias de la AEPD 2014. Contratación irregular, inclusión en ficheros de morosidad, cuestiones relativas al recobro de deudas y comunicaciones comerciales; sectores con mayor volumen de sanciones.
 - Cambios en la política de privacidad de Facebook. Apertura de una actuación coordinada por la Autoridad holandesa y en la que participa la AEPD y las Autoridades de protección de datos de Bélgica, Alemania (Hamburgo) y Francia.
 - El TJUE declara inválida la Decisión de la Comisión que declara el nivel adecuado de protección del Puerto Seguro. Llamamiento por parte de las Autoridades europeas de Protección de Datos a los Estados miembros y a las Instituciones europeas para encontrar soluciones políticas, jurídicas y técnicas que permitan transferencias de datos a EEUU respetando los derechos fundamentales. Actuación conjunta de las Autoridades para establecer contacto con todas las empresas que conste que utilizaban Puerto Seguro para la realización de transferencias internacionales e informarles de la situación.
 - Menores: publicación de datos de menores en redes sociales por parte de sus padres, recomendaciones y consejos de la Agencia. Nueva versión del proyecto Tú decides en internet, dirigido a jóvenes, padres y profesores. Incorporación de nuevas guías.
 - Convenio de colaboración con el Ministerio de Educación, Cultura y Deporte para realizar proyectos y acciones de formación y sensibilización de menores en materia de privacidad y protección de datos.
 - Plan estratégico de la AEPD. Fase de publicación del borrador del texto, consulta pública, recepción de comentarios y publicación de la versión definitiva. Detalle de algunas de las actuaciones recogidas en el documento.
- ### ■ EVENTOS, JORNADAS Y CURSOS
- Como se comentaba con anterioridad, durante el año 2015 la Agencia ha realizado diferentes acciones de comunicación específicas orientadas a difundir el derecho fundamental a la protección de datos tanto entre los ciudadanos como entre los profesionales y especialistas en esta materia. Estas actividades han estado relacionadas en gran medida con la celebración de eventos y la presentación de proyectos de largo recorrido:
- Jornada «Protección de datos y tratamientos masivos de información»
- El 28 de enero de 2015, la AEPD, con la colaboración de la Comisión Europea, conmemoró el Día europeo de la protección de datos celebrando la jornada «Protección de datos y tratamientos

masivos de información», en la que se analizó el impacto en la privacidad de los ciudadanos de fenómenos emergentes como el Big data y el internet de las cosas. El evento, organizado como una jornada de debate y análisis, contó con la participación de destacados expertos e investigadores pertenecientes tanto a entidades públicas como privadas, que trasladaron su visión de las posibilidades y retos que suponen estas tecnologías. El acto incluyó la realización de dos mesas redondas temáticas presentadas por miembros de la AEPD. La primera, denominada «El impacto del Big data en la protección de datos» contó con la presencia de Zsuzsanna Belenyessy, representante del Supervisor europeo de protección de datos, Ignacio Hernández Medrano, investigador del hospital Ramón y Cajal, y Scott Taylor, jefe de privacidad y protec-

ción de datos de HP. La segunda mesa redonda, «La privacidad en el internet de las cosas», acogió las ponencias de Manuel García Sánchez, del área internacional de la AEPD, Borja Gómez Zarceño, gerente de M2M Estrategia de Telefónica y Asunción Santamaría, directora de CeDint - Universidad Politécnica de Madrid.

■ 7.^a Sesión Anual Abierta de la AEPD

El 21 de abril se celebró la 7.^a Sesión Anual Abierta de la AEPD en el Teatro Real de Madrid. La Sesión tuvo como tema central el open data, la reutilización de la información del sector público y la alternativa de la anonimización, proporcionando además una exposición sistemática de los temas y las novedades más relevantes acaecidas en el último año en materia de protección de datos desde los diferentes



MEMORIA 2015

departamentos de la Agencia. Este evento, al que acuden en torno a 1.200 expertos, se ha convertido en un punto de encuentro de referencia entre el organismo público y múltiples sectores empresariales y sociales para dar respuesta a sus inquietudes. La Agencia pone a disposición de todos aquellos que no pueden asistir al acto o que desean acceder a los contenidos con posterioridad un microsite específico en su página web desde el que se pueden visualizar todos los vídeos de la jornada así como acceder a cada una de las presentaciones realizadas durante la misma. La creación de esta sección web tiene como objetivo que todos aquellos expertos que no pueden acudir a la celebración del evento puedan consultar los contenidos abordados.

- Curso «Retos de protección de datos en las sociedades actuales»

La AEPD organizó en la Universidad Internacional Menéndez Pelayo durante las Actividades de Verano 2015 el curso Retos de protección de datos en las sociedades actuales, que se impartió entre el 6 y el 10 de julio en el Palacio de La Magdalena de Santander. Este seminario está dirigido fundamentalmente a universitarios, abogados, consultores, expertos en protección de datos y tecnologías de la información, responsables de seguridad y privacidad, y a profesionales interesados en la protección de datos.

En esta edición del curso se analizó la incidencia de los tratamientos derivados del Big Data, el Internet de las Cosas y el Cloud computing. Además, se abordaron diferentes cuestiones relacionadas con la transparencia, la reutilización de la información del sector público, los riesgos y técnicas de la anonimización, y el derecho al olvido. El curso también dedicó un espacio a las buenas prácticas de organizaciones y empresas en materia de protección de datos, para finalizar con un análisis del estado de tramitación del Reglamento europeo.

- Jornada «Pasado, presente y futuro de la Directiva 95/46 en su vigésimo aniversario»

El 5 de noviembre la Agencia organizó la jornada «Pasado, presente y futuro de la Directiva 95/46 en su vigésimo aniversario» cuando se cumplían 20 años de su entrada en vigor. La celebración coincidió además con el proceso de revisión del marco normativo de protección de datos de la Unión, que ha desembocado en el Reglamento europeo que será de aplicación directa en todos los países de la UE.

■ PREMIOS Y CONCURSOS

- Premio Puñetas de Bronce de ACIJUR

El trabajo desarrollado por la Agencia para que se reconociese el denominado derecho al olvido fue galardonado por la Asociación de Comunicadores e Informadores Jurídicos (ACIJUR) con el Premio Puñetas de Bronce, que fue entregado el 27 de enero en un acto celebrado en la Asociación de la Prensa de Madrid. Este premio fue otorgado por la labor realizada «para conciliar los beneficios de la tecnología con la preservación de los derechos y las libertades individuales». ACIJUR quiso reconocer con este premio la apuesta que realizó la Agencia para clarificar definitivamente el régimen de responsabilidades de los buscadores de internet en relación con la protección de datos personales.

La actuación de la AEPD en relación con el «derecho al olvido» fue respaldada por el Tribunal de Justicia de la Unión Europea (TJUE), que confirmó, como ya venía reconociendo la Agencia en sus resoluciones, que los derechos de cancelación y de oposición que forman parte del derecho fundamental a la protección de datos se pueden hacer valer frente a los responsables de los motores de búsqueda para evitar la difusión universal e indiscriminada de informaciones personales que no tienen interés público.



■ Entrega de los Premios Protección de Datos 2014 (XVIII edición)

La Agencia convoca cada año los Premios Protección de Datos, que reconocen aquellos trabajos que suponen una aportación destacada a la difusión o la investigación de este derecho fundamental. Durante la celebración de la 7.^a Sesión Anual Abierta tuvo lugar la entrega de los Premios correspondientes a 2014 en las categorías de Comunicación e Investigación, que a su vez son hechos públicos en 28 de enero coincidiendo con el Día europeo de

Protección de Datos. Estos premios reconocen la difusión de este derecho fundamental que realizan periodistas y medios de comunicación, así como el trabajo desarrollado por los investigadores.

Esta edición recogió un total de 30 candidaturas, 13 en la categoría de Comunicación y 17 en la de Investigación. El jurado –compuesto por el Consejo Consultivo de la AEPD– concedió el premio de comunicación a la Corporación RTVE por el reportaje emitido en el programa Documentos TV Ojo con tus datos, que aborda la privacidad y el tratamiento

MEMORIA 2015

de datos personales en la Red. Asimismo, el jurado otorgó un accésit a Carmen Pérez, por los reportajes radiofónicos Protejamos nuestros datos y Tú decides en internet, emitidos en el programa Cuarto Mundo de Radio Exterior de España. Dentro del premio de comunicación, el jurado concedió otro accésit a Marisa Arellano, por su reportaje El negocio de nuestros datos en la Red, el petróleo del siglo XXI, emitido en Informativos Telecinco.

En la categoría de Investigación, el jurado otorgó el premio en su modalidad de trabajos originales e inéditos a Adrián Quesada por su trabajo «Protección de Datos en la Convergencia de las Telecomunicaciones», mientras que se concedió un accésit dentro de la misma modalidad a Alfonso Ortega, por su trabajo «La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita en derecho internacional privado español».

En la modalidad de investigación sobre trabajos originales e inéditos que tratan acerca del derecho a la protección de datos en países iberoamericanos, el jurado premió la candidatura de Nelson Remolina, por su trabajo «Tratamiento de información personal. Desde la transferencia transfronteriza hacia la recolección internacional de datos personales: un reto del mundo post-internet». También se concedió un accésit a Daniel Aarón López, por su «Estudio sobre las garantías en materia de protección de datos y habeas data: una visión desde Iberoamérica».

Por último, es necesario mencionar que el concurso Pandijuegos, que la Agencia presentó el 13 de mayo como una iniciativa orientada a colegios para fomentar el conocimiento de la protección de datos y promover el valor de la privacidad entre alumnos de 4.^º, 5.^º y 6.^º de Educación Primaria

se detalla posteriormente en esta Memoria en un apartado dedicado específicamente a menores.

■ ACUERDOS Y CONVENIOS DE COLABORACIÓN

- Convenio de colaboración con el Consejo General del Poder Judicial

La Agencia y el Consejo General del Poder Judicial (CGPJ) suscribieron el 23 de julio un convenio de colaboración de vigencia anual prorrogable a través del Centro de Documentación Judicial (CENDOJ) con el fin de mejorar el servicio que cada una de las instituciones ofrece en ejercicio de sus respectivas competencias.

El CENDOJ, por su parte, dispone de una base de datos de más de 6 millones de resoluciones judiciales anonimizadas, una amplísima documentación de entre la que se compromete a facilitar a la AEPD todas aquellas que tengan relación con el derecho a la protección de datos de carácter personal y la privacidad. El documento recoge que el CENDOJ dará respuesta a cuantas consultas y peticiones se cursen desde la Agencia referidas a documentos que formen parte de su acervo, así como a las realizadas a través del servicio de consulta documental del Centro. En virtud del convenio, la Agencia se compromete a facilitar al CENDOJ debidamente anonimizadas las resoluciones dictadas en materia de protección de datos y privacidad y a realizar una labor de asesoramiento técnico y legal en este ámbito, respondiendo a las consultas que se planteen.

- Convenio de colaboración con la Secretaría de Estado de Administraciones Públicas

El 18 de noviembre la AEPD firmó un convenio de colaboración de vigencia anual prorrogable con la Secretaría de Estado de Administraciones Públicas para que la Agencia pueda utilizar el Sistema de In-

terconexión de Registros (plataforma SIR), que permite el intercambio electrónico de documentos con otras administraciones integradas en el sistema.

A través de este convenio la Agencia podrá realizar la tramitación electrónica y el envío de los documentos presentados por los ciudadanos con destino a otras administraciones integradas en SIR, así como recibir documentos procedentes de otras entidades adscritas al sistema. Esta conexión con la plataforma SIR se realizará a través de la Red SARA (Sistema de Aplicaciones y Redes para las Administraciones), que es el conjunto de infraestructuras de comunicaciones que conecta a las Administraciones Públicas españolas y a las instituciones europeas para el intercambio de información y acceso a servicios. Este sistema da cobertura a más del 90% de la población española.

- Acuerdo de colaboración con el Consejo de Consumidores y Usuarios

La Agencia firmó el 14 de diciembre un acuerdo con el Consejo de Consumidores y Usuarios (CCU) para difundir los derechos de los ciudadanos y que estos conozcan cómo exigirlos en caso de que se utilicen sus datos personales para la contratación irregular de servicios, y para desarrollar acciones orientadas a fomentar las buenas prácticas empresariales.

Mediante el acuerdo, vigente durante un periodo de dos años, la AEPD y el CCU se comprometieron a trabajar en los espacios comunes de ambos organismos, especialmente en ámbitos con un gran impacto entre los ciudadanos, como la contratación irregular de servicios, sobre todo en los sectores de telecomunicaciones, suministros de agua y energía o el sector financiero. Apoyar y difundir buenas prácticas entre las empresas que contribuyan a que estas realicen un tratamiento de los datos perso-

nales de sus clientes conforme a la normativa son otros de los aspectos tratados en el documento.

El acuerdo se enmarca en las actuaciones contempladas en el Plan Estratégico 2015-2019, que recoge una batería de medidas para hacer frente a la contratación irregular, entre las que se incluye colaborar con las organizaciones sociales orientadas a la protección de los consumidores y usuarios.

Por último, el convenio firmado entre la Agencia y el Ministerio de Educación para formar y sensibilizar a los menores en materia de privacidad y protección de datos se detalla posteriormente en el apartado específico dedicado a menores de esta Memoria.

■ REPRESENTACIÓN INSTITUCIONAL Y REUNIONES DE TRABAJO

El artículo 36.1 de la LOPD establece que la figura del director de la Agencia de Protección de Datos será nombrada, de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un periodo de cuatro años. El 24 de julio de 2015 el Consejo de Ministros, a propuesta del ministro de Justicia, Rafael Catalá, aprobó el nombramiento de Mar España Martí, vocal del Consejo Consultivo de la AEPD, como directora de este organismo, tomando posesión del mismo el 27 de julio. Sucedió así en el cargo a José Luis Rodríguez Álvarez, que había tomado posesión del cargo de director de la Agencia el 21 de junio de 2011. Este cambio se refleja debido a que en esta sección se recogen las actividades de representación institucional llevadas a cabo, en función de la fecha detallada, por los dos responsables de la AEPD en este año.

Las reuniones institucionales y de trabajo son un elemento necesario para avanzar en una protección ágil y eficaz del derecho a la protección de datos. Además de los encuentros con organiza-

MEMORIA 2015

ciones sociales y profesionales de diversa naturaleza, la Agencia también ha celebrado reuniones con administraciones públicas y entidades privadas agrupadas por sectores tanto para tratar de agilizar los procesos administrativos como para fomentar el cumplimiento de la legislación.

A continuación se detallan de las reuniones institucionales y de trabajo celebradas durante 2015. En cualquier caso, estas pueden consultarse cronológicamente en la sección Notas de agenda de la página web de la AEPD.

El Consejo Consultivo de la Agencia de Protección de Datos, regulado en el artículo 37 de la Ley Orgánica 5/1992, de 29 de octubre, es un órgano colegiado de asesoramiento a la dirección de la Agencia. Este se reúne cuando así lo decide la dirección de la Agencia que, en todo caso, debe convocarlo una vez cada seis meses. También se reúne cuando lo solicita la mayoría de sus miembros. El 14 de enero y el 15 de julio fueron las fechas de reunión del Consejo Consultivo, en las que se expuso y analizó la actividad de la institución. La primera de ella abordó las acciones realizadas durante 2014 y la segunda las relativas al primer semestre de 2015. Ya fuera del ámbito temporal de esta Memoria, el Consejo se volvió a reunir el 21 de enero de 2016, esta vez con el detalle de las actividades llevadas a cabo durante todo el año 2015.

El compromiso de establecer una comunicación fluida con los sectores y entidades implicadas en el cumplimiento de la LOPD, con el objetivo de fomentar acciones preventivas que faciliten su aplicación, se ha concretado en la realización de un amplio abanico de reuniones institucionales.

De acuerdo con este objetivo, la Agencia ha celebrado encuentros con organizaciones profesionales y empresariales como la Asociación Profesional

Española de Privacidad; ISMS Forum; la Asociación Española para el Fomento de la Seguridad de la Información; la Asociación Española de la Economía Digital; la Asociación para la Autorregulación de la Comunicación Comercial e IAB Spain; la Asociación de Empresas de Electrónica, Tecnologías de la Información, Telecomunicaciones y Contenidos Digitales; la asociación empresarial Unión Española de Aseguradoras y Reaseguradoras; la Sociedad Española de Informática y Salud o la Asociación Europea de Profesionales para el conocimiento y regulación de actividades de Seguridad Ciudadana.

En el apartado de fomentar la concienciación por parte de los responsables y ofrecerles herramientas útiles que les ayuden al cumplimiento de la legislación, la Agencia mantuvo un encuentro con representantes de la Confederación Española de Organizaciones Empresariales y de la Confederación Española de la Pequeña y Mediana Empresa. En este sentido, también se han realizado reuniones con representantes de los principales operadores de telecomunicaciones y con empresas del sector energético.

En el ámbito público, la directora de la Agencia mantuvo una reunión con la Fiscal de Sala Coordinadora en materia de Criminalidad Informática, Elvira Tejada de la Fuente (30 de septiembre) y con el Fiscal de Sala Coordinador de Menores, José Javier Huete Nogueras (9 de octubre). La Agencia también participó en la reunión del Comité Sectorial de la Administración Electrónica, celebrado en Madrid, para abordar la colaboración de la AEPD en el impulso de la Administración Electrónica; y se mantuvo un encuentro el 16 de noviembre con el secretario de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI), Víctor Calvo-Sotelo; el director general de Red.es, Daniel Noguera; el director general del Instituto Nacional de Ciberseguridad (Incibe), Miguel Rego; y la sub-

directora general de Servicios de la Sociedad de la Información de la SETSI, Gema María Campillos. En materia de menores, además de la participación en actos que se detallan con posterioridad, la Agencia participó en la reunión de la Comisión General de la Conferencia de Educación.

Por otro lado, la Agencia se reunió el 30 de septiembre con el director de Tecnologías de la Información y la Comunicación (TIC) de la Administración General del Estado, Domingo Molina; el 7 de octubre con representantes de la Secretaría de Estado de Seguridad del Ministerio del Interior; y el 14 de diciembre con varios miembros de la Secretaría de Estado de Administraciones Públicas.

■ PARTICIPACIÓN EN EVENTOS, JORNADAS Y SEMINARIOS

Al igual que en las secciones anteriores, se pueden consultar de manera sistemática los eventos, jornadas y seminarios a los que ha asistido una representación de la Agencia así como más información sobre ellos en la página web -sección Notas de agenda-, que se actualiza de manera constante. Igualmente, los eventos relacionados con conferencias europeas o eventos propios de la Red Iberoamericana de Protección de Datos, aparecerán detallados en sus correspondientes apartados específicos de esta Memoria.

La Conferencia Global de Privacidad, organizada por la Asociación Internacional de Profesionales de Privacidad (IAPP), congrega anualmente a expertos en la materia del ámbito empresarial, académico e institucional. La Agencia participó en el evento de 2015, celebrado en Washington del 4 al 6 de marzo, en el que su director intervino en el panel llamado «Derecho al olvido: conflicto de intereses y diferencias culturales», donde se abordaron las implicaciones de la sentencia dictada por el Tribunal

de Justicia de la UE en relación con esta materia. En las actividades paralelas, la AEPD participó en la jornada dedicada al Proyecto «Marco de riesgo para la privacidad», organizado por el Centre for Information Policy Leadership. Asimismo, se mantuvieron reuniones con representantes de la Administración de EEUU, Autoridades de protección de datos de varios países, la Comisión Federal de Comercio (FTC, por sus siglas en inglés), así como con destacados expertos en privacidad norteamericanos.

El derecho al olvido fue también uno de los temas principales en el XII Encuentro Ibérico de Autoridades de Protección de Datos, un evento celebrado los días 8, 9 y 10 de abril y organizado por la Comisión Nacional de Protección de Datos de Portugal (CNPD). En esta duodécima edición, las sesiones de trabajo abordaron temas como el equilibrio entre la transparencia y la protección de datos o las consecuencias de la sentencia del Tribunal de Justicia de la Unión Europea sobre el denominado derecho al olvido. Por otro lado, el Grupo de investigación «Globalización, Derechos Humanos y Unión Europea» de la Universidad Complutense de Madrid seleccionó como tema para las VI Jornadas Internacionales de Derechos Humanos los «Retos y amenazas a los derechos humanos en internet. De la libertad de expresión e información al derecho al olvido». La Agencia participó en una de las jornadas, celebrada en Madrid el 24 de abril, con una intervención llamada «La protección de los derechos personales en internet y el llamado derecho al olvido».

Los retos relacionados con esta materia también se expusieron para el análisis en el «Foro Libertad de expresión y protección de datos personales. Balance de derechos», celebrado el 10 de marzo en México DF bajo la coordinación del Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) y el Instituto de Investigaciones Jurídicas de la

MEMORIA 2015

Universidad Nacional Autónoma de México. Algunas de estas inquietudes se trataron también en la conferencia organizada por la Facultad de Derecho de la Universidad de Navarra y celebrada en el Parlamento navarro el 24 de marzo.

En el marco de los nuevos desarrollos normativos, la Agencia intervino en el acto de apertura del seminario «Nuevo Reglamento General Europeo de Protección de Datos», celebrado los días 17 y 18 de abril en Madrid, bajo la organización de la Unión Internacional de Abogados (UIA).

En el apartado dedicado a las nuevas tecnologías también hay que destacar que la Agencia participó en el proyecto Big Data Ethical Assessment Process promovido por The Information Accountability Foundation, celebrado el 29 de abril en Madrid, y en el que también intervieron otras autoridades europeas de protección de datos, así como expertos procedentes del sector privado. El objetivo del

encuentro era crear un espacio de debate para explorar ideas y mecanismos que permitan acreditar el cumplimiento del futuro código ético para procesos de Big data –en el que trabaja la IAF– para aquellas organizaciones que se adhieran a él. Este primer encuentro fue seguido de otro, celebrado en Roma el 14 de julio, en el que también participó la Agencia.

Asimismo, la Agencia participó el 14 de octubre en la clausura de las III Jornadas sobre Sociedad y Economía Digital, organizadas por la Fundación España Digital y en el II Congreso Internacional de derecho digital de la Asociación de Expertos Nacionales de la Abogacía TIC (ENATIC), en el marco de la sesión «Tendencias regulatorias y privacidad: el plan estratégico de la Agencia».

Otras participaciones de la Agencia en eventos, jornadas y seminarios se recogen en apartados específicos de la Memoria.

GARANTIZAR LOS DERECHOS DE LOS CIUDADANOS

A - HERRAMIENTAS PARA FACILITAR EL CUMPLIMIENTO DE LA LOPD

La inscripción de ficheros en el Registro General de Protección de Datos (RGPD), obligación que no se contempla en el Reglamento General de Protección de Datos sobre el que, a finales de año, se ha alcanzado un acuerdo entre las Instituciones de la Unión Europea, es uno de los indicadores que se utiliza habitualmente para evaluar el grado de conocimiento de la LOPD por los responsables del tratamiento.

El año 2015 finalizó con un total de 4.107.944 ficheros inscritos en el RGPD, cifra que supone un incremento del 9,63% respecto al cierre de 2014. El 96,17% son ficheros de titularidad privada, es decir 3.950.620, y el 3,82% corresponde a los 157.324 ficheros de titularidad pública.

El número total de ficheros privados inscritos a finales de 2015 se ha incrementado en un 9,91% con respecto a la misma fecha del año anterior, una cifra inferior al crecimiento del 12% experimentado en 2014. De igual forma, el crecimiento del número de entidades del sector privado que tienen inscritos ficheros en el RGPD fue de un 8,6%, frente al 12% que se registró en 2014. Se produce así una disminución en el crecimiento tanto en el número de ficheros inscritos como en el de entidades responsables. No obstante, se sigue incrementando el número de operaciones de modificación y supresión de ficheros inscritos en el RGPD, muestra del esfuerzo de puesta al día por parte de los responsables de ficheros.

En cuanto a las finalidades de los ficheros de titularidad privada inscritos durante 2015 en el RGPD, los que tienen por finalidad la «Gestión de clientes, contable, fiscal y administrativa» siguen constituyendo el mayor número de inscripciones y son

también los que representan el mayor porcentaje, suponiendo el 58,46% del total de los ficheros privados. Asimismo, destacan los ficheros cuyas finalidades son las de «Recursos humanos», «Gestión de nóminas» y «Publicidad y prospección comercial». Al igual que en el ejercicio anterior, la inscripción de ficheros con la finalidad de «Comercio electrónico» es la que más crece, con un incremento de un 20% anual, seguida, como en 2014, de la de los ficheros que declaran tener por finalidad la de «Videovigilancia», con algo más del 17%.

El constante crecimiento de los ficheros relacionados con el comercio electrónico es un indicador del progresivo desarrollo de la economía digital y los servicios de la sociedad de la información en nuestro país.

Por sectores de actividad, el mayor número de ficheros inscritos sigue correspondiendo a los de «Comunidades de propietarios», «Comercio» y «Sanidad». Al igual que en el año 2014, debe destacarse el incremento de los ficheros a nombre de «Organizaciones empresariales y profesionales», que ha supuesto más del 20% del total de los ficheros inscritos a nombre de estos responsables.

El número total de ficheros de titularidad pública inscritos a finales de 2015 fue de 157.324, lo que supone un incremento algo inferior al 3% con respecto a la misma fecha del año anterior. Este limitado incremento en el número total de ficheros muestra el estado de adaptación a la LOPD por parte de los responsables públicos. Es destacable el número de correcciones realizadas, más de 12.000, que en su mayor parte se deben a las reestructuraciones de los órganos de las Administraciones públicas. La Administración local sigue liderando el incremento en el número de ficheros inscritos suponiendo el 58% del total de los ficheros públicos inscritos durante 2015.

En la Administración General del Estado (AGE), el Ministerio de Defensa es el Departamento con mayor número de ficheros inscritos, con más del 25% del total de los ficheros de la AGE.

Con respecto a las Administraciones de las Comunidades Autónomas cabe destacar dos tendencias sobre la actualización de su situación registral. La primera representada por la Junta de Comunidades de Castilla y la Mancha con incremento de más de un 13% en el número de ficheros inscritos. La segunda representada por la Comunidad de Madrid que decrece en el número de ficheros en un 2,4%.

En la Administración local también se mantiene el incremento del número de responsables que notificaron sus ficheros, en el que destaca especialmente la provincia de Cuenca, con un aumento de un 54%, seguida de Lugo, con un incremento de más de un 14%, y de Zamora, con un 9%. En cuanto al crecimiento en el número de ficheros inscritos destaca igualmente la provincia de Cuenca, con un incremento de un 52%, seguida de Zamora, con un 18%, Las Palmas, con un 15%, y las localidades de Asturias y Soria, con un incremento de un 11%.

Para facilitar a los responsables de los ficheros la realización de los trámites de inscripción registral, en el mes de julio la Agencia llevó a cabo dos actuaciones. Por una parte, incorporó a su Sede electrónica una versión web del formulario NOTA que ofrece, entre otras posibilidades, la de notificar varios ficheros de un mismo responsable en un solo acto, anexar documentación o notificar transferencias internacionales amparadas en una resolución marco o de encargado a subencargado. Por otra parte, se puso en marcha el sistema de notificación mediante comparecencia en la Sede electrónica de la Agencia para las solicitudes de inscripción de ficheros y de copia del contenido de la inscripción registral.

La puesta en producción del formulario NOTA a través de la Sede electrónica de la Agencia ha tenido como consecuencia que el número de notificaciones realizadas a través de internet suponga ya el 91,41% del total; donde el uso del formulario con firma electrónica supera, por primera vez, el 50% del total, dejando en un 8,59% el número de notificaciones que se realiza en formato papel. De igual forma, la notificación de las resoluciones de inscripción registral a través del sistema de Notificaciones Telemáticas (SISNOT) se ha visto incrementado en más de un 26% respecto a las realizadas en 2014.

Las herramientas EVALÚA y DISPONE que la AEPD ofrece, a través de su página web para ayudar a los responsables a analizar el cumplimiento de la LOPD y de las medidas de seguridad y para ayudar a la elaboración de la disposición general de creación, modificación o supresión de ficheros de titularidad pública, respectivamente, siguen demostrando su utilidad para los responsables de los ficheros. No obstante, EVALÚA ha visto disminuido su uso tanto en el número de accesos como en el número de informes obtenidos con respecto a años anteriores, lo que ha llevado a este organismo a empezar a trabajar en la planificación de nuevas herramientas útiles y gratuitas para los responsables que les ayuden a cumplir con la normativa de protección de datos. Por su parte, la herramienta DISPONE ha visto incrementado fuertemente su uso por las Administraciones y Organismos Locales, la Administración y Organismos de las CCAA, la Administración General del Estado, Cámaras Oficiales de Comercio e Industria, Comunidades de Regantes y Consejos Reguladores.

En relación con la herramienta EVALÚA la Agencia ha tomado la iniciativa de contrastar su utilidad para las pymes que constituyen un sector muy relevante en la estructura productiva del país. Para

ello, recabó información de las organizaciones patronales representativas de este sector de actividad.

La información recibida ha tenido como consecuencia la adopción de nuevas iniciativas para facilitar el cumplimiento de la LOPD por parte de las pymes y que se han incorporado al Plan Estratégico de la Agencia.

Estas iniciativas, como se mencionaba con anterioridad, están centradas en la creación de un canal de información que permita ofrecer soluciones prácticas adecuadas a las características de estas empresas y en la elaboración de guías y fichas accesibles y de fácil consulta para resolver las dudas puntuales que puedan plantear.

A las herramientas que se han descrito para facilitar el conocimiento y cumplimiento de la LOPD, hay que sumar las guías que ofrecen información sobre sectores concretos de actividad, siendo los datos más relevantes del número de descargas los siguientes: Guía sobre el uso de las cookies (497.747), Guía La protección de datos en las relaciones laborales (97.428); Guía para clientes que contraen servicios de Cloud Computing (144.720); Orientaciones para prestadores de servicios de Cloud Computing (22.965); Guía sobre seguridad y privacidad de las tecnologías RIFD (63.533); Guía de videovigilancia (45.247); Guía para una Evaluación de Impacto en la Protección de Datos Personales –EIPD- (111.017).

2



MEMORIA 2015

El análisis del volumen de descargas ratifica el mayor interés que generan las guías relacionadas con el uso de la tecnología. A ello hay que añadir la relevancia de las descargas de la Guía para una Evaluación de Impacto en la Protección de Datos Personales, indicativa del interés por parte de los responsables del tratamiento por los modelos de cumplimiento normativo basados en acciones preventivas que anticipen las que serán exigibles con el nuevo Reglamento General de Protección de Datos Personales de la Unión Europea, cuya aprobación se detalla en otros apartados de esta Memoria.

Por otro lado, la LOPD prevé la adopción de códigos tipo, o códigos de conducta, como fórmulas de autorregulación que permitan a sectores de actividad, empresas, Administraciones o Corporaciones públicas adecuar el cumplimiento de la normativa a sus características específicas.

Durante 2015, se acordó la inscripción de los siguientes códigos tipo:

- Código tipo de protección de datos personales del fichero Asnef Protección, inscrito el 21 de enero de 2015 y cuyo promotor es la Asociación Nacional de Entidades de Financiación (ASNEF).
- Código tipo del tratamiento de datos de carácter personal aplicable al tratamiento de datos de las oficinas de farmacias del Colegio de Farmacéuticos de Barcelona, inscrito el 21 de julio de 2015 y cuyo promotor es el Colegio Oficial de Farmacéuticos de Barcelona. Su tramitación se realizó en colaboración de la Autoridad Catalana de Protección de Datos, al incluir en su ámbito objetivo de aplicación tratamientos de datos competencia de dicha Autoridad.
- Código tipo de la Asociación Nacional de Entidades de Gestión de Cobro (ANGECO), inscrito el 5 de noviembre de 2015.

Igualmente, durante 2015 quedó prácticamente finalizada la tramitación de la inscripción del Código Tipo presentado por la Federación Nacional de Clínicas Privadas, la Asociación Nacional de Actividades Médicas y Odontológicas de la Sanidad Privada, la Asociación Nacional para la Promoción de la Excelencia en las Actividades Sanitarias Privadas, la Asociación Catalana d'Entitats de Salut y la Asociación de Empresas de Prestación Asistencial de Andalucía, así como la inscripción de la modificación de Código tipo del fichero histórico de seguros del automóvil y del Código tipo del fichero de automóviles de pérdida total, robo e incendios, promovidos ambos por la Unión Española de Entidades Aseguradoras y Reaseguradoras.

El análisis de los Códigos tipo inscritos en el Registro General de Protección de Datos permite apreciar el desarrollo que esta figura alcanza en el sector sanitario.

■ Consultas al Gabinete Jurídico

En cuanto a las consultas de mayor complejidad dirigidas a facilitar la aplicación de la LOPD a los responsables de tratamientos públicos y privados, se atendieron un total de 485, de las cuales 305 (63%) fueron planteadas por las Administraciones Públicas y 180 (37%) por el sector privado.

Se produce así una disminución de un 8% en el volumen de consultas planteadas respecto a las formuladas el año anterior, por lo que el número total vuelve a ser semejante al de los años 2011 (484 consultas), 2012 (483 consultas) y 2013 (489 consultas). Como se ha venido comentando en Memorias de ejercicios anteriores, la especialización de las consultas es cada vez mayor, siendo más singulares las características de las situaciones y tratamientos a los que las mismas se refieren y continuando la tendencia decreciente en el planteamiento de du-

das de carácter general que habían podido suscitarse tras la entrada en vigor del RLOPD.

Igualmente se aprecia, en cuanto al reparto de las consultas de los sectores público y privado, una absoluta similitud con el que se producía en el año 2014, en que las consultas del sector público alcanzaron el 63% del total. Con ello parece que en los dos últimos ejercicios se ha frenado la tendencia al incremento del peso de estas consultas, que había venido produciéndose en los últimos años.

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

- El mantenimiento de un número relativamente significativo de consultas relacionadas con las cesiones de datos de carácter personal, que sigue siendo la cuestión objeto de un mayor número de las mismas, pese a que en 2015 se produce una disminución de su número de en torno al 20%.
- La mayor importancia relativa que pasan a tener las cuestiones relacionadas con los ficheros de los que son responsables las Administraciones Públicas, que pasan a ocupar la segunda posición en número, reemplazando en este lugar a las relacionadas con la aplicación de los principios de calidad de datos, contenidos en el artículo 4 de la LOPD y centradas esencialmente en el principio de proporcionalidad. Estas últimas consultas disminuyen en un 35% pasando a representar un 18% de las planteadas durante 2015.
- El más que significativo incremento de las cuestiones planteadas en torno a la conciliación de las normas de protección de datos con el principio de transparencia y el acceso a la información pública, en atención a lo establecido, esencialmente, en el artículo 15 de la Ley 19/2013,

MEMORIA 2015

de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Como ya se indicó en la Memoria de 2014 se produjo un número significativo de estas consultas en el último trimestre de 2015, habiéndose confirmado esa tendencia, al incrementarse en 2015 en un 169%, pasando de representar un 2.5% a un 7.2% del total de consultas. A ello debe añadirse la elaboración conjunta por la Agencia y el Consejo de Transparencia y Buen Gobierno de criterios interpretativos relacionados con el citado artículo 15.

- El importante repunte (de un 53%) de las cuestiones relacionadas con la existencia y funciones de los encargados del tratamiento, especialmente vinculadas a la prestación de estos servicios en entornos de computación en nube y, en los últimos meses, con la transferencia internacional a prestadores de servicios ubicados en EEUU, como consecuencia de la sentencia del Tribunal de Justicia de la UE de 6 de octubre de 2015, analizada en el apartado 5. C) de esta Memoria.
- El incremento significativo de las consultas relacionadas con el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (ARCO), un 45%, con especial incidencia en las relacionadas con el último de estos derechos como consecuencia de la Sentencia del tribunal de Justicia de la UE de 13 de mayo de 2014. Igualmente es relevante el incremento de las cuestiones relacionadas con la implantación de medidas de seguridad (de un 30%, con lo que no sólo se recuperan los niveles anteriores a 2014, sino que incluso se superan los mismos en un 7%).
- La importante disminución de las consultas relacionadas con la videovigilancia tras el incre-

mento producido en 2014 como consecuencia de la aprobación de la Ley 5/2014, de 4 de abril, de Seguridad Privada. Estas consultas disminuyen en torno a un 41% volviéndose a situar, en términos absolutos, en niveles prácticamente similares a los de 2013.

- La significativa disminución de las cuestiones relacionadas con la cesión de datos a la Hacienda Pública (un 64%), la aplicación de la regla de equilibrio de intereses contenida en el artículo 7 f) de la Directiva 95/46/CE (un 62.5%), el cumplimiento de las obligaciones de confidencialidad y secreto establecidas en el artículo 10 de la LOPD (un 50%) y el contenido de la información que ha de ser facilitada a los interesados (un 34%).
- El mantenimiento de un volumen relevante de cuestiones relacionadas con el ámbito de aplicación, tanto objetivo como territorial, de la LOPD, que mantienen un peso específico similar al de 2014, de en torno a un 12.5%.
- La desaparición, dentro de las cuestiones relevantes a tomar en consideración, de las relacionadas con el Padrón Municipal de Habitantes, que han pasado en los últimos diez años, junto con la relativa en general a las cesiones de datos, de ser objeto de un mayor número de consultas a resultar irrelevante en la descripción de las materias a las que esas consultas se refieren (sólo hubo una cuestión sobre esta materia en 2015).

Dentro del sector público el peso de las consultas formuladas por las distintas Administraciones Territoriales y la Administración Corporativa y los Órganos Constitucionales se mantiene en términos similares a los del año 2014, produciéndose un ligero aumento (1.3%) del peso de las consultas formuladas por la Administración General del Estado,

acompañado de una también ligera disminución (2.1%) de las planteadas por la Administración Corporativa y los Órganos Constitucionales.

En cuanto al sector privado, atendiendo a la distribución sectorial de las consultas, las principales conclusiones son:

- El muy importante incremento de las cuestiones planteadas por particulares, en las que en un gran número de supuestos se somete al parecer de la Agencia el desarrollo de una determinada actividad o de un determinado proyecto que lleva aparejado un tratamiento de datos de carácter personal. Estas consultas, que ya se habían incrementado en un 22% en 2014, aumentan en 2015 en un 68% respecto de 2014, lo que supone un aumento acumulado de un 104% en los dos últimos años.
- La disminución en un 32% de las consultas planteadas por las entidades dedicadas a la prestación de servicios de asesoría y consultoría. Nuevamente, es preciso recordar en este punto el criterio de la Agencia de atender únicamente las consultas relacionadas con sus ficheros y tratamientos y no con las de sus clientes, que deberán formularse por estos últimos. No obstante, la mayor parte de las consultas se referían a los tratamientos llevados a cabo por las propias entidades, bien como responsables, bien como encargadas del tratamiento.
- El importante aumento de las consultas relacionadas con la prestación de servicios de la sociedad de la información e informáticos (67%), así como las provenientes de los sectores financieros (60%), de investigación (50%) o de solvencia patrimonial y crédito (50%), relacionadas fundamentalmente con el desarrollo por estas entidades de nuevos servicios que ya no

guardan relación directa con el artículo 29 de la LOPD.

- La muy significativa reducción de las consultas efectuadas por entidades dedicadas a actividades de seguridad privada (80%), correlativa con la disminución ya apuntada anteriormente de las consultas relacionadas con los tratamientos con fines de videovigilancia.
- Los significativos descensos del número de cuestiones planteadas por el sector de las telecomunicaciones (54%), así como los sindicatos y partidos políticos (42%).
- El mantenimiento en términos prácticamente similares de las consultas planteadas por la empresas de distribución, las asociaciones y fundaciones y las asociaciones empresariales o profesionales, así como las procedentes del sector sanitario.

Los informes no preceptivos relacionados con consultas externas que pueden revestir una mayor trascendencia en materia de protección de datos versaron, entre otras, sobre las siguientes materias:

- La posibilidad de que los centros docentes no universitarios faciliten a los progenitores de los alumnos, incluso cuando éstos sean mayores de edad, los datos referidos a sus calificaciones sobre la base de la existencia de un interés legítimo de los progenitores, vinculado al abono por los mismos de los gastos escolares de los hijos mayores de edad. Esta presunción de un interés legítimo prevalente de los progenitores podría, no obstante, ser destruida en virtud del derecho de oposición establecido en el artículo 6.4 de la LOPD, por ejemplo en los supuestos en que el hijo sufragase sus propios gastos de educación.

■ La conformidad con lo dispuesto en la LOPD el establecimiento por un centro escolar de un sistema de control de acceso al comedor basado en la huella dactilar del alumno, siempre que el sistema no almacene el algoritmo de la huella dactilar, sino que el mismo se conserve en una tarjeta electrónica que sea introducida por el alumno en el momento de ingreso al comedor, autorizándose dicho ingreso en caso de coincidir el dato contenido en la tarjeta con la huella situada en el lector.

■ La posible legitimación para la instalación de sistemas de videovigilancia en zonas comunes de centros docentes (tales como los patios o el comedor) sobre la base de un interés legítimo relacionado con el principio de interés superior del menor consagrado en el art. 2 de la Ley Orgánica 1/1996 de protección jurídica del menor, siempre y cuando se adopten garantías especiales en cuanto al acceso, seguridad y conservación de las imágenes, que sólo deberían tratarse para la garantía de los derechos de los menores.

■ La posibilidad de que los centros escolares pudieran recabar, en tanto se pusiera en funcionamiento el Registro Central de Delincuentes Sexuales un certificado de antecedentes penales de quienes fueran a trabajar con menores, pudiendo conservarlo únicamente para la finalidad prevista en el art. 13.5 de la Ley Orgánica 1/1996, y no para otros fines y careciendo también de eficacia a todos los efectos las condenas penales que pudieran existir por delitos distintos a los que se refiere ese precepto.

■ La licitud de la cesión de datos de antecedentes penales de progenitores de los menores sometidos a tutela a las Entidades Públicas autonómicas competentes en materia de guarda y

protección de menores con arreglo a las modificaciones introducidas por la Ley 26/2015 en la Ley Orgánica 1/1996 de protección jurídica del menor.

■ La procedencia de la cesión de datos de salud de la progenitora de un menor con expediente en curso por situación de desamparo a la entidad pública autonómica encargada de la tramitación del mismo al amparo de la salvaguarda del interés superior del menor, si bien limitada a los datos de salud necesarios para la adecuada protección del menor por los poderes públicos mediante la prevención, detección y reparación de situaciones de riesgo, con el ejercicio de la guarda y, en los casos de declaración de desamparo, para la asunción de la tutela por ministerio de la ley.

■ La conformidad con la LOPD de la comunicación por un centro escolar a un progenitor que lo solicite de la relación de personas autorizadas por el otro progenitor para recoger a los hijos, en los supuestos de separación o divorcio, mientras el solicitante sea titular de la patria potestad, no siendo posible la cesión en los casos en que aquélla haya sido inhabilitada o suspendida.

■ La conformidad con la LOPD de que los servicios de urgencias y emergencias comuniquen a las personas que llamen identificándose como familiares y allegados de otra que ha sido previamente atendida el dato de si ha sido efectivamente atendida o no, así como del centro hospitalario al que ha sido trasladado, en aplicación de los artículos 7.d) de la Directiva 95/46/CE y art. 7.6 y 11.2.f) LOPD, concurriendo en estos supuestos la causa de interés vital del afectado. Cualquier otra información pudiera ser considerada excesiva en relación con el art. 4 LOPD.

■ Las salvaguardas que deberán establecerse en los supuestos en los que determinadas publicaciones relacionadas con expedientes de subvenciones públicas (tanto las relativas a su adjudicación con arreglo a lo previsto en la legislación de transparencia como las publicaciones edictales de las resoluciones por las que se concedieran las ayudas) pudieran revelar datos especialmente protegidos de los beneficiarios o las personas de su entorno o la identificación de una mujer víctima de violencia de género o los datos que permitieran su localización, debiendo aplicarse estrictamente el principio de minimización en dicha publicación (reducida si es posible en el caso de los edictos solamente a sus iniciales y DNI) y adoptarse salvaguardas que impidan la indexación de los datos por motores de búsqueda en internet.

■ La especial atención que habrá de tenerse a las previsiones de la LOPD en relación con los supuestos de publicación en blogs, páginas web o redes sociales de información que hubiera sido obtenida como consecuencia del ejercicio del derecho de acceso a la información pública, toda vez que la Ley 19/2013 prevé expresamente en su artículo 15.5 la íntegra aplicación de la LOPD a esta publicación, que deberá estar legitimada por alguno de los supuestos establecidos en su artículo 11.

■ La publicación en el Portal de Transparencia de una Comunidad Autónoma que prevé la publicidad de las relaciones nominales de puestos de trabajo de los datos relacionados con las comisiones de servicios del personal funcionario siempre que las mismas se limiten exclusivamente a la indicación del nombre y apellidos del funcionario, su puesto de origen y su puesto de destino, a menos que dicha publicación pudiese colocar a la persona a la que los datos se refie-

ren en una situación de riesgo que haga prever la posibilidad de que su derecho fundamental a la protección de datos de carácter personal.

■ La posibilidad de que una Comunidad Autónoma pueda publicar información sobre las cuentas bancarias abiertas a nombre de los órganos que la integran, que únicamente sería posible en caso de que se prevea expresamente que la publicación de la información se llevará a cabo previa disociación de los todos los datos de carácter personal que pudieran incluirse en la cuenta, tanto en relación con las autorizaciones como en cuanto a los movimientos de la cuenta, de forma que de esa información no pueda derivarse el acceso a datos relacionados con personas físicas identificadas o identificables. Todo ello, además, sin perjuicio de que no procediera la publicidad en caso de concurrir los restantes límites establecidos en la normativa básica y autonómica sobre transparencia.

■ La publicación por una Comunidad Autónoma, cuya normativa permite la publicidad de la relación nominal de empleados públicos, de los datos relacionados, para cada empleado, con su titulación académica, jornada desempeñada, si es el primer destino o no, y dentro de un apartado «observaciones» de información relativa a idiomas, si dispone de permiso de conducir, si tiene horario especial o jornada nocturna, o si pernocta en el centro de trabajo, entre otros.

■ La existencia de legitimación para la cesión de datos por un Ayuntamiento a los concejales que forman parte de una comisión de investigación, aun cuando no existe norma legal que habilita directamente la cesión de los datos a la propia comisión, quedando limitado, en todo caso, el uso de los datos al ejercicio de la fun-

MEMORIA 2015

ción de control y sin que sea posible su divulgación posterior.

■ La conformidad con lo establecido en la LOPD de la cesión por MUFACE al órgano competente en materia de sanidad de una Comunidad Autónoma de los datos correspondientes al nombre y apellidos, Documento Nacional de Identidad y domicilio de los mutualistas que, habiendo optado por recibir sus asistencia sanitaria a través de una entidad privada hubieran hecho uso de los medios del citado Servicio autonómico de salud, a fin de que por el cesionario pueda facturarse al mutualista la prestación sanitaria.

■ La licitud de la cesión a la Administración Tributaria por parte de un Tribunal Arbitral de la totalidad de un expediente, reclamado por aquélla al amparo de los artículos 93 y 94 de la Ley General Tributaria, salvo en la información que careciera absolutamente de trascendencia tributaria.

■ El carácter desproporcionado, salvo que se acredite lo contrario, del requerimiento llevado a cabo por una Administración tributaria autonómica al Servicio de Salud de la Comunidad Autónoma de determinada información que, a su juicio, resultaría necesaria para verificar el domicilio fiscal de determinados contribuyentes, incluyendo no sólo la información referida a la vigencia de la tarjeta sanitaria, su fecha de expedición, altas y bajas en la misma, teléfono y dirección de contacto facilitados, sino también la de los centros asistenciales de referencia que tuviera asignados el contribuyente y la especificación de la realización de determinados actos médicos referidos a aquél.

■ La validez de la cesión a los órganos competentes en materia estadística de los datos del

número de teléfono de los hogares o personas a las que se fuera a realizar una determinada encuesta incluida en el correspondiente Plan Estadístico por parte de distintos Órganos de las Administraciones Públicas que se hallasen en posesión del citado dato, al amparo de lo dispuesto en la legislación reguladora de la función estadística pública.

■ El posible amparo en la regla del interés legítimo prevalente de un tratamiento consistente en la recogida de un número limitado de datos relacionados con las redes WIFI abiertas existentes en una determinada localidad, que incidentalmente podrían incluir datos de carácter personal, con la finalidad de realizar un estudio para mostrar el estado de seguridad WIFI de la ciudad y concienciar a la ciudadanía de su importancia, teniendo en cuenta las salvaguardas adicionales facilitadas por el solicitante y relacionadas con la reducción de los plazos de conservación de los datos o la limitación en el acceso a los mismos.

■ La imposibilidad de amparar en un interés legítimo meramente comercial el tratamiento, a través de un software de reconocimiento facial, de los patrones biométricos del rostro de los clientes que accedan a un establecimiento, a fin de identificar si los clientes vuelven al mismo, así como la periodicidad con que lo hacen, suponiendo una injerencia desproporcionada en su intimidad.

■ La proporcionalidad de la inclusión en la base de datos de puntos de suministro eléctrico de los datos relacionados con el consumo, si bien agregados por período tarifario, sin que se incluyan los datos correspondientes a la curva de carga horaria, toda vez que ello permitiría una realización de perfiles detallados de los consu-

midores que excedería de la finalidad de la mencionada Base de datos.

■ La procedencia de atender el derecho de oposición ejercitado por un interesado en relación con la publicación en un Diario Oficial de la lista de admitidos y excluidos en un proceso selectivo siempre que concurriesen los requisitos exigidos por la STJUE de 13 de mayo de 2014, lo que sucedería en caso de que los datos pudieran considerarse obsoletos por haber devenido firme la resolución que pusiera fin al procedimiento selectivo en cuyo seno se llevó a cabo la publicación. El derecho podría atenderse mediante el establecimiento de protocolos de no indexación.

■ El mantenimiento de la doctrina de la Agencia en lo que respecta a la legitimación para el tratamiento derivada del establecimiento de sistemas de videovigilancia, que no se ve alterada como consecuencia de la entrada en vigor de la Ley 5/2014, de Seguridad Privada. De este modo, la intervención de una empresa de seguridad privada únicamente sería exigible para el tratamiento de datos relacionado con la videovigilancia en caso de que aquél se encontrase conectado a una central de alarmas, amparándose el tratamiento en lo dispuesto en el artículo 7 f) de la Directiva 95/46/CE, tal y como se deriva de la STJUE recaída en el asunto Tynes, UOUU.

■ La licitud de la instalación en una finca de una videocámara que captaría imágenes de una zona en que está constituida una servidumbre de paso a favor de los titulares de la finca colindante a la misma, siempre que se dé cumplimiento a lo exigido por la Instrucción 1/2006 de la AEPD en cuanto al cumplimiento del principio de proporcionalidad y del deber de información.

- La ilicitud del establecimiento por centros docentes de sistemas de videovigilancia para el seguimiento continuo de la actividad de los trabajadores de un centro, monitorizando por completo su actividad laboral, debido a la intrusión en la vida privada que ello representa, al carácter amplio e ilimitado del sistema y a la posible utilización de otros medios alternativos que permitieran la consecución de los fines de control perseguidos. También se indicó que la utilización de las imágenes tomadas para el control laboral con otros fines, tales como poner al empleado que se considere como ejemplo de buen trabajo o lo contrario, e incluso utilizar las imágenes para la publicidad de la empresa no resultaba amparado en el artículo 20.4 del estatuto de los Trabajadores.
- La conformidad a derecho de la publicación de los censos que sirven de base para el desarrollo de las elecciones sindicales en los que se contienen diversos datos personales de los empleados públicos como la edad, antigüedad en la Administración y número del DNI, al amparo de la normativa laboral y las especiales características del procedimiento aplicable a las elecciones sindicales.
- La irrelevancia de la doctrina sentada por la sentencia del Tribunal de Justicia de la UE de 6 de octubre de 2015 (asunto Schrems) en los supuestos de transferencias internacionales de datos a Estados Unidos que se fundamenten en modelos contractuales cuyos contratos marco hubieran sido previamente objeto de autorización específica por parte de esta Agencia (en el supuesto en cuestión se trataba de transferencias efectuadas en a un proveedor de servicios de cloud computing cuyo contrato marco había sido ya autorizado por la Agencia en 2014).

■ Transferencias internacionales de datos

Las transferencias internacionales de datos constituyen un elemento consustancial al tratamiento de datos personales en una economía globalizada y en la prestación de servicios tecnológicos y de la sociedad de la información en la que intervienen agentes ubicados en una multiplicidad de países. Es por ello necesario ofrecer una información sobre la evolución de los flujos internacionales de datos personales que permita apreciar sus tendencias en el ámbito nacional y europeo.

En 2015 se presentaron 128 solicitudes de autorización de transferencias internacionales de datos que han dado lugar a 108 autorizaciones, cifra inferior a las autorizaciones concedidas en el pasado año (150), con las que se elevan a 1.340 el total de autorizaciones para transferencias internacionales concedidas por la Agencia Española de Protección de Datos.

Por países destinatarios de los flujos de datos, destacan las transferencias autorizadas a India (39), EEUU (30) y a diversos países de Iberoamérica (29).

En lo que respecta al tipo de garantías aportadas en las solicitudes de autorización, la gran mayoría (66%) ha utilizado las cláusulas contractuales tipo que regulan la prestación de servicios, es decir, las previstas en la Decisión de la Comisión Europea 2010/87/CE, mientras que el 18% de las autorizaciones se han basado en las garantías proporcionadas por los dos modelos de cláusulas tipo establecidas por la Comisión Europea en su Decisión 2001/497/CE para transferencias entre responsables de tratamiento.

También se han tramitado y concedido 11 autorizaciones para transferencias internacionales de datos basadas en las garantías proporcionadas por

MEMORIA 2015

las denominadas Reglas Corporativas Vinculantes (BCR, por sus siglas en inglés).

Durante 2015 se tramitaron 6 expedientes para la autorización de transferencias internacionales de entidades exportadoras de datos que actúan en la transferencia en calidad de encargados de tratamiento de los responsables de los ficheros. En estos casos, la autorización para la transferencia internacional de datos de carácter personal permite que el encargado del tratamiento pueda actuar como exportador de datos y realizar transferencias internacionales en el marco de una subcontratación de servicios y al amparo de la autorización solicitada. De este modo, los responsables de tratamiento que contratan sus servicios ven simplificadas sus obligaciones ya que sólo tienen que notificar a la Agencia Española de Protección de Datos los ficheros afectados por la transferencia para su inscripción registral.

Desde 2012 se han concedido 22 autorizaciones de este tipo, de las que se han beneficiado 900 entidades responsables de ficheros que no han necesitado solicitar la correspondiente autorización para la transferencia internacional de sus datos.

Asimismo, durante 2015, nueve responsables de ficheros han notificado las transferencias internacionales de los datos de 27 ficheros inscritos en el RGPD al amparo de la resolución, dictada en 2014 por la Agencia Española de Protección de Datos, que consideró como garantías suficientes para las transferencias internacionales a EEUU las incluidas en los modelos de contrato aportados por un prestador de servicios de computación en la nube. De conformidad con dicha decisión, los clientes que contraten los servicios a los que afecta la resolución y suscriban los contratos que fueron considerados como garantías suficientes no necesitan solicitar la autorización para las transferencias internaciona-

les, sino sólo notificar los ficheros a cuyos datos afecta la transferencia.

Estas cifras permiten valorar positivamente las iniciativas de la AEPD para impulsar fórmulas flexibles que faciliten las transferencias internacionales de datos, imprescindibles en un mundo globalizado.

En el marco del procedimiento coordinado establecido por el Grupo del Artículo 29 de la Directiva 95/46/CE, la AEPD ha participado en la revisión de 10 solicitudes de aprobación de BCR de grupos multinacionales presentadas ante las siguientes Autoridades de Control:

- Francia (CNIL): grupo Capgemini, tanto BCR de responsables del tratamiento como de encargados del tratamiento, en las que las entidades del grupo actúan como encargados del tratamiento de los datos de sus clientes.
- Reino Unido (ICO): grupo BT, con BCR de responsables y BCR de encargados, y grupo Fluor.
- Holanda: grupo Gibson Innovation (BCR para datos de clientes y para datos de empleados), grupo NetApp y grupo Nutreco (también dos juegos de BCR, una para datos de clientes y otra para los empleados).

Asimismo, la AEPD ha continuado participando en el Subgrupo de Transferencias Internacionales creado por el Grupo del Artículo 29 en el que a lo largo de 2015 se han discutido diversos asuntos como las BCR, tanto de responsable como de encargado, la revisión de cláusulas contractuales en el marco de la prestación de servicios de contratación en la nube, cláusulas contractuales de encargado a subencargado, así como la discusión de diversos temas comunes relacionados con las transferencias internacionales de datos.

B - UNA RESPUESTA INTEGRAL PARA GARANTIZAR LOS DERECHOS DE LOS CIUDADANOS

En 2015 se ha producido una disminución del número de denuncias presentadas ante la Agencia. Así, mientras que en 2014 se recibieron 10.074 denuncias, lo que supuso un incremento de un 14,80% respecto de 2013, en 2015 se han recibido 8.489, lo que ha supuesto un decremento descenso respecto de 2014 de un 15,73%. Se produce así en 2015, grosso modo, una vuelta a las cifras registradas en 2013.

En el caso de las reclamaciones de tutela de derechos, en cambio, no se han producido variaciones sustanciales en los últimos tres años, siendo su número (2.082), muy similar al del año anterior (2.099).

En cuanto a la tramitación realizada de esas denuncias y reclamaciones, hay que destacar el esfuerzo realizado por el personal de la Agencia que en 2015 han tramitado 10.871 denuncias frente a las 9.404 resueltas en 2014 o las 8.633 resueltas en 2013. Ello supone, respecto de 2014, un incremento de las resoluciones de denuncias de un 15,60%. En el ámbito de las tutelas, se han resuelto en 2015 2.113 reclamaciones, frente a las 1.818 resueltas en 2014 o las 2.108 resoluciones de 2013. Respecto de 2014, por tanto, se produce un incremento de un 16,23%. De esta información se desprende que ha habido, respecto de 2014, un incremento medio de las resoluciones de reclamaciones y denuncias de un 15,70%.

Por otra parte, hay que destacar, que desde la última ampliación de personal asignado a la AEPD en el año 2008, se ha ido produciendo un incremento sistemático de las resoluciones de denuncias y de reclamaciones de tutelas de derecho. El total de resoluciones en 2008 fue de 3.519, y en 2015 se

produjeron 12.984 resoluciones de denuncias y de reclamaciones, por lo que en los últimos años se ha casi cuadruplicado la productividad de los efectivos de la Agencia.

A finales de año, se creó una Unidad de admisión a trámite de las reclamaciones de los ciudadanos, encargada específicamente de analizar las denuncias recibidas para permitir, en un breve lapso temporal desde su presentación, indicar las evidencias en la que la colaboración del reclamante es necesaria para fundar la reclamación ofreciendo información sobre cómo pueden obtenerlas.

La creación de esta Unidad es una de las medidas organizativas contemplada en el Plan Estratégico 2015-2019 de la Agencia para mejorar la gestión y la atención a los ciudadanos. Se espera que dicha Unidad facilite la tramitación de las reclamaciones, dando curso de las mismas a las áreas de la S.G. de Inspección de las denuncias que puede suponer vulneración LOPD y tramitando de manera ágil las que carezcan de fundamento o no sean de competencia de esta Agencia.

Dicha Unidad también ha empezado a encargarse de la solicitud de subsanación de la documentación aportada por el denunciante en aquellos supuestos en que las carencias en dicha documentación resulten evidentes. Todo ello pretende conseguir redundará en una mejora de los tiempos de tramitación que será visible previsiblemente en 2016.

Como se comentaba con anterioridad, las resoluciones de apercibimiento han tenido un incremento en 2015 de un 26% respecto de 2014. Este incremento tiene su reflejo fundamentalmente en el ámbito de la videovigilancia debido a la habitual presencia, como denunciados, de particulares y pymes sobre los que procede aplicar los criterios de atenuación de la culpabilidad



y antijuridicidad previstos en la LOPD en el caso de no haber sido sancionados o apercibidos previamente. Dentro de las resoluciones de apercibimiento también hay que señalar que en 2015 se produjo un aumento de las resoluciones que declaran el archivo. En 2015 se resolvió el archivo en 216 casos, mientras que en 2014 se produjo en 127 casos. Es decir, se ha producido un incremento de más de un 70% en las resoluciones de archivo de apercibimientos. Como se ha mencionado, su número afecta mayoritariamente al ámbito de la videovigilancia, aunque también hay que añadir el caso de comunicaciones comerciales electrónicas (spam).

Dado que en el ámbito sancionador se pretende una intervención mínima cuando se puedan elegir otras medidas correctivas, sobre todo, teniendo en cuenta la entidad y el carácter del denunciado (par-

ticulares o pequeñas empresas), este cambio de tendencia tiende a salvaguardar los intereses de las personas o entidades, sin merma de las garantías y obligaciones contenidas en la LOPD.

Las cifras correspondientes a las actuaciones de investigación iniciadas en 2015 también son equivalentes a las de procedimientos sancionadores resueltos por actividad investigada. Así, se puede decir que las investigaciones en telecomunicaciones (23,68%), entidades financieras (21,26%) y video-vigilancia (14,23%), por ese orden, y porcentualmente respecto del total de investigaciones realizadas, han sido las más trascendentales por número de expedientes tramitados. Destaca el incremento de las dos últimas respecto de 2014 (12,27% y 19,77%), a pesar del menor número de denuncias presentadas en la Agencia.

En el capítulo de las sanciones impuestas, se confirma la tendencia decreciente en los últimos años. Durante 2015 se han declarado sanciones por importe de 13.712.621 euros. En 2014 el importe fue de 17.002.622 euros y en 2013 fue de 22.339.440 euros. Entre las principales causas del descenso se sitúan las ya apuntadas anteriormente, como son la reducción de las denuncias presentadas ante la Agencia o la utilización de la figura del apercibimiento con expresión de las medidas correctoras necesarias. Las sanciones de mayor cuantía han recaído, como en otros años, en empresas de telecomunicaciones (51% del total), seguidas de las entidades financieras (17%), y en tercer lugar, a las empresas encargadas del suministro y comercialización de energía o agua (8,7%). De estas cifras, en comparación con 2014, destaca la disminución de las sanciones impuestas a las empresas de telecomunicaciones o a las de los citados suministros.

Estas sanciones, que en sus cuantías superiores suelen imponerse por actividades que vulneran normas en materia del consentimiento para la contratación o la inclusión de personas en ficheros de solvencia patrimonial, han tenido, como se dice, un significativo decremento. También es de destacar el incremento importante de las sanciones impuestas a empresas que se dedican a la emisión de comunicaciones electrónicas comerciales (un 39% respecto de 2014).

En cumplimiento de las competencias atribuidas en relación al artículo 22.2 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, la AEPD recibió y trató un 43% más de denuncias (56) que durante 2014 (39) sobre la falta de la adecuada información a los usuarios de internet a la hora de utilizar cookies en las páginas web y por no recabar el consentimiento para la utilización de estos dispositivos.

MEMORIA 2015

Durante el año 2015 se aplicó la modificación introducida en el apartado 38.4.g de la Ley 34/2002 por la disposición final segunda de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, por la que también resulta sancionable la falta de un consentimiento previo del usuario a la utilización por parte de un sitio web de dispositivos de almacenamiento y recuperación de datos, lo que generó las primeras resoluciones en ese sentido.

Pormenorizando las denuncias formuladas ante la Agencia los sectores más relevantes son los siguientes:

■ CONTRATACIÓN IRREGULAR Y MOROSIDAD

En el año 2015, aunque ha habido un descenso respecto al año 2014, las reclamaciones registradas en el área de morosidad y fraude se han centrado en varios supuestos. En relación al fraude, al igual que otros años, destaca el supuesto de contratación sin el consentimiento del titular. Esto ha afectado especialmente al sector de las telecomunicaciones y al de las empresas comercializadoras de los suministros de agua y energía.

Asimismo, se han incoado numerosos procedimientos por la compra de terminales móviles sin el consentimiento del titular que, siendo cliente, tiene conocimiento de ello a través de las facturas.

Además tiene importancia la contratación fraudulenta de líneas telefónicas que generan una deuda, que posteriormente es cedida a otra empresa, ésta con sede fuera de España.

En cuanto a la tipología de las denuncias investigadas y sancionadas en el área de morosidad, aparecen referidas a la inclusión en ficheros de solvencia patrimonial, ya sea tras el pago de la deuda, tras haber sido cuestionada ante la Secretaría de Esta-

do de Telecomunicaciones y para la Sociedad de la información (SETSI), las Juntas Arbitrales o ante los juzgados; o bien sin que la entidad haya requerido previamente el pago de la deuda por la entidad acreedora ni haya facilitado un plazo para el pago de la misma, transcurrido el cual deberían haber informado al afectado de la posibilidad de dicha inclusión.

También ha sido común la venta de cartera de deudas entre las que se incluye una deuda pagada.

En relación con estas conductas es preciso reiterar que la inclusión indebida en ficheros de morosidad produce unos efectos especialmente negativos para los ciudadanos afectados en relación con el acceso a todo tipo de servicios, por los que las empresas han de extremar su diligencia antes de comunicar información inexacta a los mismos.

Finalmente, destaca la consulta de datos personales en ficheros de solvencia patrimonial de afectados que no son clientes de la entidad que efectúa la consulta.

Por otro lado, se consolida en 2015 el criterio de considerar documentación suficiente, a efectos de lo previsto en el artículo 38.3 del RLOPD, la aportación de una serie de documentos que vendrían a acreditar el cumplimiento de requerimiento de pago con anterioridad a la inclusión en ficheros comunes de solvencia.

Esta serie de requisitos, o para ser más exactos, fases de la trazabilidad del envío efectivo con diligencia, se podrían resumir en: (1) carta referenciada e individualizada a nombre del denunciante con detalle de la deuda y advertencia de que su impago puede ocasionar la inclusión en ficheros de morosidad; (2) certificado de tercera/s entidad/es independiente/s que acredite su generación, impresión y puesta en correos; (3) documento acreditativo del

correspondiente gestor postal de dicha recepción para su tramitación y (4) certificado de un control auditible de la devolución de dicho requerimiento.

■ VIDEOVIGILANCIA

En materia de videovigilancia se viene a confirmar la tendencia general de los ejercicios anteriores, tal y como se señaló anteriormente. Las resoluciones recaídas han sido de nuevo mayoritariamente de apercibimiento, debido a la habitual presencia –como denunciados– de particulares y pymes sobre los que procede aplicar los criterios de disminución de culpabilidad y antijuridicidad exigidos en la LOPD así como el requisito de no haber sido sancionados o apercibidos previamente.

Como novedades respecto a años anteriores, cabe destacar el cambio en el criterio de la Agencia en relación con las cámaras simuladas/sin funcionamiento. Frente a la práctica de sancionar por incumplimiento de los requerimientos de la Agencia, ahora se archivan las actuaciones investigadoras ante la ausencia de tratamiento real de datos de carácter personal.

También hay que mencionar el criterio adoptado por la Agencia en relación a la videovigilancia en centros escolares, donde la instalación de cámaras puede servir al interés superior del menor contribuyendo a una mayor seguridad en los patios y en el comedor. Ahora bien, dicho interés no tiene por qué ser absoluto, ya que es fundamental la ponderación de los intereses afectados. Por ello, deberán imponerse estrictas medidas en cuanto al acceso a las imágenes, tanto en el visionado inicial como en los posibles accesos a las grabaciones.

Asimismo, en materia de videovigilancia, durante 2015 la Agencia ha procedido a interpretar y aplicar en múltiples resoluciones, lo dispuesto en el artículo 7.f) de la Directiva 95/46/CE que esta-

blece dos requisitos acumulativos para que un tratamiento de datos personales sea lícito; 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. Es necesaria una ponderación 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.

En la actividad de videovigilancia cabe destacar las siguientes resoluciones:

- Videovigilancia que capta imágenes de espacios públicos y ajenos - A/00359/2014

La Guardia Civil informa que una empresa dispone de un sistema de videovigilancia que podría infringir la LOPD. De las actuaciones practicadas se acredita que dos cámaras (una de ellas con propiedades de zoom y movimiento), de las ocho que componen el sistema, enfocan y captan imágenes de espacios públicos ajenos a los propios de la empresa denunciada. Los hechos constituyen una infracción del artículo 6 de la LOPD, tipificada como grave en el artículo 44.3.b), al tratar las imágenes captadas en dichos espacios sin disponer del consentimiento de los afectados ni de legitimación para ello, pues la instalación de videocámaras en lugares públicos es competencia exclusiva de las Fuerzas y Cuerpos de Seguridad (Ley Orgánica 4/1997). La empresa ha comunicado que ha desactivado las propiedades del zoom y movimiento de la cámara y modificado los ángulos de enfoque, pero no acredita que

ya no se capten imágenes desproporcionadas. En aplicación de lo dispuesto en el artículo 45.6 de la LOPD se apercibe a la empresa denunciada y se la requiere para que retire las cámaras de referencia, o bien las reoriente para que no capte datos desproporcionados, y se informe y acredite a la Agencia el cumplimiento del requerimiento.

- Vídeo grabado a efectos probatorios - E/04071/2014

Se denuncia la grabación de las imágenes del acto de ejecución de una decisión judicial sobre derecho de paso a una finca, propiedad del denunciante y de los denunciados, al que aquel acudió acompañado de un notario. La grabación se llevó a cabo por los denunciados, que alegan que se realizó para disponer de una prueba en caso de que se denunciase que se había impedido el derecho de paso. En este caso la captación de imágenes resulta proporcional y nada impide la grabación de imágenes de un funcionario público, por lo que al no haberse acreditado tratamiento de difusión alguno de las imágenes no se puede considerar que la grabación haya sido indebida. No obstante, la utilización de las imágenes únicamente puede tener como fin el ejercicio del derecho de defensa. Se acuerda el archivo de las actuaciones.

■ SANIDAD

En el sector de Sanidad se ha producido un incremento de las denuncias debidas a los accesos injustificados a las historias clínicas de los denunciantes. Se han declarado infracciones al hospital afectado por incumplimiento de las medidas de seguridad; y al autor de los accesos por desvío de finalidad.

También se han investigado las denuncias presentadas sobre las actuaciones de las clínicas privadas como colaboradoras de las Administraciones Públi-

cas sanitarias, resolviéndose que, al existir Conciergos entre las Administraciones sanitarias de cada Comunidad Autónoma y determinadas clínicas privadas, existe habilitación legal para la comunicación de datos entre los centros públicos y los privados. Los procedimientos más destacados se recogen en el apartado de «Administraciones públicas de esta Memoria».

■ MEDIDAS DE SEGURIDAD

Las resoluciones más destacadas son las siguientes:

- Incumplimiento de medidas de seguridad por parte de operador de telecomunicaciones - PS/00713/2014

La Agencia tuvo conocimiento, a través de un abonado, de que resultaba posible acceder, sin restricción alguna, a los datos personales (incluyendo facturas) de otros clientes, a través del Área de Clientes habilitada en el sitio web de Jazztel, con solo modificar en el navegador el identificador numérico que se incluye en la dirección web de acceso. Esta quiebra suponía un nuevo incumplimiento por parte del operador, que ya había sido sancionado en el 2012 por los hechos similares.

- Incumplimiento de medidas de seguridad por parte de operador de telecomunicaciones - PS/00467/2015

A través de dos denuncias la Agencia detecta un error en la generación de un proceso de facturación del operador ONO, que permitió a unos abonados acceder, en un limitado período de tiempo, a los datos de otros. Durante el procedimiento el operador reconoció su responsabilidad, exponiendo las medidas adoptadas para evitar una nueva quiebra de seguridad.

- Incidencia de seguridad en una web especializada en la venta de servicios turísticos - PS/00320/2015

Acreditación de una quiebra de seguridad que permitía a la denunciante, en determinadas circunstancias, acceder a las facturas de otros clientes. La compañía manifestó que la incidencia ya había tenido lugar en otras ocasiones y se creía solucionada, reconociendo su responsabilidad.

- Indexación en buscadores de los documentos de tramitación judicial de reclamaciones de clientes de una entidad financiera - PS/00687/2014

Se constata un incumplimiento de medidas de seguridad por parte del despacho que llevaba la defensa jurídica de un banco, al no haber evitado que, debido a una incidencia de configuración, los documentos almacenados en los servidores de un tercero (que incluían requerimientos de pago, escrituras, actas notariales, demandas hipotecarias, etc.) pudieran ser indexados por los motores de búsqueda.

- Medidas de seguridad insuficientes para garantizar la confidencialidad en internet de los clientes de una empresa de servicios de mensajería con un gran volumen de actividad - PS/00240/2015

Se sancionó una insuficiente implementación de medidas de seguridad al acreditarse que los clientes que habían puesto una reclamación podían acceder a datos de otros reclamantes con solo modificar en el navegador el número de la reclamación. Durante la tramitación del procedimiento la compañía acreditó haber restringido el acceso al contenido del texto de las reclamaciones.

- Empleo de tecnologías contactless - PS/00002/2015

Se inició una investigación en relación a una denuncia sobre el acceso a distancia de los datos de

nombre y PAN (número de tarjeta) de las tarjetas de crédito de una entidad financiera que incorporan la tecnología contactless. Durante las actuaciones se puso de manifiesto que las tarjetas bancarias se habían entregado a los clientes sin informarles de los riesgos, pese a disponer de informes internos que alertaban de los mismos en relación a la privacidad. Dicha investigación culminó con una sanción por una infracción del artículo 9 de la LOPD, tipificada como grave.

■ REDES SOCIALES

- Divulgación de detalles íntimos de una relación de pareja por parte de uno de los miembros - PS/00721/2014

El procedimiento se tramitó a raíz de las denuncias presentadas por una mujer y sus familiares contra el exnovio de la primera, por la publicación en la red social Facebook de abundantes detalles íntimos, incluyendo fotografías, tras la ruptura de la relación de pareja. El perfil expresamente creado para difundir estas informaciones había sido vinculado por el autor con numerosas organizaciones religiosas del entorno de la afectada, para darle mayor proyección pública. Se sancionó el tratamiento no consentido de los datos de la afectada y sus familiares.

- Suplantación en redes sociales de la identidad de varios trabajadores de una empresa pública madrileña - PS/00327/2013

Los denunciantes se referían a varios perfiles, creados en Facebook, Twitter y Linkedin, con sus nombres y apellidos, y fotografías. Tras la resolución de las correspondientes actuaciones judiciales, la Agencia sancionó al autor de algunos de los perfiles denunciados por el tratamiento no consentido de los datos personales.

- Utilización no consentida de la imagen de la denunciante en un portal de contactos - PS/00709/2014

La afectada denunciaba a otra persona, por utilizar, sin su consentimiento, su imagen fotográfica en un perfil personal en un portal como reclamo para contactar con personas que pudieran estar interesadas en participar en los espectáculos de contenido sexual que organiza la empresa que dirige el denunciado. Se sancionó al denunciado como creador del perfil.

■ COMUNICACIONES COMERCIALES

En materia de publicidad destaca el incremento de los procedimientos sancionadores y de apercibimiento tramitados por el envío, a través de medios electrónicos, de publicidad no deseada; o de publicidad que no ofrece un procedimiento para solicitar el cese en los envíos. En este sentido, se considera que no se ofrece dicho procedimiento si el medio proporcionado no funciona.

El volumen de procedimientos sancionadores tramitados por la realización de llamadas comerciales sin consentimiento o a través de una línea telefónica registrada en la lista Robinson se mantiene en segundo lugar en el caso de los tramitados por el envío de publicidad electrónica, ocupando el tercer lugar los relacionados con la publicidad postal.

En dicho ámbito de la publicidad postal cabe resaltar que en la mayoría de los casos la entidad responsable del fichero, utilizado para la campaña publicitaria, no pudo acreditar el origen de los datos personales utilizados.

Dado el número de denuncias que se reciben y de procedimientos que se tramitan por las acciones publicitarias realizadas por unas entidades concretas, se han realizado investigaciones para escla-

MEMORIA 2015

recer la responsabilidad de los anunciantes o de otros sujetos en aplicación de lo que dispone el Reglamento de desarrollo de la LOPD, y así decidir quién ha fijado los parámetros de la campaña y a quiénes corresponde la responsabilidad del tratamiento de datos.

Así, se han analizado diversas bases de datos comercializadas para marketing directo que incluyen datos de empresas y direcciones electrónicas de personas de contacto, cuyo tratamiento está sujeto a la LOPD, al superar el uso estrictamente profesional, limitado a las funciones empresariales o profesionales de sus titulares, pues su finalidad es la de marketing directo (Business to Consumer).

También hay que mencionar la tramitación de procedimientos sancionadores y de apercibimiento en relación con la adecuación a la LOPD de numerosas cláusulas informativas recogidas en páginas web, iniciándose un total de 18 procedimientos sancionadores, 21 de apercibimiento y uno de Administraciones públicas.

Por otro lado, la Agencia ha sancionado a los operadores que facilitaron a la CNMC, para su inclusión en Guías, datos de abonados que habían manifestado su negativa a figurar en ellas.

En este sentido se pueden destacar las siguientes resoluciones:

- Base de datos para marketing directo - PS/00609/2014

Se inician de oficio actuaciones de inspección en relación con la venta de una base de datos de empresas para campañas de publicidad. La base de datos incluye direcciones electrónicas que se consideran datos de carácter personal al encontrarse asignadas a personas físicas y superar su uso el ámbito estrictamente profesional, pues su recogida y

utilización tiene como finalidad realizar acciones de marketing directo dirigidas a su titular (Business to Consumer). No se ha justificado que las direcciones electrónicas procedan de fuentes accesibles al público, ya que internet no tiene esta consideración. En consecuencia, su tratamiento necesita el consentimiento del interesado, hecho que la entidad no acredita.

- Llamadas telefónicas comerciales a una línea de teléfono incluida en la Lista Robinson utilizando datos sin actualizar - PS/00369/2014

Se denuncia la recepción de llamadas telefónicas comerciales en una línea que había sido incluida en la Lista Robinson. La entidad denunciada realizó las llamadas sin el consentimiento del interesado y sin que concurriera ninguna causa para la legitimación de dicho tratamiento, pues la fuente de la que obtuvo los datos había perdido su carácter de fuente accesible al público al haber transcurrido, en el momento de efectuarlas, más de un año desde su obtención. También se constató la emisión de llamadas al número del denunciante por otras entidades, que recurrieron a una página web en la que el dato relativo a la línea de telefonía del denunciante estaba asociado a los datos de un tercero. Además, quedó acreditada la inclusión de la citada línea en la Lista Robinson.

- Remisión de correos electrónicos comerciales a un destinatario después de haber solicitado el cese de los envíos - PS/00454/2015

El denunciante había solicitado a la entidad remitente el cese en el envío de comunicaciones comerciales. Sin embargo, la entidad continuó tratando los datos del denunciante para remitirle comunicaciones comerciales a través de medios electrónicos. La entidad atribuye dichos envíos a una deficiencia

técnica que, según considera, excluye la culpabilidad. La resolución razona que no se había adoptado la diligencia debida y declara el incumplimiento de la prohibición de enviar comunicaciones promocionales sin autorización previa, pues se había comunicado la oposición a recibirlas.

- Campaña de promoción comercial. Obstaculización del derecho de oposición. Ausencia de consentimiento - PS/00290/2015

El denunciante recibe correos electrónicos comerciales de productos de una entidad a la que había manifestado su oposición al tratamiento de sus datos con fines publicitarios. La campaña de marketing fue llevada a cabo por una tercera entidad contratada por el anunciante, que debía utilizar bases de datos propias o de terceros. El anunciante no trasladó la oposición del denunciante a recibir comunicaciones comerciales a dicha entidad, obstaculizando con su conducta el derecho de oposición del denunciante al no adoptar medidas, tendentes a hacerlo efectivo. Estos hechos constituyen una infracción de los artículos 17.1 y 30.4 de la LOPD. En este caso, la resolución también considera que se incumplió la prohibición contenida en el artículo 21 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, por parte de la entidad responsable del fichero utilizado al no contar con el consentimiento previo del denunciante.

- Tratamiento del dato de una dirección de correo electrónico excluida del ámbito de aplicación de la normativa de protección de datos - E/07930/2014

El denunciante, empleado de una universidad, manifiesta haber recibido un correo electrónico no consentido en su dirección electrónica profesional.

El citado correo no tiene un contenido comercial y se dirige al denunciante en su condición de empleado de la universidad. No resulta de aplicación a este caso la LSSI al no tener el correo finalidad comercial y tampoco la LOPD, ya que el artículo 2.2 del RLOPD excluye de su aplicación los tratamientos de datos de las personas físicas –entre ellos el correo electrónico profesional– que presten sus servicios en personas jurídicas, por lo que se archivan las actuaciones.

■ PROCEDIMIENTOS JUDICIALES

La doctrina según la cual resulta acorde con la LOPD la entrega de documentación sin requerimiento del Juzgado por las partes en el procedimiento en el ejercicio del derecho a la defensa se consolida. En este caso, se pueden destacar las siguientes resoluciones:

- Aportación de antecedentes penales a procedimiento judicial. Cesión de Datos - E/1021/2015

Denuncia que, formulada demanda de desahucio contra el denunciante y un tercero, en dicha demanda el letrado aporta los antecedentes penales del denunciante mediante un certificado del Registro Central de Penados.

La resolución de archivo señala que el certificado fue obtenido legalmente por funcionario habilitado de la Oficina judicial del Juzgado de Instrucción e incorporado a las diligencias urgentes. Sobre si los abogados y procuradores están exceptuados de obtener el consentimiento para el tratamiento de datos de sus contrarios, la respuesta es afirmativa, ya que de lo contrario la exigibilidad del consentimiento del oponente supondría dejar a disposición de aquél el hecho de que el denunciante pueda ejercer, en plenitud, su derecho a la tutela judicial efectiva.

■ RELACIONES LABORALES

En este ámbito, se consolida la interpretación del acceso del empresario a los correos, accesos a internet e instalación y acceso a los datos del GPS, siempre que previamente se haya informado a los trabajadores/representación sindical.

El Tribunal Supremo se ha manifestado sobre la prohibición de que se recoja en los contratos laborales la obligación de los trabajadores de facilitar el número de teléfono y/o correo electrónico particular como medio de comunicación entre el empresario y el trabajador. Son reseñables los siguientes casos:

- Cuestionario a cumplimentar por los trabajadores en el que se solicitan datos de terceros.
Tratamiento sin consentimiento - E/4485/2014

Denuncia a una empresa por remitir a sus trabajadores un cuestionario de conflicto de intereses en el que se solicitan datos de terceros que tengan vínculos familiares o de otro tipo ante la posible existencia de un conflicto de intereses en la relación laboral.

El tratamiento de datos de terceros por parte de la empresa se basa en el interés legítimo que prevalece sobre los derechos de terceros, toda vez que se trata de datos pertinentes. Se informa del motivo y las condiciones para llenar el cuestionario (que sólo es obligado en determinados supuestos); el tratamiento de los datos se limita a la finalidad para la que se recaban y no consta que estos trasciendan fuera del ámbito de la empresa, por lo que se procede al archivo.

- Utilización de localizador GPS en un vehículo de empresa y uso de los datos a efectos disciplinarios - E/ 6036/2014

Varios trabajadores denuncian a su empresa por haber sido despedidos utilizando los datos obte-

nidos de un sistema de control de flotas con dispositivo GPS. El uso de dicho dispositivo no fue comunicado debidamente a los trabajadores, que desconocían la utilización que la empresa estaba haciendo de este sistema de control y nunca presataron el consentimiento.

Se declara el archivo, ya que se acredita que la empresa denunciada informa previamente a los trabajadores de la instalación de GPS en los vehículos de la empresa, conducta que observa las prescripciones previstas en la normativa sobre protección de datos y jurisprudencia consolidada.

- Videovigilancia en entorno laboral
- E/03579/2014

Denuncia contra AENA y Segur Ibérica por la visualización de las imágenes captadas por las cámaras del sistema de videovigilancia del aeropuerto de Tenerife Los Rodeos para la imposición de sanciones a trabajadores de Segur Ibérica. AENA es responsable del sistema de videovigilancia del aeropuerto, cuya implantación responde tanto a su interés legítimo como a la finalidad, también legítima, de seguridad. Segur Ibérica accede a las imágenes en condición de encargado del tratamiento siguiendo las instrucciones de AENA. En el presente caso, la auditoría llevada a cabo por AENA detectó incumplimientos y fallos en los filtros de seguridad por parte del personal de Segur Ibérica, que le fueron comunicados para que adoptase las medidas oportunas. Las imputaciones realizadas a los trabajadores sancionados tienen incidencia en materia de seguridad por lo que, en este caso, la utilización de las imágenes por el encargado del tratamiento se enmarca en la finalidad del sistema, sin que se aprecie que se hayan tratado para finalidades distintas de las conferidas en el encargo del tratamiento. Se archivan las actuaciones.

■ OTRAS RESOLUCIONES RELEVANTES EN EL SECTOR PRIVADO

En el ámbito de la contratación de servicios, es importante el volumen, como en otros años, de las denuncias presentadas por la reclamación de deudas (sin inclusión en ficheros de morosos) realizadas por los acreedores directamente o a través de encargados de tratamiento, que han dado lugar a la apertura de procedimientos sancionadores cuando la reclamación se realiza a persona distinta del deudor o sin constancia acreditada de la relación contractual que genera la deuda o a pesar del pago de la misma o de la anulación de las facturas. También se han tramitado expedientes relacionados con cesiones de créditos inexistentes realizadas en escenarios análogos a los anteriores.

Asimismo, se han tramitado numerosos procedimientos relacionados con la infracción del deber de secreto en las áreas virtuales habilitadas por las entidades a sus clientes, y con el tratamiento de datos sin consentimiento materializado en facturaciones tras baja del servicio o emisión de facturas a cuentas bancarias de titulares ajenos al contrato.

En particular, en el sector de las telecomunicaciones, continuando la línea seguida por esta Agencia tras la entrada en vigor de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, se ha sancionado a los operadores que facilitaron a la Comisión Nacional de los Mercados y la Competencia, para su inclusión en guías, datos de abonados que habían manifestado su negativa a figurar en ellas.

En el sector financiero, se ha analizado la adecuación a la LOPD de las solicitudes de información, documentación y consentimiento realizadas por las entidades financieras como consecuencia de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terroris-

mo. También ha habido procedimientos derivados de la falta de calidad de datos en los riesgos declarados por las entidades financieras al fichero CIRBE.

En materia de seguros, se han tramitado denuncias por la contratación de seguros de daños o de vida asociados a préstamos hipotecarios sin consentimiento de los afectados.

En el ámbito de las comunidades de propietarios, se consolida el criterio de tramitación de procedimiento sancionador/apercebimiento en las denuncias contra los administradores de fincas (encargados del tratamiento) por los órganos de la comunidad de propietarios (responsable del fichero) por no atender los requerimiento de devolución de la documentación de la comunidad, al ser cesados en su cargo sin tener suscrito un contrato para dicho encargo.

En el sector educativo muchas denuncias son consecuencia de la publicación de fotos de menores por parte de los centros de enseñanza sin que haya consentimiento de los padres. Es muy frecuente que las denuncias sean de padres separados y que haya consentido uno de los padres.

En cuanto a partidos políticos, la mayoría de las denuncias han sido objeto de inadmisión a trámite. Al ser año electoral, se han recibido varias denuncias sobre la publicidad electoral sin previo consentimiento de los afectados (se archivan porque la Ley Electoral habilita a que los partidos políticos envíen propaganda electoral durante el período previo a las elecciones). También hay denuncias sobre el tratamiento inconsentido de datos (se archivan si son personas relevantes y conocidas pertenecientes a partidos políticos o que desempeñen cargos públicos como concejales, alcaldes, etc.)

Las resoluciones más destacadas en este sentido son las siguientes:

MEMORIA 2015

■ Tratamiento de datos de carácter ideológico - PS/235/2015

Tras recibir diversas denuncias de ciudadanos por la recogida de datos en el marco de una encuesta relativa a las actividades del 9N y dirigida a cubrir todos los domicilios de la Comunidad de Cataluña, se iniciaron investigaciones que derivaron en un procedimiento sancionador contra las entidades Assemblea Nacional Catalana (ANC) y Òmnium Cultural. Se encontró, en las diferentes actuaciones de investigación realizadas, que ambas entidades habían cometido sendas infracciones del artículo 7.2 de la LOPD por realizar un tratamiento de datos de carácter ideológico, tipificada como muy grave, por lo que fueron sancionadas con sendas multas. En las investigaciones se determinó que era posible la identificación de determinadas personas que habían expresado ciertos juicios de valor que eran encuadrables en una determinada corriente ideológica, debido a anotaciones manuscritas hechas por los encuestadores y que aparecían en diversa documentación de las encuestas realizadas.

Además, se impuso una sanción adicional a la ANC por una falta de medidas de seguridad, calificada como grave, que expuso los datos de ciudadanos en internet.

■ Emisión de un contrato de seguro sin el consentimiento del interesado - PS/00330/2015

El afectado denuncia la contratación de dos seguros de hogar sin su consentimiento por parte de la aseguradora sobre viviendas que se encuentran hipotecadas con la entidad financiera, perteneciente al mismo grupo de empresas. Las pólizas se realizaron con la mediación de la entidad financiera, que actuó como operador de banca-seguros. Se acreditó la falta de consentimiento del denunciante que no concurrió ni en el momento de la contratación

de las pólizas ni en el momento de la firma de la escritura de préstamo. Los hechos constituyen, por parte de la aseguradora, una infracción del artículo 6 de la LOPD, por tratar datos de carácter personal del afectado para formalizarle un contrato sin su consentimiento, y por parte del operador de banca-seguros de una infracción del artículo 11 de la LOPD, que comunicó a la aseguradora los datos del denunciante.

■ Publicación de fotos de menores por parte de centros de enseñanza sin consentimiento de los padres - A/00145/2015

En el presente caso, se insertó una fotografía del hijo de la denunciante, menor de edad e incapacitado, en la revista del colegio, que no acreditó el consentimiento de los padres para hacerlo. Además, el modelo de formulario habilitado para la recogida del consentimiento que permitiera la realización y utilización de fotografías no incluye ninguna leyenda informativa, ya que se refiere únicamente a la normativa de protección del menor.

■ Publicación de fotos de policía antidisturbios formando parte de la exposición de una galería de arte - E/330/2015

Un sindicato policial denuncia que en una galería de arte se acoge una exposición compuesta por una serie de retratos de policías pertenecientes a las Unidades de Intervención de Policía del Cuerpo Nacional de Policía, que permitía la identificación de los mismos. Una fotografía que permite identificar una persona ha de considerarse un dato personal y para su tratamiento se precisa el consentimiento previo. Sin embargo, existen circunstancias que legitiman el tratamiento de dichos datos aun cuando no concurra el consentimiento. Por un lado la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal

y familiar y a la propia imagen en su artículo 8 establece un régimen de tratamiento de datos que permite la captación de imágenes dentro de un acontecimiento público, y su posterior difusión, sin que lo anterior suponga una intromisión ilegítima en el derecho a la intimidad del afectado, lo que se proyecta, de forma análoga, al ámbito regulado por la LOPD. Además, en este caso, las imágenes controvertidas se vinculan con el desarrollo de la actividad profesional de los afectados como funcionarios de la Policía Nacional, tomadas en ejercicio de sus funciones, ante un acontecimiento público. El acontecimiento fue objeto de cobertura por una pluralidad de medios de comunicación, es decir, no se trataba de una actividad privada o doméstica desarrollada en un ámbito íntimo, sino ante un acontecimiento de participación ciudadana, objeto de una amplia cobertura mediática, donde actuó la Policía en ejercicio de sus funciones profesionales. A esto se añade lo dispuesto en el artículo 20 de la Constitución Española, que reconoce y protege el derecho a la producción y creación literaria, artística, científica y técnica, por lo que, añadido a lo anterior, se resuelve archivar el expediente.

- Envío de propaganda electoral por varios partidos políticos - E/04054/2015

La denuncia se dirigía a varios partidos políticos: PP, PSOE, Nueva Canarias, IU y Alternativa Nacionalista Canaria, porque le habían mandado a su domicilio propaganda electoral con las papeletas de votación.

La Ley Orgánica 5/1985, de 19 de junio, de Régimen Electoral General, permite la realización de dichos envíos. Por tanto, se podrán llevar a cabo actos de propaganda dentro de dicho periodo a partir de los datos recabados del correspondiente censo electoral, al que están legitimados a acceder los representantes de las candidaturas legítimamente proclamadas

para participar en las correspondientes elecciones, sin que el ejercicio de dicha actividad se encuentre supeditado a la concurrencia de un consentimiento por parte de los electores para la recepción de la correspondiente propaganda electoral.

Finalmente en diciembre de 2015 se acordó la apertura de actuaciones previas de investigación (E/07646/2015) en relación con los hechos difundidos por los medios de comunicación sobre una supuesta quiebra de seguridad que habría afectado a los usuarios de juguetes de la marca VTECH, particularmente a los españoles, pudiendo estar afectados datos de menores de edad. Estas actuaciones no habían concluido en el periodo temporal al que se refiere esta Memoria.

■ ADMINISTRACIONES PÚBLICAS

En cuanto a los procedimientos de infracción seguidos contra Administraciones Públicas, destaca su incremento (78 procedimientos resueltos que dieron lugar a 57 infracciones declaradas) respecto de 2014 (60 procedimientos) y 2013 (58). Entre ellos, han tenido un fuerte incremento los seguidos contra Administraciones autonómicas (25 en 2015, frente a los 12 de 2014).

Las principales resoluciones son las siguientes:

- Cámaras en dependencias de policía local - E/02729/2014

El Sindicato Profesional de Policías Municipales de España denuncia al Ayuntamiento de Elche por no responder a su solicitud de información sobre la instalación de cámaras de videovigilancia en la Jefatura de Policía Local. Las cámaras se ubican tanto en el interior como en el exterior de la sede de la citada jefatura de policía con la finalidad de prevenir actos vandálicos y delictivos y garantizar la seguridad ciudadana, cuya gestión y control se

MEMORIA 2015

lleva a cabo por la Policía Local. Según el artículo 2.1 del Reglamento de desarrollo y ejecución de la Ley orgánica 4/1997, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, la LOPD no es de aplicación a las instalaciones fijas de videocámaras que realicen aquéllas en sus inmuebles, siempre que se dediquen exclusivamente a garantizar la seguridad y protección interior o exterior de los mismos, exclusión que no ampararía otras finalidades como el control laboral. Se acuerda el archivo de las actuaciones.

- Videovigilancia en centro penitenciario. Ausencia de carteles informativos - AP/00049/2014

Se denuncia la existencia de un sistema de videovigilancia en el centro penitenciario Madrid III – Valdemoro, sin tener inscrito el fichero en el RGPD. El tratamiento de las imágenes como datos de carácter personal obliga al responsable a informar a los afectados de los extremos establecidos en el artículo 5.1 de la LOPD. La falta de información constituye una infracción del mencionado artículo, de carácter leve, atribuible a la Secretaría General de Instituciones Penitenciarias.

- Inexistencia de medidas de seguridad adecuadas para impedir los accesos no autorizados - AP/00029/2015- PS/00266/2015

Se sanciona a la Consejería de Sanidad de la Comunidad Valenciana por no tener incorporadas las medidas de seguridad adecuadas que impidan accesos no autorizados. Se constató que entre enero de 2013 y abril de 2014, de los 603 accesos realizados a la historia clínica de la denunciante de este procedimiento, 496 fueron realizados por un profesional médico que no tiene encargada la asistencia sanitaria de la denunciante. La entidad imputada informó que los accesos realizados no tenían justificación clínico asistencial.

Todo ello llevó a considerar que la Conselleria denunciada carece de un control efectivo de los accesos a la información recogida en el fichero de historias clínicas de sus pacientes para el cumplimiento del principio de seguridad de los datos.

Se sancionó asimismo al profesional sanitario que accedió 496 veces sin justificación a la historia clínica de la denunciante. Era un médico, ex marido de la denunciante. Se sanciona porque ha accedido a la historia clínica para finalidades distintas para las que tiene habilitación.

- Envío de correos electrónicos sin cifrar - AP/00047/2015

El Servicio Madrileño de Salud, Hospital de Fuenlabrada, fue investigado por haber enviado correos electrónicos con datos de salud sin cifrar. De la información obtenida en el procedimiento se concluyó que el correo electrónico utilizado por el Servicio Madrileño de Salud para su uso institucional constituye un canal seguro de intercambio de información porque se utilizan los mecanismos que garantizan que la información no sea inteligible ni manipulada por terceros. Se procedió al archivo de las actuaciones.

- Envío de correos con datos de salud - AP/00048/2015, PS/00411/2015

Se investigó en el Servicio de Salud de la Comunidad de Castilla-La Mancha, tanto al Hospital Virgen de la Luz como al Hospital Recoletas. Se declaró la infracción de Virgen de la Luz por enviar correos electrónicos sin cifrar con datos de salud, aunque la situación fue corregida durante la tramitación del expediente. El procedimiento sancionador contra el hospital Recoletas se debió a que este subcontrató la prestación de servicios que tenía con Virgen de la Luz sin consentimiento.

- Tablón de anuncios de la TGSS –TEASS. Implementación de medidas de seguridad y deber de secreto - AP/00028/2015

Se denuncia a la Tesorería General de la Seguridad Social (TGSS) porque navegando por internet, asociado al nombre del denunciante consta indexado que la TGSS ha publicado en el Tablón de Edictos y Anuncios de la Seguridad Social (TEASS) la reclamación de deuda por «derivación de responsabilidad a deudores no localizados», estando además a dicha fecha abonada la deuda. Se declara la infracción por la Secretaría de Estado de la Seguridad Social, respectivamente, al haber permitido, por un lado, indexación de los datos del denunciante por los motores de búsqueda y, por otro, el permanecer incorporados los datos del afectado transcurrido el plazo legal, de un año y 20 días.

- Cesión de datos por la DGT a empresas de Portugal - E/7396/2014, E/610/2015

Denuncias contra la Dirección General de Tráfico (DGT) al haber facilitado los datos personales de los destinatarios de multas recibidas por ciudadanos españoles por el impago de las tasas por la circulación por las autovías portuguesas.

Se archivan al no acreditarse que los datos personales de los sancionados fueran facilitados por la DGT de su fichero de vehículos, que es público, ni que se hayan realizado por el momento tratamientos por empresas españolas.

- Agencia Tributaria de las Islas Baleares. Quiebra en las Medidas de Seguridad - AP/00058/2014

Denuncia a la Agencia Tributaria de las Islas Baleares (ATIB) por notificar un expediente de apremio en cuyo anverso y en el exterior consta visible la indicación «embargo de salario», además de los

datos identificativos del apremiado. Se declara la infracción al artículo 9 de la LOPD al no haber implementado la ATIB las medidas de seguridad que evitasen el tratamiento de los detalles de la deuda.

- IVIMA. Tratamiento de datos en internet - AP/00030/2014

Denuncian la divulgación en la web del IVIMA de un procedimiento de enajenación de viviendas públicas de la Comunidad de Madrid que en el pliego de contratación y sus anexos contenía la relación de procedimientos litigiosos de 41 viviendas con información del nombre y apellidos del arrendatario y la dirección de la vivienda y la condición de deudor del arrendamiento social. Se declara la infracción al artículo 6 LOPD, puesto que el tratamiento no era pertinente para el fin pretendido, que se alcanzaba igual sin incluir los datos identificativos de los arrendatarios deudores y de sus domicilios.

- Consejería de Educación, Cultura y Deporte de la Junta de Andalucía. Tablón de anuncios con datos personales - E/4885/2005

Denuncia a la Consejería por haberse publicado en la sala de Profesores del I.E.S Virgen del Carmen un «Estadillo Mensual de Ausencias de Personal» con el nombre y apellidos, DNI, número de ausencias y causa codificada. Se archiva por la previsión legal de la existencia de un tablón de anuncios, la delimitación de la información al ámbito interno del Instituto, la codificación de la causa origen de la ausencia y la proporcionalidad del medio empleado para la fluidez de las relaciones entre el trabajador y el empresario.

Por otro lado, hay que destacar que, en el ámbito local, respecto al tratamiento y la publicación de las Actas de los Plenos en los Ayuntamientos, se consolida la doctrina de que, dado que los Plenos, en principio, son públicos, pueden ser objeto de

MEMORIA 2015

publicación, si bien en forma resumida, preservándose aquellos aspectos que afecten a la intimidad y privacidad del afectado.

- Ayuntamientos de Madrid y Sevilla. Falta de información y cesión de datos sin consentimiento - E/3652/2015 - E/7336/2014

Sendas denuncias a ambos ayuntamientos y a otras entidades, dado que al estacionar se exige al usuario un tratamiento de dato personal, número de matrícula del vehículo, que se ha de teclear en el parquímetro y se producen cesiones sin recabar el consentimiento entre el Ayuntamiento y las entidades implicadas en el cobro de las sanciones. Se archivan, considerando que en el documento emitido por el parquímetro no se tratan datos personales ni en el ticket y tampoco el boletín de denuncia (que no es obligatorio).

En el caso de infracción, el boletín de denuncia se da traslado al Ayuntamiento como responsable de la tramitación de los procedimientos «sancionadores» por las infracciones de movilidad y, en esta fase, se procede a la identificación del titular del vehículo. En la notificación de denuncia e incoación de expediente sancionador remitida al titular del vehículo, constan los datos del vehículo, la infracción de la Ordenanza y el procedimiento para realizar el pago; en el reverso se detallan los aspectos correspondientes al derecho de información del artículo 5 de la LOPD.

- El Ayuntamiento de Murcia exige la exhibición del carnet del taxista con su DNI fotografía. Deber de Secreto - AP/00010/2015

Denuncia al Ayuntamiento de Murcia al exigir a los taxistas que exhiban en el parabrisas de los vehículos el carnet con, además de los datos de filiación, el DNI y fotografía. Se declara la infracción

del Ayuntamiento por incumplimiento del deber de secreto del artículo 10 de la LOPD.

- Ayuntamiento de Alcalá de Guadaira. Deber de secreto - AP/00045/2014

Denuncia al Ayuntamiento de Alcalá de Guadaira por publicar en el Boletín Oficial de Sevilla una notificación por comparecencia que afecta a 6.677 contribuyentes y que es accesible en internet. Se declara la infracción pues, realizado un muestreo de 22 expedientes de contribuyentes incluidos en la notificación publicada, se constató que en cinco casos se había practicado la notificación personal a los interesados, por lo que no procedía su inclusión en la notificación por comparecencia publicada.

Asimismo, es de destacar la iniciación, en septiembre de 2015, de actuaciones previas de investigación (E/05706/2015) en relación con las noticias publicadas en prensa sobre la existencia de una quiebra de seguridad en los servicios tributarios que el Ayuntamiento de Sevilla ofrece a los ciudadanos a través de internet. Dichas actuaciones han continuado más allá del periodo recogido en esta Memoria.

■ PROCEDIMIENTOS DE TUTELA DE DERECHOS

En 2015 se han resuelto 2.113 reclamaciones de tutela de derechos, que como se señaló anteriormente, ha supuesto un incremento de un 16,23% respecto de 2014. Otro año más hay que resaltar que las reclamaciones del derecho de cancelación son las más numerosas, destacando, por su número, las reclamaciones planteadas frente a ficheros de solvencia patrimonial.

Como hecho más relevante del año 2015 hay que resaltar la aplicación, por parte de la Audiencia Nacional de la Sentencia del Tribunal de Justicia de la

Unión europea de 13 de mayo de 2014 (Google vs. Agencia Española de Protección de Datos). A partir de diciembre de 2014 y durante 2015 la Audiencia Nacional ha resuelto multitud de las demandas planteadas; entendiendo que cuando colisionan dos derechos fundamentales, para determinar cuál de ellos debe prevalecer, es necesario realizar una ponderación de intereses y así poder estimar o desestimar las pretensiones de los afectados.

Entre los criterios a tener en cuenta se debe señalar, sobre todo, el tiempo transcurrido desde la publicación de las informaciones, así como si el afectado es una persona de relevancia pública, lo que pudiera determinar una especial relevancia del interés público de dicha información y justificar un interés preponderante del público en tener acceso a la misma en el marco de una búsqueda por el nombre del interesado.

Desde la STJUE antes citada hasta el 31 de diciembre de 2015, se han dictado 371 resoluciones de tutelas de derechos, de las que 157 han sido estimatorias y 82 desestimatorias. Asimismo, se han inadmitido 131 reclamaciones, fundamentalmente por no haber ejercitado adecuadamente el derecho y en un caso el reclamante ha desistido.

Con ello, la Audiencia Nacional ha venido con carácter general a confirmar los criterios que ya utilizaba esta Agencia para resolver las reclamaciones sobre esta materia.

A esta doctrina de la Audiencia hay que añadir la Sentencia del Tribunal Supremo de la Sala de lo Civil de fecha 15 de octubre de 2015 sobre la obligación por parte de los editores de que adopten medidas para evitar la indexación de noticias por parte de los buscadores cuando las noticias sean ya obsoletas y haya sido solicitado por los afectados.

Por otra parte, se observa un mayor número de reclamaciones referidas a historiales clínicos, tanto si se ejerce el derecho de acceso como los derechos de rectificación y cancelación.

Dentro de los procedimientos de tutela de derechos más destacados de 2015 se pueden señalar los siguientes:

- Derecho de cancelación frente a Google. Accesibilidad de la información a cualquier internauta no justificada – TD/1955/2014

Reclamación de tutela frente a Google para la cancelación de los datos del reclamante que aparecen publicados en varias direcciones web. De conformidad con lo establecido por el TJUE en su sentencia de 13 de mayo de 2014, la actividad del motor de búsqueda en internet constituye un tratamiento de datos del que es responsable el propio motor de búsqueda y al que resulta de aplicación la normativa nacional de protección de datos. Por ello, debe valorar y, en su caso, atender el ejercicio del derecho de cancelación cuando, como en esta ocasión, la información de una persona física es accesible a cualquier internauta que realice una búsqueda a partir de su nombre. La información a la que se refiere la tutela -comentarios publicados en un blog hace más de 10 años donde se dice que el reclamante, al que llaman ladrón, ha estafado en la venta de teléfonos- es considerada relevante y de interés público por Google. No se valora la publicación inicial de la información, sino su accesibilidad a través del buscador, que resulta inadecuada y no pertinente, al no prevalecer el interés del público en acceder a dicha información, debiendo rechazarse cualquier justificación amparada en la libertad de expresión dado el tiempo transcurrido. Se estima la tutela y se insta a Google a adoptar medidas para que el nombre del reclamante se desvincule en los resultados de búsquedas.

MEMORIA 2015

■ Derecho de cancelación frente a Google. Información de interés público - TD/1671/2014

Reclamación de tutela del derecho de cancelación frente a Google para la desindexación de un enlace al buscar por el nombre del afectado que lleva a una noticia, publicada recientemente, que informa de que el reclamante había adulterado recetas, por lo que fue condenado por falsedad en documento oficial y estafa. Google rechazó la cancelación al considerar que la información es de interés público. La información que se ofrece en la noticia es de interés para los ciudadanos y no resulta obsoleta, sin que se haya demostrado que sea inveraz, por lo que desestima.

■ Acceso a documentación no amparado por la LOPD - TD/00434/2015

Tutela del derecho de acceso frente a una empresa eléctrica, a quien el reclamante ha pedido copia de las facturas emitidas y manifiesta que no ha recibido copia del contrato solicitado. El ámbito del derecho de acceso regulado en la LOPD no alcanza a documentos concretos, como pueden ser las facturas por suministros o servicios. Además, la AEPD no es competente para resolver cuestiones civiles relativas a la validez de contratos, que habrán de plantearse ante los órganos administrativos o judiciales competentes. Se inadmitió la reclamación.

■ Ejercicio del derecho al olvido no solo frente a Google.es sino frente a Google.com – TD/00921/2015

En relación con las reclamaciones de tutela de derechos que han instado la adopción de medidas para evitar que los nombres de los afectados se vincularan a las direcciones web indicadas en la versión del buscador google.com, o de otros países no miembros de la UE, Google manifiesta que limita el bloqueo a las páginas de los dominios de

la UE. Alega que la eliminación de resultados de las versiones no europeas de su buscador constituiría una restricción absoluta y universal a la libertad de expresión e información de los editores y usuarios de internet, no necesaria para la protección del derecho al olvido. Asimismo añade que las versiones nacionales del motor de búsqueda son las que suelen utilizar los usuarios pues disponen de un mecanismo de redirección automática a dichas versiones.

Para el Grupo de Autoridades de Protección de Datos de la UE, el derecho debería ser efectivo en todos los dominios relevantes. Se ha constatado que, sin recurrir a medios desproporcionados, resulta posible realizar búsquedas en google.com por el nombre de los reclamantes que ofrecen como resultado enlaces a algunas de las direcciones web objeto de las reclamaciones evitando, mediante procedimientos sencillos, el sistema de redirección automático. Además, se ha comprobado que es sencillo para usuarios españoles acceder a versiones del buscador correspondientes a países fuera de la UE.

Relacionado con ello, y teniendo en cuenta ese marco, se planteó la reclamación detallada en el encabezamiento. En varios enlaces aparecen los datos del interesado publicados en medios de comunicación así como en el Boletín Oficial de la Junta de Andalucía, en referencia a la decisión del Servicio Andaluz de Salud de Cádiz de suspender de empleo y sueldo al interesado, médico de profesión, por agredir a uno de sus pacientes.

En este caso y sin esfuerzos desproporcionados es posible acceder a los enlaces reclamados en una búsqueda en google.com realizada desde España, dado que el sistema de redireccionamiento ofrecido por el buscador no impide que los usuarios, mediante procedimientos sencillos, puedan evadir

lo y acceder directamente a otros dominios usando equipos situados en territorio español.

Consecuentemente con todo lo expresado con anterioridad, procede el bloqueo de las URLs que aparecen en los resultados de búsqueda ofrecidos por el buscador al realizar una consulta desde España a partir de su nombre en google.com.

- Cancelación de datos en historia clínica - TD/00323/2015

Reclamación frente a la Dirección Provincial del Instituto Nacional de la Seguridad Social en Las Palmas para que proceda a eliminar determinados antecedentes personales que constan en la anamnesis del reclamante. Con ese término se designa la información que proporcionan los pacientes al profesional sanitario para incorporarla a la historia clínica, y comprende datos subjetivos relativos al paciente, antecedentes familiares y personales, y signos y síntomas de la enfermedad, que se usan para analizar la situación clínica. Los datos de la historia clínica, en la medida en que se relacionen con la salud de la persona y su consulta sea adecuada para preservar su salud, deben conservarse durante el tiempo adecuado en cada caso según criterio médico, no pudiendo cancelarse si se perjudicase la salud futura del paciente. Ello sin olvidar que pueden darse otros intereses legítimos de terceros, así como otras obligaciones derivadas del resto de usos previstos en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. Se desestima la tutela.

- Acceso a historia clínica. Entrega rechazada por el interesado - TD/00322/2015

Se solicita la tutela de la Agencia frente a la Asociación de Salud Mental para el acceso a toda la

documentación oficial, personal y médica del reclamante. La asociación hizo entrega de la documentación, que no fue aceptada al considerarse incompleta por el reclamante. El derecho de acceso previsto en la LOPD no ampara el acceso a documentos concretos, que pueden contener información de terceras personas. Conforme a la Ley 41/2002, de 14 de noviembre, se tiene derecho a obtener copia de la documentación clínica del reclamante que obre en poder de la asociación. En el presente caso, la asociación entregó la documentación, pero fue rechazada, por lo que se entiende que se ha renunciado a la materialización del derecho de acceso. Debería haberse aceptado la documentación, pudiendo hacer constar en el recibí su disconformidad, y si se considera incompleta, instar la tutela de la Agencia. Se inadmite la reclamación.

C - LA SEGURIDAD JURÍDICA COMO OBJETIVO PRIMORDIAL

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

De este modo en 2015 fueron informadas 146 disposiciones de carácter general, lo que supone un ligero descenso del 7% respecto de las que fueron informadas en el ejercicio anterior, pese a representar la segunda cifra anual más elevada de la serie histórica. El descenso se produjo como consecuencia de la disminución del número de Proyectos sometidos al parecer de la Agencia a lo largo del último trimestre del año, probablemente como consecuencia de la celebración de elecciones generales al término del mismo.

MEMORIA 2015

De entre las disposiciones sometidas al parecer de la Agencia cabe hacer referencia a las siguientes:

- Anteproyecto de Ley del Procedimiento Administrativo Común de las Administraciones Públicas.
- Anteproyecto de Ley de Régimen Jurídico del Sector Público.
- Anteproyecto de Ley sobre reutilización de información del sector público.
- Anteproyecto de Ley de Resolución Alternativa de Conflictos de Consumo.
- Proyecto de Real Decreto Legislativo por el que se aprueba el Texto Refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios.
- Proyecto de Real Decreto por el que se aprueba el Reglamento de Ordenación, Supervisión y Solvencia de las Entidades Aseguradoras y Reaseguradoras.
- Proyecto de Real Decreto por el que se regula el Registro Central de Delincuentes Sexuales.
- Proyecto de Real Decreto por el que se aprueba el Reglamento por el que se desarrolla la ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado.
- Proyecto de Real Decreto por el que se modifican distintas disposiciones en el sector eléctrico.
- Proyecto de Real Decreto sobre comunicaciones telemáticas en la Administración de Justicia.
- Proyecto de Real Decreto por el que se aprueba el reglamento sobre la adquisición de la nacionalidad española por residencia.
- Proyecto de Real Decreto por el que se modifica el Reglamento del Dominio Público Hidráulico aprobado por el Real Decreto 849/1986, de 11 de abril, en materia de gestión de riesgos de inundación, caudales ecológicos, reservas hidrológicas y vertidos de aguas residuales.
- Proyecto de Real Decreto por el que se regulan los registros públicos de profesionales de los Consejos generales de los Colegios oficiales de las profesiones.
- Proyecto de Real Decreto por el que se aprueba el Reglamento del Registro Estatal de prestadores de servicios de comunicación audiovisual.
- Proyecto de Real Decreto por el que se modifica el RD 843/2011, de 17 de junio, por el que se establecen los criterios básicos sobre la organización de recursos para desarrollar la actividad sanitaria de los servicios de prevención.
- Proyecto de Real Decreto por el que se regula la realización de los controles sanitarios sobre determinados productos de uso o consumo humano procedentes de terceros países y se establecen las condiciones de autorización de los puntos de control sanitario y de los almacenes de inmovilización de mercancías.
- Proyecto de Real Decreto por el que se crea y regula el Registro Estatal de Enfermedades Raras.
- Proyecto de Real Decreto por el que se fijan las bases para la implantación de las Unidades de Gestión Clínica en el ámbito de los Servicios de Salud.
- Proyecto de Real Decreto por el que se regula el procedimiento de autorización para la realización de promoción y publicidad de la donación de células y tejidos humanos.

- Proyecto de Real Decreto por el que se establecen las bases generales sobre autorización de centros, servicios y establecimientos sanitarios y se determinan los requisitos mínimos comunes para su autorización.
- Proyecto de Real Decreto por el que se regula la financiación y fijación de precios de medicamentos y productos sanitarios y su inclusión en la prestación farmacéutica del Sistema Nacional de Salud.
- Proyecto de Orden por la que se regula el tablón de anuncios de la Seguridad Social.
- Proyecto de Orden por la que se desarrolla el Real Decreto 640/2014, de 25 de julio, por el que se regula el Registro Estatal de Profesionales Sanitarios.
- Proyecto de Orden Ministerial reguladora del Órgano Centralizado de Prevención del Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles.
- Proyecto de Orden reguladora de la declaración de movimientos de medios de pago en el ámbito de la prevención del blanqueo de capitales y de la financiación del terrorismo.
- Proyecto de Orden ministerial por la que se establecen los requisitos y condiciones para la suscripción de convenios de habilitación para la presentación electrónica de solicitudes de nacionalidad española por residencia en representación de los interesados.
- Proyecto de Orden por la que se establece y las normas reguladoras de las Hojas de Servicios del personal de la Guardia Civil.
- Proyecto de Orden del Ministerio de Agricultura por la que se regula la estructura informática del registro de aguas y la base central del agua.

MEMORIA 2015

- Proyecto de orden por el que se establecen los requisitos técnicos y condiciones mínimas de la hemodonación y de los centros y servicios de transfusión.
- Proyecto de Orden por la que se crea la Comisión calificadora de documentos administrativos y de Coordinación de archivos del Ministerio de Justicia y de sus órganos públicos.
- Instrucción de 15 de septiembre de 2014, del Defensor del Pueblo, por la que se regulan los ficheros de datos de carácter personal de la Institución del Defensor del Pueblo.
- Proyecto de Instrucción de la Secretaría de Estado de Economía y Apoyo a la Empresa, por la que se establecen los requisitos mínimos que deben cumplir las solicitudes de datos del Fichero de Titularidades Financieras, efectuadas a través de los puntos únicos de acceso.

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 2015 se han dictado por la Sala de lo contencioso-administrativo de la Audiencia Nacional 201 sentencias, de las cuales:

- 146 fueron desestimatorias de los recursos formulados contra resoluciones de la Agencia (que quedaron plenamente confirmadas) (73%).
- 19 estimaron parcialmente los recursos (10%).
- 29 estimaron íntegramente las pretensiones anulatorias de las resoluciones de la Agencia (14%).
- 7 inadmitieron los recursos interpuestos contra resoluciones de la Agencia (3%).

MEMORIA 2015

Debe en particular tenerse en cuenta que durante el año 2015 se han dictado un total de 45 sentencias en recursos interpuestos por Google contra resoluciones de la Agencia que estimaban la solicitud de cancelación u oposición planteada por el interesado y que se veían afectados por lo señalado en la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014. De ellas 37 han sido desestimatorias (un 82%), 5 estimatorias (un 11%) y en tres ocasiones (un 7%) se ha estimado parcialmente el recurso interpuesto, ordenándose la supresión del enlace en el motor de búsqueda pero no la supresión de la información, que se encontraba alojada en los tres casos en la plataforma de blogs gestionada por la propia Google.

A la vista de las cifras generales que se han mencionado, cabe concluir que la confirmación de los criterios de la Agencia en cuanto al fondo del asunto ha sido de un 76%, resultando así ser el mismo que el producido en el año 2014. No obstante, debe destacarse que en este porcentaje total tienen más peso las sentencias en que se produce la desestimación del recurso (un 73% del total frente a un 70% en 2014), lo que supone que es mayor la incidencia de las sentencias que confirman las resoluciones de la Agencia previa valoración jurídica de los criterios de fondo que la fundan, reduciéndose el peso de las sentencias que confirman la resolución al no proceder la tramitación del recurso. El porcentaje de sentencias estimatorias en 2015 es el más elevado desde el año 2007.

Por otra parte, se observa un notable descenso de la litigiosidad referida a la actuación de la Agencia, por cuanto el número total de sentencias se reduce en casi un 15%, siendo el descenso acumulado de la litigiosidad si se compara con las cifras de 2013 de más de un 26.5%.

En relación con los sectores de actividad a los que afectan las sentencias dictadas el sector que pre-

senta una mayor litigiosidad sigue siendo el de las telecomunicaciones, con un 27% del total, reduciéndose su cantidad en un 12% respecto de 2014. Igualmente se mantiene el volumen significativo de sentencias relacionadas con prestadores de servicios de la sociedad de la información (que se incrementan en 21%, siendo el aumento de su relevancia en relación con el total de sentencias de casi 7 puntos porcentuales hasta un total del 23%); no obstante, es preciso recordar que la práctica totalidad de estas sentencias se refieren a los recursos interpuestos por Google y relacionados con la Sentencia del Tribunal de Justicia de la UE de 13 de mayo de 2014.

Asimismo, cabe hacer referencia a los recursos interpuestos por los particulares, bien contra resoluciones de archivo de actuaciones, bien contra resoluciones desestimatorias en procedimientos de tutela de derechos, que se incrementan en un 26% hasta alcanzar el 17% del total. Igualmente son relevantes los incrementos producidos en el sector de la distribución y venta (un 33%) y los sindicatos y asociaciones empresariales (un 40%), pese a su menor volumen en relación con el total.

Se produce un muy importante descenso de las sentencias relacionadas con el sector financiero, que disminuyen en términos absolutos en un 47%, pasando el porcentaje de las mismas en relación con el total de casi el 14% a casi el 9%. Es igualmente significativo el descenso en el sector energético (un 26%).

Finalmente, y aun cuando su peso total es menor, se producen igualmente descensos muy significativos en los sectores de asesoría y consultoría (un 69%) y solvencia patrimonial (un 75%). No obstante, respecto del primero de los sectores, cabe recordar, como se indicaba en la memoria correspondiente a 2014 que el incremento producido

en aquel año se debía a la existencia de un gran número de sentencias relacionadas con una sola empresa y vinculadas a un tratamiento muy específico; descontado este efecto, las cifras de 2015 del sector de la asesoría y consultoría son ligeramente más elevadas que las del 2014.

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 materias analizadas por la Audiencia Nacional destacan las siguientes cuestiones:

- En relación con la aplicabilidad de la LOPD, la AN ha considerado que está sujeto a la misma el tratamiento de los 20 dígitos que componen una cuenta bancaria, dado que tienen la naturaleza de dato de carácter personal, que permite sin esfuerzos desproporcionados identificar a su titular (SSAN de 15/1/15 y 3/11/15). Por otra parte, ha considerado aplicable la excepción de la aplicación de la LOPD en relación con el tratamiento de datos de empresarios individuales cuando los datos de nombre, apellidos y DNI de uno de ellos habían sido incluidos en ficheros de solvencia patrimonial y crédito vinculados a deudas de su establecimiento (SAN de 28/4/15). También la AN ha considerado que no es aplicable la LOPD en los supuestos en que se solicita la rectificación de una información contenida en un fax, no pudiendo considerarse en este caso la existencia de un tratamiento (SAN 31/3/15).

Asimismo, ha considerado necesario diferenciar los tratamientos de datos de las aplicaciones o plataformas que dan soporte a los mismos, siendo posible el ejercicio de los derechos respecto de los primeros pero no respecto de esas plataformas.

- En relación con el cumplimiento del deber de información, la SAN de 13/11/15 ha señalado, en un supuesto de cesión de créditos, que la carga de la prueba de su cumplimiento corresponde al cedente, no al deudor, no bastando la mera invocación de que la carta no ha sido devuelta. Por su parte, la SAN de 8/5/15 confirma la sanción impuesta por la AEPD a la titular de una página web que no incluía cláusula de protección de datos en sus formularios.
- La AN se ha referido en distintas sentencias a la aplicación de la regla de equilibrio de derechos e intereses establecida en el artículo 7 f) de la Directiva 94/46/CE. Como punto de partida, la SAN de 13/5/15 ha indicado que la mera invocación de un interés económico y de que los datos eran accesibles a través de Internet no resulta suficiente para legitimar el tratamiento. Por su parte, las SSAN de 11/9/15 y SAN de 30/12/15 han considerado aplicable el artículo 7 f) en los supuestos de videovigilancia si se cumplen los restantes requisitos legalmente exigibles.
- En varios supuestos la aplicación del artículo 7 f) se ha relacionado con la ponderación de diversos derechos fundamentales. Así, además de las sentencias dictadas como consecuencia de la sentencia del TJUE de 13 de mayo de 2013, la AN ha considerado prevalente el tratamiento en garantía de la libertad de información en las SSAN de 24/2/15, 12/3/15 y 14/7/15. Igualmente, ha considerado prevalente la libertad de expresión en los casos de inclusión en una web por

el editor de informaciones relativas a sentencias judiciales que habían sido publicadas en medios de comunicación (SAN de 27/2/15), aunque no en caso de que no hubiera existido esa previa divulgación por los medios (SAN de 31/3/15). Asimismo, la SAN de 3/3/15 ha considerado prevalente la libertad sindical en el caso de remisión en el entorno laboral de una sentencia judicial relacionada con la existencia de acoso a un trabajador. Finalmente, ha considerado que prevalece el derecho a la participación política en el supuesto de divulgación en un pleno municipal de la identidad de quien había presentado una queja contra el Ayuntamiento ante el Defensor del Pueblo al contestar una pregunta de la oposición sobre esa misma cuestión (SAN de 27/10/15)

■ En cuanto a otros supuestos de legitimación para el tratamiento, la SAN de 16/7/15 considera amparada en la Ley la inclusión en la convocatoria de una Junta de comunidad de propietarios de los datos de propietarios morosos. Por su parte, se ha apreciado falta de legitimación en los supuestos de contratación o mantenimiento de un contrato después de que los afectados solicitasen expresamente su resolución (SSAN de 15/1/15 y 3/2/15), o cuando se han utilizado los datos del afectado para la celebración de un contrato no solicitado sobre la base de que existía consentimiento para la remisión de comunicaciones relacionadas con ese tipo de productos (SAN de 10/11/15). También se considera contraria a la LOPD la emisión por una entidad bancaria de una tarjeta de crédito a un cliente que expresamente había manifestado su negativa a contratarla (SAN 29/9/15) o la inclusión en guías telefónicas de los datos de un abonado que había manifestado expresamente su negativa a la inclusión, habiéndose produ-

cido una portabilidad a otra compañía (SAN de 31/3/15). Finalmente, la SAN de 27/3/15 ratifica la sanción a un partido político por el envío de comunicaciones a antiguo afiliado que había solicitado la cancelación de sus datos.

■ Como en otros ejercicios son muy numerosas las sentencias relacionadas con el tratamiento de datos personales asociados con la contratación de servicios por un tercero utilizando los datos de los denunciantes. En este sentido, la AN ha señalado que existe responsabilidad de la empresa prestadora del servicio aun cuando se hubieran facilitado los datos por una encargada del tratamiento encargada de la captación de clientes en caso de que no haya concurrido en la responsable la debida diligencia en el control de la actuación del distribuidor, sin perjuicio de la responsabilidad de éste (SSAN de 17/2/15 y SAN 10/9/15). No obstante, no cabría sancionar al responsable por un mero error humano exclusivamente imputable al distribuidor (SAN de 25/2/15) o cuando el encargado se ha extralimitado absolutamente de lo contratado con el responsable (SAN de 28/4/15 en que se facilitaron por el responsable los datos de los destinatarios de una campaña y el encargado los amplió incluyendo personas dadas de alta en ficheros de exclusión publicitaria o SAN de 3/7/15 en que se incluyó por el encargado a una persona que había ejercitado su derecho a no recibir publicidad de ese responsable).

■ Por otra parte, la AN ha considerado que existen indicios de la celebración del contrato en los supuestos de aportación de una grabación de verificación de la contratación del servicio mínimamente audible (SSAN de 10/4/15 y 10/3/15), uso del servicio durante seis meses incluso después de haber solicitado la baja en el mismo alegando no haberlo contratado

(SAN 12/5/15), abono del servicio durante más de un año (SAN 27/5/15), aportación de un contrato firmado por el denunciante respecto del que éste alega la existencia de un engaño que no ha quedado acreditado (SSAN de 17/4/15 y 23/4/15) o apreciación de indicios razonables de identidad de la firma de un contrato con la del denunciante, incluso aunque no conste en la documentación el DNI (SAN de 11/11/15), aunque las similitudes no sean totalmente conciliadoras (SAN de 8/5/15).

■ Por el contrario, la AN ha considerado que no existen indicios suficientes en la celebración del contrato cuando no se aporta acreditación alguna de su celebración (SSAN de 17/4/15, 5/6/15 y 11/6/15), limitándose el prestador a invocar la relación de confianza entre él y el denunciante (SAN de 28/4/15) o no se aporta copia del DNI (SSAN de 28/4/15, 14/5/2015 y 22/9/15) ni se obtiene, en caso de contratación electrónica, en el momento de la entrega del equipamiento (SAN de 14/5/15), cuando las firmas del contrato son distintas a las del DNI (SSAN de 18/6/15 y 13/10/15) o a las de otros contratos celebrados por el denunciante con el mismo prestador (SAN de 9/6/15), cuando en el ámbito de la contratación telefónica no se aporta grabación (SAN de 29/5/15) o ésta ni siquiera se identifica al afectado con su nombre sino con otro distinto (SAN 30/4/15) o sólo consta en ella el dato de un DNI que no es el del denunciante, pero no su nombre y apellidos (SSAN de 2/7/2015 y 14/10/15); y cuando en contratación electrónica no se aporta más acreditación que la mera constancia del afectado en un «histórico» de la propia compañía (SAN 17/3/15). Tampoco existen indicios de celebración del contrato cuando consta un DNI distinto al del denunciante al que se dio de alta y se giraron las

MEMORIA 2015

facturas (SSAN de 17/2/15 y 10/9/15) o cuando la instalación del equipamiento contratado se hizo en un domicilio distinto al del denunciante (SSAN 20/3/15 y 12/5/15).

- En cuanto al derecho de acceso, existen dos sentencias relacionadas con el acceso a datos de salud: por una parte, la SAN de 14/5/15 reconoce el derecho del titular de la patria potestad a obtener la totalidad de la documentación de la historia clínica de su hijo menor de edad y por otra la SAN de 10/2/15 reconoce el derecho de acceso a los informes emitidos por un perito médico de una mutualidad a efectos de determinar si existe o no incapacidad, aunque cuando los mismos no formen estrictamente parte de la historia clínica.
- La AN ha reconocido la procedencia del derecho de cancelación respecto de la publicación en una web de sentencias sin anonimizar (SAN de 31/3/15), considerando que no procede, entre otros casos, respecto de antecedentes policiales, dada la gravedad de los hechos (detención por apología del terrorismo al subir a internet videos de contenido yihadista, habiendo el afectado sido absuelto por enajenación mental, SAN de 20/3/15) o cuando un empleado público solicita la cancelación de los datos de la firma electrónica que le es facilitada por la Administración, al ser consustancial el uso de la firma a la relación del empleado con la Administración empleadora (SAN de 2/10/15)
- En relación con los supuestos de ejercicio del derecho de oposición a la aparición de información en internet, la AN ha considerado que el mismo no procede respecto de los buscadores internos de los medios de comunicación, que tampoco están obligados a eliminar los datos personales del afectado de la noticia indexada

por esos buscadores y respecto de la que sí se ha estimado su pretensión contra buscadores generalistas (SSAN 24/2/15 y 12/3/15). No obstante, el derecho sí puede ejercitarse en el sentido de solicitar la adopción de medidas que impidan la indexación de los datos publicados en diarios oficiales si se cumple lo señalado por la STJUE de 13 de mayo de 2014 (SAN 14/3/15) e incluso, en un supuesto, la adopción de estas medidas por un medio de comunicación (SAN de 2/10/15, que tiene en cuenta que la noticia tiene una antigüedad de más de quince años, la existencia de errores en la información facilitada – al hablar de «condena» de la CNMV por la comisión de un «delito»- y la falta de relevancia pública del afectado).

■ En materia de seguridad, la AN ha apreciado falta de diligencia del responsable que permite el acceso a través de su web a la totalidad del Registro de Vehículos, pudiendo identificarse a los titulares a partir de matrícula o número de bastidor (SAN de 28/1/15), confirmando también la sanción en caso de accesibilidad en una oficina virtual a los datos de persona distinta del usuario que accede a la página (SSAN 17/3/15 y 24/3/15 Gas Natural). También se ha apreciado vulneración del deber de seguridad en un supuesto en que se hizo accesible por internet a la lista de afiliados de un partido político (SAN de 25/6/15).

■ En cuanto al cumplimiento del deber de secreto, la AN lo considera vulnerado en caso de envío de un correo electrónico de contenido político en que aparecen visibles todos sus destinatarios (SAN 13/5/15) o en el envío a cada uno de los cónyuges, junto con información de su plan de pensiones, de información del que había sido suscrito por el otro, aun cuando cada uno era beneficiario en el plan en que el otro es

tomador (SAN 30/6/15). Por el contrario no se ha vulnerado este deber cuando en un informe elaborado en el seno de un procedimiento en materia de personal se incluyeron datos relacionados con la salud del interesado que eran relevantes a los efectos de resolver el fondo (SAN 15/1/15).

■ En relación con los ficheros de solvencia patrimonial la AN ha considerado que existe una infracción del artículo 6 de la LOPD en los supuestos de consulta del fichero en relación con una persona con la que no se tiene ninguna relación de negocio (SSAN de 21/7/15 y 9/7/15).

■ En relación con los requisitos de la deuda, la AN ha continuado señalando que no concurrirían éstos en caso de que el deudor hubiera interpuesto una reclamación ante una Junta Arbitral de Consumo SSAN de 22/2/15, 22/9/15 y dos de 3/11/15 o las SSAN de 17/9/15 y 24/9/15, en que la conservación es incluso posterior a la existencia de un laudo estimatorio; así como los supuesto de reclamación, en el ámbito de telecomunicaciones, ante la SETSI (SSAN 15/1/15, 2/7/15 y SAN 7/10/15): igualmente ha considerado la improcedencia de incluir datos de un avalista respecto del que existe un auto que le excluye de la ejecución por extinción del crédito (SAN de 16/4/15) o cuando el propio acreedor conoce de la existencia de un fraude en la contratación, pero el dato se mantiene en el fichero de solvencia aun después de conocerse esta circunstancia (SSAN de 23/3/15, 10/4/15 y 12/5/15).

■ En cuanto al requerimiento de pago como requisito previo a la inclusión, la SAN de 12/6/15 señala que en caso de vencimiento periódico no sería necesario un nuevo requerimiento en cada incumplimiento, sino sólo en el primero (aun-

que se refiere a un supuesto en que había habido más de veinte antes del que se denuncia por su inexistencia). En relación con la prueba, la AN ha considerado que sólo sería suficiente la acreditación de la no devolución por un operador postal y no por la empresa a la que el acreedor encargue la «puesta en correo» del requerimiento (SSAN de 17/3/15, 14/4/15 y 2/6/15).

■ En el ámbito de la videovigilancia es interesante lo señalado en las SSAN de 11/9/15 y 30/12/15, que ponen de manifiesto que el hecho de que las entidades bancarias estén obligadas a la instalación, a disposición únicamente de las Fuerzas y Cuerpos de Seguridad de estos sistemas, no les exime de su condición de responsable, aplicando los criterios de proporcionalidad en el sentido de considerar desproporcionada la grabación de la totalidad de la acera aledaña al local objeto de vigilancia en los dos casos que se han señalado. Por el contrario, la SAN de 29/5/15 considera que no es desproporcionada la grabación de la vía pública si ésta es parcial y además sólo se visualiza de forma borrosa, constando en autos un acta notarial que lo acredita.

■ En el ámbito de la publicidad, la SAN de 30/4/15 recuerda la responsabilidad del anunciante beneficiario de la publicidad que fija los parámetros identificativos de la muestra en caso de falta de consentimiento por la empresa a la que se encarga la campaña.

■ En relación con la LSSI, cabe hacer referencia a tres sentencias relacionadas con el envío de comunicaciones comerciales no solicitadas: la de 19/1/15, que confirma la sanción por envío a quien cinco años antes había manifestado su voluntad de no recibirlas; la de 28/4/15, en que se declara ilícito el envío de comunicaciones co-

merciales a una persona sobre la única base de que había invitado en redes sociales, de forma genérica, a que se pusieran en contacto con ella y la de 4/12/15, en que la comunicación se remite a una dirección de correo compartida por varias personas, bastando con que sólo una de ellas manifieste su negativa a la recepción de las comunicaciones para que la misma no pueda tener lugar. Además es especialmente reseñable que la SAN de 8/5/15 confirma la primera sanción que impuso la Agencia por la instalación de dispositivos de almacenamiento masivo en los terminales de los usuarios (en este caso cookies) sin haberse ofrecido al usuario información alguna y mucho menos recabado su consentimiento para la instalación.

■ Por lo que respecta a los criterios de atenuación derivados de lo dispuesto en el artículo 45.5 cabe hacer referencia a la apreciación por la AN de la existencia de una regularización por el responsable en supuestos en que la misma tuvo lugar a la mayor celeridad (SAN de 14/6/15, o 24 horas después de detectada la vulneración SSAN de 30/4/15 y 2/6/15) o en el plazo de cuatro días (SAN 17/3/15). También se ha apreciado la aplicación de la atenuación por la existencia de precedentes en este sentido en resoluciones similares de la AEPD (SAN de 22/10/15), por falta de beneficios, falta de perjuicios al afectado, escasa entidad de la culpa y rápida reparación (SSAN de 24/2/15 y 2/7/15). O por la existencia de un hecho imputable al interesado (SAN de 23/6/15)-

■ Por último la AN se ha referido en dos supuestos a la falta de atención de los requerimientos de la AEPD derivados de una previa resolución de apercibimiento: en la SAN de 21/5/15 aprecia la existencia de infracción al no haberse corregido la conducta, limitándose el recurrente

a manifestar su oposición a la legalidad de la resolución de apercibimiento, aun siendo firme y en la SAN de 29/1/15 se considera no atendido el requerimiento cuando la respuesta tuvo lugar al tiempo de evacuar alegaciones en el expediente abierto por falta de atención de aquél.

Por su parte, el Tribunal Supremo, dictó un total de 8 resoluciones (5 sentencias y 4 autos) 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. Como ya se indicó en las Memorias correspondientes a los últimos ejercicios, el número de recursos ha sufrido una drástica reducción como consecuencia de la reforma operada en la Ley Jurisdiccional por la Ley 37/2011, de 10 de octubre.

En relación con estos recursos, el Tribunal Supremo:

- Declaró en tres sentencias no haber lugar a los recursos interpuestos contra sentencias que confirmaban las resoluciones de la Agencia, que quedaron así, a su vez, confirmadas.
- Acordó en cuatro supuestos la inadmisión del recurso.
- Declaró en dos sentencias haber lugar a los recursos interpuestos contra sentencias que confirmaban las resoluciones de la Agencia.

En consecuencia el Tribunal Supremo confirmó en los ocho asuntos que llegaron a su conocimiento el criterio que había mantenido la Agencia Española de Protección de Datos

■ SENTENCIAS TJUE

Durante 2015 ha sido particularmente relevante la doctrina jurisprudencial emanada del Tribunal de Justicia de la Unión Europea. De este modo, y ade-

más de la sentencia de 6 de octubre de 2015, dictada en el Asunto C362/14 (Schrems), de la que ya se ha dado debida noticia en esta Memoria, cabe hacer referencia a otras dos sentencias, ambas de 1 de octubre de 2015:

- La primera recayó en el asunto C-201/14 (Smaranda Bara y otros) y se refiere a un supuesto en que la Administración Tributaria rumana facilitó a la Administración de la Seguridad Social de dicho país los datos referidos a los ingresos derivados de las actividades de los interesados, planteándose la cuestión de si dicha cesión es lícita sin haberse informado a los afectados de que la misma iba a producirse y, en el caso del cesionario, del tratamiento que iba a hacerse de los datos. Es relevante tener en cuenta que la legislación rumana únicamente prevé expresamente la cesión entre estas dos administraciones de los datos necesarios para determinar la condición de asegurado del interesado y no datos de carácter económico.

El Tribunal, a la vista de la legislación rumana considera que debía haberse procedido a informar a los interesados con anterioridad a la transmisión por parte de la autoridad tributaria de que se iba a proceder a la cesión. Del mismo modo, la cesionaria debía haber informado a los interesados acerca de las finalidades para las que iba a tratar los datos y las categorías de datos objeto de tratamiento. No cabe oponer en este caso la excepción de que la transmisión está expresamente reconocida por una Ley ni cabe considerar aplicables las excepciones del artículo 13 de la Directiva 95/46/CE, al entender el Tribunal que las mismas deben encontrarse recogidas en una Ley que prevea salvaguardas adecuadas.

- La segunda, dictada en el asunto C230/14 (Weltimmo) analiza el ámbito de aplicación te-



G. Fessy ©TJUE

rritorial de las normas de protección de datos en relación con la prestación de servicios de la sociedad de la información. Se trataba de un portal inmobiliario propiedad de una empresa eslovaca dedicado a la venta de inmuebles situados en Hungría. La información se refería únicamente a inmuebles de ese país y aparecía únicamente en húngaro en la página web. La empresa tenía un representante en Hungría que se encargaba de la gestión de cobros a los propietarios anunciantes y representó a la entidad ante las autoridades húngaras de protección de datos.

La sentencia considera que en este supuesto es posible la aplicación del artículo 4.1 a) de la Directiva, al poderse considerar que el tratamiento se lleva a cabo en el contexto de las actividades de un establecimiento del responsable situado en Hungría. En este sentido, recuerda la doctrina derivada de la sentencia de 13 de mayo de 2014 (Asunto Google) para señalar que el concepto de establecimiento previsto en la Directiva debe interpretarse en un sentido no restrictivo, indicando que la actividad de la empresa de nacionalidad eslovaca consiste, como mínimo, en la gestión de uno o varios sitios de Internet de anuncios de inmuebles situados en

Hungría, que están redactados en húngaro y que pasan a ser de pago transcurrido el primer mes, concluyendo que «dicha sociedad ejerce una actividad real y efectiva en Hungría»; además se llega a esta conclusión sobre la base de la existencia de un representante en Hungría con las funciones que ya se han citado, entendiendo asimismo que el tratamiento se lleva a cabo en el contexto de las actividades reales y efectivas de la entidad en Hungría.

Por otra parte, se analiza en la sentencia si una autoridad de protección de datos puede imponer a una empresa que estuviera localizada en otro Estado Miembro las sanciones que prevea la Ley del país de esa autoridad. La respuesta del Tribunal es que las autoridades conocerán de todas las reclamaciones que se les planteen, incluso aunque se refirieran a responsables de otros Estados, pero no podrán imponer por sí mismas las medidas sancionadoras, sino únicamente recabar el auxilio de la autoridad de protección de datos del Estado en que se encontrase la responsable.

■ Transparencia y protección de datos personales

Como es sabido, el 9 de diciembre de 2014 entró en vigor la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la información pública y Buen gobierno (LTAIBG). A su vez, mediante Real Decreto 919/2014, de 31 de octubre, se aprobó el Estatuto del Consejo de Transparencia y Buen Gobierno.

El artículo 36.1 f) establece que integrará la Comisión de Transparencia y Buen Gobierno un representante de la Agencia Española de Protección de

Datos, habiendo sido designado en representación de la Agencia el Abogado del Estado-Jefe del Gabinete Jurídico.

La función de la Agencia en esta materia no se limita a la participación del miembro de la Comisión designado por aquélla en los trabajos de la misma, sino que además, de conformidad con lo establecido en la disposición adicional quinta, corresponderá de forma conjunta a la Agencia y al Consejo de Transparencia y Buen Gobierno la adopción conjunta de los criterios de aplicación de las reglas contenidas en el artículo 15 de la propia Ley, «en particular en lo que respecta a la ponderación del interés público en el acceso a la información y la garantía de los derechos de los interesados cuyos datos se contuviesen en la misma».

A lo largo de 2015 se han adoptado conjuntamente por la Agencia y el Consejo dos criterios de interpretación referidos a la determinación de los criterios para el acceso en el ámbito de la Administración General del Estado, a los datos relativos al importe de las retribuciones y del complemento de productividad de los empleados públicos. Asimismo, se ha adoptado un criterio relacionado con el modo en que deberá procederse a la aplicación sucesiva de los límites del derecho de acceso a la información pública establecidos, respectivamente, en los artículos 15 y 14 de la LTAIBG y a la publicación de la información referida a los firmantes de los Convenios de colaboración, objeto de publicidad conforme a lo dispuesto en el artículo 8.1 b) de la LTAIBG, en particular en lo que se refiere a la firma manuscrita de los intervinientes.

L A PROTECCIÓN DE LOS MENORES: UNA APUESTA ESTRATÉGICA PARA EL PRESENTE Y FUTURO DE LA PRIVACIDAD

La edad de acceso de los menores a internet ha venido experimentando un descenso con el paso de los años. La Comisión Europea, ya en su comunicación de 2012 sobre una «Estrategia europea a favor de una internet más segura para los niños», señalaba que en Europa la edad media de comienzo a navegar por internet es de 7 años.

Por otra parte, el uso de internet por los menores, es prácticamente universal a partir de determinadas edades. Según la encuesta del Instituto Nacional de Estadística sobre «Equipamiento y uso de tecnologías de información y comunicación en los hogares» de 2015, el 93,6% de los menores de 10 a 15 años usa internet. Otros estudios y encuestas también confirman ese grado de utilización (9 de cada 10 menores entre 6 y 14 años navegan ya por internet).

Internet ofrece, especialmente para los menores, todo un mundo de oportunidades para su desarrollo personal, familiar y social. Para aprovechar esas oportunidades es preciso generar los pilares que les permitan poder disfrutarlas en condiciones de igualdad y de seguridad, pues el mundo online no es ajeno a las situaciones que producen daños en las que los menores son tanto víctimas como autores.

Los estudios e informes realizados a este respecto muestran que estas situaciones son una realidad sobre la que los poderes públicos tenemos el compromiso de actuar para evitar que se produzcan. La Organización Mundial de la Salud, en un reciente informe que engloba a 42 países de Europa y de América del Norte, concluye que España es uno de los países en los que más situaciones de ciberacoso se producen entre los menores de 13 años. Otro reciente estudio de una Universidad española concluye que el 90% de los encuestados de 11 a 19 años conoce, padece o comete ciberacoso. Y

en estas situaciones, así como las de grooming o sexting, la utilización de información personal, de datos de carácter personal tanto propios como de terceros, por parte de los menores constituye una de sus características.

La importancia de promover la protección de los datos personales de los menores, especialmente en internet, ha determinado su incorporación al Plan Estratégico 2015-2019 como una de las líneas de actuación más relevantes para la Agencia.

La AEPR sitúa la información, la prevención y la concienciación como elementos esenciales para proteger de forma eficaz a los menores, un colectivo especialmente vulnerable que puede verse involucrado en situaciones de alto riesgo. Es por ello que la Agencia considera imprescindible ofrecer herramientas preventivas que permitan evitar riesgos a un colectivo en el que las nuevas tecnologías tienen especial incidencia.

En el año 2015 se han anticipado algunas actuaciones relevantes orientadas a fomentar la concienciación en materia de privacidad por parte de los menores, así como de sus padres y profesores. A continuación, se recogen las más relevantes:

■ Concurso Pandijuegos

El 13 de mayo se presentó el concurso escolar Pandijuegos, una iniciativa orientada a colegios para fomentar el conocimiento de la protección de datos y promover el valor de la privacidad entre los alumnos de 4.^º, 5.^º y 6.^º de Educación Primaria. Para llevarlo a cabo, se contó con la colaboración del Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF), del Ministerio de Educación, Cultura y Deporte, que lo alojó en su plataforma para ponerlo a disposición de todos los



profesores. El juego, diseñado para niños de entre 10 y 12 años, está compuesto de cinco minijuegos secuenciales y temáticos, e incluye un cuestionario final. Para completar la herramienta didáctica, se puso a disposición de los docentes una guía con los objetivos de cada minijuego, asociado a una ficha didáctica para que estos pudiesen profundizar en aquellos contenidos que consideraran más apropiados, obteniendo además propuestas de actividades para realizar en clase.

El colegio San José de Calasanz, de Barbastro (Huesca), resultó el ganador del concurso en el que participaron más de 130 colegios públicos, concertados y privados, registrando más de 28.000 partidas.

Una vez finalizado el concurso, el juego se ha mantenido activo en la página web [www.tudecidese-](http://www.tudecidese-ninternet.es)

ninternet.es para que los profesores interesados puedan seguir utilizándolo como un material de aprendizaje lúdico para sus alumnos.

■ Convenio con el Ministerio de Educación, Cultura y Deporte

El ministro de Educación, Cultura y Deporte, Íñigo Méndez de Vigo, y la directora de la Agencia Española de Protección de Datos firmaron un convenio el 13 de octubre que tiene por objeto establecer un marco estable de colaboración para realizar proyectos y acciones de carácter educativo en la formación y sensibilización de los menores de edad en materia de privacidad y protección de datos, sobre todo en el ámbito de internet y, en virtud del mismo, ambas partes acordaron realizar actuaciones conjuntas para impulsar la educación de los menores en los

entornos digitales, fomentando a la vez la participación tanto de los padres como de los profesores.

En la colaboración establecida se despliegan varias líneas de actuación que cubren, entre otros aspectos, el desarrollo y difusión de materiales para concienciar a los menores sobre el valor de la privacidad y la importancia de la información que publican en internet. Además, el MECD y la AEPD acordaron realizar acciones conjuntas para la elaboración de recursos formativos para padres, así como la organización de cursos, seminarios y jornadas sobre protección de datos y privacidad para profesores. En el documento se recoge también la posibilidad de crear materiales que puedan ser utilizados en la docencia para el contenido curricular sobre tecnologías de la información y la comunicación o la puesta en marcha, en cooperación con las Comunidades Autónomas, de fichas dirigidas a centros educativos. Por otro lado, entre otras iniciativas, ambos organismos se han comprometido a colaborar en la convocatoria de premios y concursos en materia de privacidad y protección de datos dirigidos tanto a alumnos como a centros educativos.

■ Canales de comunicación

La Agencia actualizó en octubre un canal de comunicación específico para familias, profesores y menores que incluye varias formas de contacto: correo electrónico (canaljoven@agpd.es), un teléfono de atención (901 233 144) y un sistema de WhatsApp (616 172 204) para informar y asesorar a estos grupos sobre cuestiones relacionadas con la privacidad.

■ Renovación www.tudecideseninternet.es

La Agencia presentó en noviembre de 2015 la nueva versión de su web Tú decides en internet (www.tudecideseninternet.es), un proyecto dirigido a

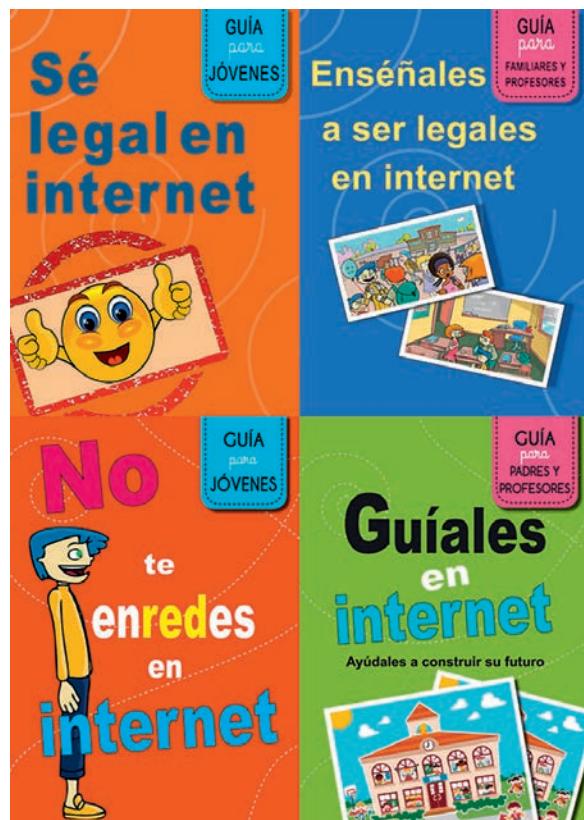
concienciar tanto a jóvenes como a padres y profesores sobre la importancia de proteger la privacidad. La renovación se centró en un rediseño que fue acompañado por la incorporación de nuevos contenidos y secciones actualizadas. La Agencia va a seguir apostando por la ampliación progresiva de los materiales que se ofrecen en esta web, tanto de elaboración propia como realizados con otras instituciones y entidades, ya que considera que las labores preventivas y de concienciación son básicas para difundir el derecho a la protección de datos de los menores.

■ Guías y nuevos materiales

La renovación en noviembre de la página web www.tudecideseninternet.es estuvo acompañada del lanzamiento de nuevos materiales, entre los que destacan dos guías con recomendaciones y consejos para una navegación segura en internet. La guía «No te enredes en internet» está orientada a los menores y está compuesta por ocho fichas didácticas dirigidas a menores de entre 10 y 14 años. Su amplio contenido abarca desde explicar a los jóvenes qué son los datos personales y qué información podría obtener un desconocido de ellos a las consecuencias de publicar o reenviar fotos y vídeos de uno mismo o de terceros sin plantearse las consecuencias. La guía ofrece también consejos y recomendaciones en temas como el reenvío automático de mensajes, la utilización segura de contraseñas, el comportamiento en grupos de mensajería instantánea, qué hacer para eliminar fotos o vídeos o cómo reaccionar ante el acoso. Por otro lado, la Agencia también presentó «Guíales en internet», una guía orientada a padres y profesores que ha sido diseñada como respuesta complementaria de la guía de menores y que tiene como objetivo, a partir de las fichas dirigidas a los niños, ofrecer a padres y profesores un texto orientador que pueda ayudarles con la

tarea de fomentar hábitos responsables entre los jóvenes en materia de privacidad y protección de datos.

Estos materiales elaborados por la Agencia se realizaron en colaboración con el Ministerio de Educación, Cultura y Deporte (MECD). Por su parte, el Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF), del MECD, aloja los contenidos en su plataforma para ponerlos a disposición de todos los profesores interesados en utilizarlos en el aula. Cada una de las guías mencionadas anteriormente –que están disponibles tanto en formato web como en PDF para imprimir– cuenta con un breve vídeo explicativo del contenido de las mismas.



Por último, y ya fuera del ámbito temporal de esta Memoria, la AEPD ha presentado e incorporado a la página web www.tudecideseninternet.es dos nuevas guías para no cometer ni ser víctima de conductas delictivas en internet: «Sé legal en internet» dirigida a jóvenes, y «Enséñales a ser legales en internet», para padres y profesores.

■ Colaboración institucional

La Agencia ha puesto en marcha varios canales de colaboración institucional para trabajar con los actores, públicos y privados, involucrados en la defensa, formación y concienciación de los menores. El objetivo es trabajar de manera conjunta en la elaboración, producción y difusión de materiales que contribuyan a sensibilizar y educar en el uso seguro de las nuevas tecnologías. En este sentido, la AEPD participó el 13 de octubre en la jornada «La mejora de la convivencia en los centros educativos: Confiar en la fuerza de la Educación», organizado por el Ministerio de Educación, Cultura y Deporte. Asimismo, la directora de la Agencia participó el 23 de octubre en el XVI Encuentro Nacional de Inspectores de Educación, celebrado en Sigüenza (Guadalajara), bajo la organización de la Unión Sindical de Inspectores de Educación (USIE). La privacidad de los menores también se abordó el 10 de diciembre en Madrid en la jornada «La protección de la infancia y la adolescencia en el entorno audiovisual. Desafíos para una regulación eficaz», organizada por la Comisión Nacional de los Mercados y la Competencia (CNMC) y el Observatorio de Contenidos Televisivos Audiovisuales (CTA). En este apartado de concienciación también hay que destacar la participación de la Agencia en la Jornada de presentación del Informe sobre el uso responsable de las Redes Sociales realizado por el Congreso, celebrada el 16 de octubre en la sede de la Secretaría de Estado de telecomunicaciones y para la sociedad de la información (SETSI)

y en la que abordó diferentes facetas del proyecto global orientado a menores puesto marcha por la Agencia.

La Agencia también ha participado en los grupos de trabajo sobre educación digital creados en eje-

cución de la recomendación que surgió de la Conferencia Internacional de las Autoridades de Protección de Datos celebrada en Varsovia en 2013, y la presentación de la experiencia del concurso escolar en el marco de la Conferencia celebrada en Ámsterdam en el mes de octubre de 2015.

3

E L PLAN ESTRATÉGICO 2015-2019. UNA HERRAMIENTA PARA DAR RESPUESTA A LAS NECESIDADES DE LOS CIUDADANOS, LOS RESPONSABLES Y LOS PROFESIONALES DE LA PROTECCIÓN DE DATOS

La protección de datos y la privacidad aparecen en numerosas encuestas como una de las mayores preocupaciones de los ciudadanos. La universalización del uso de internet y de los servicios de la sociedad de la información y la generalización de los dispositivos móviles inteligentes, entre otros factores, han conducido a un nuevo escenario en el que el volumen de información disponible y las posibilidades de elaborar perfiles e incluso predicciones sobre los usuarios de internet se han incrementado exponencialmente. El ciudadano ha pasado de ser un mero receptor de información a ser también un contribuyente activo al caudal disponible sobre él o sobre otros.

En el ámbito europeo, la protección de datos tiene el rango de derecho fundamental, correspondiendo a la Agencia Española de Protección de Datos tanto difundir el derecho como proteger a los ciudadanos velando por el cumplimiento de la legislación española. Para ello es imprescindible conocer las necesidades que plantean todos los implicados y articular los mecanismos para fomentar las garantías necesarias.

Los modelos más tradicionales de cumplimiento, basados en la corrección de las vulneraciones de la legislación, tienen limitaciones para hacer frente a las nuevas circunstancias. El contexto actual exige la implantación de nuevas políticas y herramientas proactivas de cumplimiento, así como acciones decididas que contribuyan a sensibilizar, formar y apoyar a los ciudadanos, al tiempo que permitan avanzar en la colaboración público-privada.

Estas acciones deben partir de una dimensión preventiva en la que los ciudadanos, como titulares de los datos, deben ser parte imprescindible de cualquier estrategia de protección. En las sociedades actuales los individuos deben ser conscientes de las múltiples situaciones en las que sus datos pueden

ser tratados, de cómo afectan esos tratamientos a sus derechos y de cómo pueden mantener el control sobre su información personal.

Ante el desconocimiento sobre qué información personal se genera, qué se comparte y con quién en un escenario marcado por una red global, se ha de perseverar en un modelo basado en la confianza mutua que evite la sospecha e incluso el rechazo a las nuevas tecnologías y que, simultáneamente, no se aprecie como una barrera para el desarrollo social y económico y la innovación.

En este contexto, la próxima aprobación de un nuevo marco legal europeo va a traer cambios significativos en la actividad de quienes tratan datos y, de modo especial, de los supervisores europeos.

Desde la perspectiva de las Autoridades de protección de datos, la gran novedad del Reglamento europeo es, sin duda, la intensa cooperación entre Autoridades que deberá presidir el ejercicio de sus funciones. El llamado sistema de ventanilla única para responsables y ciudadanos, el mecanismo de coherencia y las diversas modalidades de cooperación, que incluyen la posibilidad de realizar inspecciones conjuntas, dibujan un panorama en que muchas de las decisiones se tomarán en procesos colectivos.

El nuevo Reglamento será determinante en la actividad de la Agencia Española de Protección de Datos en los próximos años, y va a requerir analizar los cambios que será necesario introducir en la estructura y funcionamiento interno de la Agencia para adecuarse a las exigencias impuestas por la norma europea, tratando de anticiparnos a las competencias que debe asumir.

Las Autoridades de protección de datos europeas han puesto de manifiesto a lo largo de

los años su empeño en colaborar con todos los agentes. En este sentido, esta Agencia ha tratado de compatibilizar su labor supervisora con el propósito de ofrecer soluciones que permitan conciliar el desarrollo efectivo de iniciativas públicas y privadas con el respeto de los derechos individuales.

Para afrontar con garantías estas nuevas responsabilidades, y poder afianzarse como un organismo cercano que refuerce y amplíe las vías de comunicación con el ciudadano y con las empresas e instituciones, dando una respuesta integral a sus necesidades e inquietudes, la AEPD ha considerado necesario dotarse por primera vez de una hoja de ruta, su Plan Estratégico 2015-2019, con la que pretende movilizar sus recursos y potencialidades de una forma programada y eficiente; reforzar la cohesión interna de la institución y su imagen exterior; dar a conocer desde una perspectiva global e integradora todas las iniciativas y proyectos que se pretende desarrollar; facilitar la puesta al día de los procedimientos y sistemas de gestión interna mediante la Administración electrónica con vistas a la mejora continua en la prestación de los servicios y, lo que es más importante, posibilitar la mayor participación posible de los ciudadanos, responsables y profesionales de la privacidad en su elaboración y en su posterior ejecución, seguimiento y control.

La Agencia apostó por su elaboración con los medios propios y por escuchar todas las voces interesadas en participar en la elaboración del Plan Estratégico y, en consecuencia, acordó la apertura de un proceso de información pública, cuyas propuestas, sugerencias y comentarios, casi 400, contribuyeron, sin duda, a enriquecer el documento.



El documento se sometió a un cuestionario que podía responderse en la página web de la Agencia, recibiendo aportaciones de ciudadanos, responsables de tratamiento, expertos en protección de datos y organizaciones públicas y privadas, todas ellas de gran utilidad para la elaboración de la versión final del Plan Estratégico. Una gran parte de las aportaciones recibidas por este canal se centraron en las cuestiones relativas a la protección de menores, las relaciones de la Agencia con los responsables y profesionales de la privacidad y el impacto y evaluación de los efectos del nuevo Reglamento europeo.

Por otra parte, el documento sometido a consulta recibió otro grupo numeroso de aportaciones y propuestas procedentes de organizaciones, asociaciones y entidades, públicas y privadas, del ámbito de la economía digital y las telecomunicaciones, auditoría y certificación, seguros, consumo, etc.

Una gran parte de los comentarios y sugerencias recibidas nos han permitido constatar su coincidencia básica con las prioridades apuntadas por el Plan Estratégico:

- Apuesta por las medidas de carácter preventivo, de modo especial en el ámbito de la protección de los menores y la educación.

- Exigencia de un mayor diálogo y cercanía con los principales destinatarios de los servicios de la Agencia, los ciudadanos, los responsables y los profesionales de la privacidad.
- Impulso de medidas que contribuyan a fomentar la privacidad como un factor de confianza y favorecedor del desarrollo de la economía digital, la competitividad empresarial y la creación de empleo.
- Fomento de una labor proactiva de la Agencia que permita detectar, desde las primeras fases de diseño de los nuevos productos y servicios, el impacto que los mismos pueden tener en la privacidad de los ciudadanos.
- Mejora de la calidad y eficiencia de la gestión de los servicios que presta la Agencia, con especial referencia a los mecanismos de la Administración electrónica.

En consonancia con estos objetivos, el contenido del Plan se ha estructurado sobre cinco grandes Ejes estratégicos:

- Eje estratégico 1. Prevención para una protección más eficaz. Comprende un conjunto de iniciativas orientadas a promover actuaciones de carácter preventivo para garantizar el derecho a la protección de datos, centradas en ámbitos con un gran impacto ciudadano como la educación y la protección de los menores, la sanidad o la contratación irregular de servicios.
- Eje estratégico 2. Innovación y protección de datos: factor de confianza y garantía de calidad. Engloba medidas encaminadas a impulsar una labor proactiva en la Agencia que permita detectar el impacto de los nuevos desarrollos tecnológicos en la privacidad de los ciudadanos, favoreciendo la introducción, desde sus primeras fases de diseño, de los requerimientos legales en materia de protección de datos.

Con ello se busca contribuir a generar un clima de confianza en el ámbito de la economía digital, y en los usos de la tecnología por los sectores público y privado, favoreciendo la competitividad de las empresas de contenidos digitales, la creación de empleo, el desarrollo y la innovación de las industrias TIC. En definitiva, fomentando un ambiente propicio de cumplimiento normativo en materia de privacidad por parte de los responsables.

- Eje estratégico 3. Una Agencia colaboradora, transparente y participativa. Incluye distintas acciones encaminadas a favorecer la comunicación y las relaciones de la Agencia con los ciudadanos, facilitando el acceso a sus servicios mediante el uso de herramientas adecuadas a sus necesidades.
- Eje estratégico 4. Una Agencia cercana a los responsables y a los profesionales de la privacidad. Comprende un conjunto de actuaciones dirigidas a ofrecer unos canales próximos y especializados de relación con los responsables, encargados y profesionales de la privacidad que sean de utilidad para el cumplimiento del nuevo marco regulatorio.
- Eje estratégico 5. Una Agencia más ágil y eficiente. Prevé un grupo de iniciativas encaminadas a impulsar la mejora de la gestión y la calidad de los servicios que presta la Agencia, con especial atención a la simplificación de los procedimientos, la reducción de los tiempos de tramitación, la optimización de recursos y el uso intensivo de las herramientas de la Administración electrónica.

En el desarrollo de estas cinco líneas estratégicas, el Plan contempla 113 actuaciones concretas, siendo algunas de las más significativas las siguientes:

- Puesta en marcha de un canal específico de atención para padres y madres, profesores y menores.

- Desarrollo de actuaciones para la prevención de delitos cometidos contra o por los menores en internet, en colaboración con la Fiscalía y las Fuerzas y Cuerpos de Seguridad, mediante el traslado de actuaciones delictivas que conozca la Agencia en el curso de sus investigaciones, y la realización de acciones formativas orientadas a fomentar una utilización segura de internet por parte de los menores y sus familias.
- Creación de una Unidad de Atención a los responsables y a las pymes.
- Creación de la Unidad de Evaluación y Estudios Tecnológicos, destinada a promover la colaboración con las empresas y las universidades en relación con la evaluación del impacto en la privacidad de los nuevos desarrollos e innovaciones tecnológicas, a través de estudios, convenios, creación de grupos interdisciplinares, becas para graduados en titulaciones tecnológicas, encuentros y seminarios.
- Diseño de herramientas y materiales que faciliten la comunicación y las relaciones con los ciudadanos, responsables y profesionales de la privacidad, mediante la elaboración de fichas prácticas, vídeos, aplicaciones móviles o guías.



El conjunto de actuaciones recogidas en el Plan Estratégico son el reflejo de hacia dónde debe encaminarse esta institución los próximos años, cuáles son sus prioridades y sus objetivos esenciales. Todo ello responde no sólo a una necesaria puesta al día tras veinte años de funcionamiento, en un período que ha experimentado cambios profundos, sino también, y sobre todo, a la exigencia de dotar a la Agencia de una base sólida para afrontar el esfuerzo de adaptación que va a requerir el Reglamento europeo, de modo que pueda seguir siendo una de las autoridades de referencia en el escenario internacional.

En cualquier caso, el Plan se concibe como un documento dinámico, de forma que se puedan incorporar nuevas actuaciones o adaptar las previstas a la vista del diagnóstico realizado y los medios disponibles. A tal fin, se llevará a cabo una labor de seguimiento continuo de su ejecución por parte de las diversas áreas y unidades de la Agencia, que se plasmará en un Informe anual que dará cuenta de su grado de cumplimiento, las nuevas propuestas al mismo y, en su caso, las eventuales medidas correctoras a adoptar en caso de incumplimiento. Este informe se remitirá a la Comisión Constitucional del Congreso y se hará público en la web de la Agencia.

Este es el compromiso público asumido por la Agencia, para el que confía en seguir contando con la colaboración activa de todos los sectores y agentes concernidos, públicos y privados.

A-ACTUALIZACIÓN DEL MARCO JURÍDICO DE LA UNIÓN EUROPEA EN MATERIA DE PROTECCIÓN DE DATOS

En 2015 se ha dado un paso decisivo en la revisión del marco europeo de protección de datos. Como se ha venido recordando en las últimas Memorias, el 25 de enero de 2012 la Comisión Europea presentó dos propuestas de Reglamento General sobre Protección de Datos y de Directiva sobre protección de datos en el ámbito policial y judicial penal.

El pleno del Parlamento Europeo había confirmado el 12 de marzo de 2014 los informes sobre ambos textos adoptados por la Comisión LIBE en octubre de 2013. El Consejo, por su parte, siguió unos ritmos más lentos, pero bajo la Presidencia letona alcanzó en junio de 2015 la Orientación General sobre la propuesta de Reglamento. Posteriormente, en el mes de octubre y ya bajo Presidencia de Luxemburgo, el Consejo alcanzó igualmente el acuerdo de Orientación sobre la propuesta de Directiva.



Con la adopción de la Orientación General sobre el Reglamento se inició, en el mes de junio, la fase de negociación a tres bandas (Comisión, Parlamento y Consejo) con vistas a alcanzar una posición común que pueda ser ratificada por Parlamento y Consejo. Posteriormente, y ya con la aprobación en el mes de

octubre de la correspondiente Orientación General, estos «trílogos» se ampliaron también a la Directiva.

Las negociaciones culminaron en un tiempo que podría considerarse récord el 17 de diciembre de 2015, cuando las Instituciones dieron su acuerdo al paquete de reforma completo, incluyendo Reglamento y Directiva.

Con la aprobación por parte de COREPER y LIBE se inicia la fase final, que es la adopción definitiva por el pleno del Parlamento Europeo y por el Consejo, lo que requiere disponer de los documentos revisados por los servicios jurídicos y por juristas lingüistas en todos los idiomas oficiales. Sin que pueda darse una fecha precisa, las informaciones procedentes de las Instituciones avanzan la posibilidad de que ambos textos estén adoptados y publicados en el mes de junio de 2016. Aunque el proceso no esté totalmente finalizado, es muy improbable que se produzcan cambios en el contenido de los textos acordados, que pueden considerarse prácticamente definitivos en su versión actual.

Una vez que los textos sean aprobados por los plenarios de Parlamento y Consejo entrarán en vigor de forma inmediata, al día siguiente de su publicación, pero su aplicación se pospondrá en el tiempo. En el caso de la Directiva hay un periodo de dos años para su trasposición a los ordenamientos nacionales, mientras que en el del Reglamento, es la propia norma la que establece que será aplicable a los dos años de la fecha de entrada en vigor.

Como ya se ha insistido en anteriores Memorias, la AEPD, como órgano independiente de la Administración del Estado, no ha asumido en ningún caso la representación española en las discusiones que sobre este nuevo marco normativo se desarrollaron en el Consejo. No obstante, ha participado de forma muy activa, a título consultivo, prestan-

do asesoramiento y asistencia a los departamentos responsables en el marco de los mecanismos de coordinación que se han establecido para la tramitación de este paquete normativo.

Junto con esa labor de cooperación, la AEPD ha participado también activamente en la preparación de las reacciones del Grupo de Trabajo del Artículo29 (GT29) a estas iniciativas normativas. Además de en las Opiniones ya mencionadas en anteriores memorias, ha tenido un papel relevante en la elaboración de las posiciones que se citan posteriormente, en particular en la preparación de la posición del Grupo ante los «trílogos».

■ El nuevo Reglamento europeo de protección de datos

El Reglamento General de Protección de Datos que se aprobará definitivamente en 2016 contiene importantes novedades con relación a la Directiva actual.

La que sin duda tiene un alcance más transversal es el tipo de acto jurídico que se ha elegido para materializar la revisión del marco europeo de protección de datos. El Reglamento es una norma de efecto y aplicación directa que no requiere iniciativas normativas internas de trasposición o derogación. De este modo se busca la unificación de los derechos nacionales a través de una norma aplicable en toda la Unión. La aplicación de la Directiva del 95 en los Estados Miembros se ha realizado con la intermediación de las normas nacionales de transposición. Ello ha conducido a una dispersión que con frecuencia se ha criticado tanto desde la óptica de responsables y encargados, obligados a enfrentarse con regímenes jurídicos en ocasiones muy diferenciados, como de los interesados, cuyos derechos se protegen de distinta forma e intensidad, según el Estado miembro en que residan.

La aplicación directa del Reglamento no implica, sin embargo, una total uniformidad. El Reglamento contiene elementos que introducen flexibilidad y posibilitan la adaptación a los contextos nacionales. Por ejemplo, cuando exige que la identificación de los intereses públicos que pueden legitimar un tratamiento se realice mediante normas nacionales o de la Unión, abre la posibilidad de que esa determinación varíe en función de las diversas percepciones nacionales. Igual sucede con las posibles derogaciones al régimen de derechos de los interesados que incluye en su artículo 21, homólogo del artículo 13 de la actual Directiva, con la configuración de algunas de las excepciones que permiten el tratamiento de datos sensibles o con las reservas a la normativa de los Estados Miembros en cuestiones como las relaciones entre protección de datos y libertad de expresión y los tratamientos en el ámbito laboral.

Otra novedad del Reglamento se encuentra en su ámbito de aplicación territorial. Aunque se mantiene el criterio de que el Reglamento será aplicable a responsables, y encargados que tengan un establecimiento en la Unión Europea, el criterio del uso de medios para empresas no establecidas incluido en la Directiva del 95 se sustituye por el de la existencia de tratamientos que se deriven de una oferta de bienes y servicios a quienes se encuentren en la Unión o de un seguimiento de su conducta. Se trata de una modificación que busca adaptar la aplicabilidad del Reglamento al mundo a los servicios de la sociedad de la información donde la presencia física no es ya condición necesaria para desarrollar una actividad comercial y, en general, para recoger y tratar datos.

El Reglamento mantiene y refuerza principios y conceptos ya establecidos en la Directiva. Es el caso de la definición de dato personal, muy similar a la actual pero que incluye específicamente los datos seudonimizados o los identificadores online

en determinadas condiciones. En el terreno de los principios, junto a los clásicos como legalidad, finalidad o minimización, se incluyen algunos que hasta ahora no recibían esa calificación, como sucede con el principio de «integridad y confidencialidad» o el principio de «rendición de cuentas».

Uno de los objetivos del Reglamento es reforzar el control que el individuo tiene sobre sus datos. Para ello, se ha incluido una más precisa definición del consentimiento, que ha de seguir siendo libre, informado, específico e inequívoco, pero entendiendo este último concepto como algo que sólo se consigue cuando el consentimiento se manifiesta mediante una declaración en tal sentido o una «clara acción afirmativa». Se introducen, además, determinados criterios interpretativos sobre la carga de la prueba de la prestación del consentimiento, el carácter libre del consentimiento, especialmente en situaciones de desequilibrio entre quien lo solicita y el afectado, o el consentimiento de los menores en el ámbito de los servicios de la sociedad de la información.

En esa misma línea, el Reglamento reconoce dos nuevos derechos junto a los conocidos derechos ARCO: el derecho al olvido y el derecho a la portabilidad. En ambos casos, se trata de derechos vinculados al entorno online. En el caso del derecho al olvido, lo cierto es que la Sentencia del TJUE en el caso Google vs Agencia Española de Protección de Datos ha hecho innecesario tanto el derecho como tal como las previsiones que sobre el mismo hizo inicialmente la Comisión. El Tribunal confirmaba que el derecho al olvido no es un derecho autónomo o diferenciado, sino más exactamente la aplicación al entorno online, y en concreto a la actividad de los motores de búsqueda, de los derechos de oposición y cancelación. Consecuentemente, este derecho se ha configurado finalmente en el Reglamento como una consecuencia del derecho al bo-

rrado (el borrado conduce al olvido) y como una obligación del responsable que ha hecho públicos los datos que han de ser borrados de comunicar el mismo a los terceros a los que se hayan podido ceder.

El derecho a la portabilidad, por su parte, supone que el interesado que tenga sus datos almacenados en forma electrónica podrá decidir trasladarlos a otro servicio similar sin que el responsable pueda obstaculizar ese traslado. Este derecho está sometido a diversos requisitos y limitado por una restricción en lo que se podría definir como portabilidad pura: la transmisión directa de los datos desde un responsable a otro responsable, sin que el interesado tenga que participar activamente más allá de presentar su solicitud, se condiciona a que sea «técnicamente posible».

Uno de los aspectos en que el Reglamento presenta mayores innovaciones es el relativo a las obligaciones de responsables y encargados. Mientras que en la Directiva hay apenas una mención de estas obligaciones, la relativa a las medidas de seguridad, el Reglamento dedica todo un capítulo a enumerar las medidas que quienes tratan datos deberán poner en práctica para estar en condiciones de cumplir adecuadamente con las previsiones del Reglamento.

En este sentido, el Reglamento pasa del enfoque reactivo (hay unas normas, deben cumplirse, un organismo supervisa y si hay incumplimiento se sanciona) a un enfoque basado en la responsabilidad activa. Se espera que el que trata datos se centre en la prevención, adoptando medidas que aseguren razonablemente que se puede cumplir lo previsto legalmente. La razón fundamental, especialmente importante en un contexto en que cada vez se tratan más datos, de más tipos, con finalidades más diversas y por procedimientos más

variados, es que con frecuencia los incumplimientos conducen a daños para los interesados que difícilmente pueden ser reparados o compensados mediante una sanción.

Entre las medidas previstas por el Reglamento hay algunas ya presentes en la normativa de protección de datos europea o española, como son las medidas de seguridad, pero la mayor parte no tenían todavía reflejo normativo, por mucho que no fueran desconocidas en la práctica de la protección de datos. Es el caso de las medidas de protección de datos desde el diseño o por defecto, de la necesidad de realizar evaluaciones de impacto sobre la protección de datos en determinadas situaciones, de la notificación de quiebras de seguridad (ya existente en el sector de las telecomunicaciones) o de la introducción de la obligatoriedad de la figura del delegado de protección de datos en algunos supuestos.

En este mismo terreno es importante destacar cómo el Reglamento parece atribuir un mayor peso a figuras de co-regulación como son los códigos de conducta y los sellos o esquemas de certificación. Mientras que los segundos no se mencionan en la Directiva y a los primeros se les dedica sólo un artículo, el Reglamento incluye una regulación bastante detallada de ambos instrumentos, con referencia a posibles contenidos, procedimientos de adopción y adhesión, y supervisión.

El régimen de transferencias internacionales en el Reglamento sigue, en sus líneas básicas, el modelo de la Directiva. Se parte de que los datos sólo pueden ser enviados a países que ofrezcan un nivel de protección adecuado. En los casos en que el país en su conjunto no presente ese nivel de protección, las transferencias serán posibles cuando el exportador ofrezca garantías suficientes de protección. Finalmente, cuando no se dé ninguna de esas con-

diciones, los datos podrán seguir siendo enviados en el caso de determinadas excepciones relacionadas con la necesidad de las transferencias para satisfacer el interés del propio titular de los datos o intereses generales.

Las novedades que contiene el Reglamento se refieren, en primer lugar, a la inclusión de unos criterios para determinar el nivel de protección adecuado mucho más extensos y pormenorizados que los mencionados en la Directiva. En el terreno de las garantías suficientes se flexibilizan y amplían los instrumentos actualmente existentes, con una mención expresa de las normas corporativas vinculantes para responsables y encargados y de la adhesión a códigos de conducta o esquemas de certificación, siempre que vaya unida a compromisos vinculantes y ejecutables del importador asumidos por el importador para aplicar salvaguardas adecuadas en particular en lo relativo al ejercicio de derechos de los interesados.

El catálogo de excepciones es muy similar al de la Directiva, con el añadido de la posibilidad de transferir datos a países sin nivel adecuado de protección cuando esa transferencia sea necesaria para satisfacer el interés legítimo del responsable del tratamiento, no sea repetitiva y afecte a un número limitado de interesados, previo establecimiento de las garantías adecuadas para salvaguardar los derechos de los afectados.

Los mecanismos de control ocupan también una parte sustancial de las previsiones del Reglamento. Por un lado, profundiza en el modelo de supervisión europeo, consolidando el carácter especializado e independiente de las autoridades de protección de datos y reforzando y armonizando sus poderes, que expresamente se extienden a la potestad sancionadora.

Se establecen también mecanismos de coordinación y cooperación entre las autoridades. Quizás el mejor exponente de ellos sea el del Comité Europeo de Protección de Datos, que sustituirá al actual Grupo de Trabajo del Artículo 29. Esa sustitución no es sólo nominal. El futuro Comité se configura como un organismo de la Unión, con personalidad jurídica propia y con competencias ampliadas, entre las que destaca la de adoptar decisiones jurídicamente vinculantes.

En la versión final del Reglamento se ha mantenido la idea de un sistema de ventanilla única que la Comisión presentaba en la propuesta original. Sin embargo, ha habido una evolución significativa desde los planteamientos originales, rígidamente articulados en torno al principio de que, en caso de existir varios establecimientos de un responsable o encargado en la Unión Europea, toda la supervisión y todas las decisiones serían competencia de la autoridad del país donde se sitúe el establecimiento principal de la empresa. En el Reglamento se ha abandonado esa noción de competencia exclusiva de la autoridad principal, pasándose a un sistema en que todas las autoridades relacionadas con un responsable o encargado (por existir establecimientos en el territorio de los correspondientes estados miembros o porque sus ciudadanos estén afectados por los tratamientos) tienen participación en las decisiones. Una participación que será mayor o menor dependiendo de los tipos de temas que se planteen.

El sistema tiene unas mayores dosis de lo que durante las negociaciones se definió como «proximidad a los interesados» y se han resuelto algunos de los principales aspectos criticables contenidos en las propuestas iniciales. Sin embargo, ha ganado en complejidad, su funcionamiento va a requerir de un alto grado de compromiso por parte de todas las autoridades implicadas y deja sin resolver

los problemas que pueden derivarse del hecho de que el enfoque de ventanilla única en el nivel administrativo no va emparejado con un enfoque similar en ámbito judicial.

La atribución a todas las Autoridades de protección de datos de las mismas competencias de investigación y el establecimiento de un régimen común de infracciones y sanciones posibilitará que no existan las asimetrías que han generado la percepción de que algunas autoridades con mayores competencias, como consecuencia de la disparidad de transposiciones de la Directiva 95/46/CE, son más rigurosas que otras a la hora de garantizar el derecho a la protección de datos personales.

■ La nueva Directiva de protección de datos en el ámbito penal

El tratamiento de datos de carácter personal en el ámbito policial y judicial tiene unos rasgos específicos que pueden requerir normas diferenciadas de protección de los datos personales adaptadas a sus peculiaridades y que permitan garantizar la correcta ejecución de dichas actividades a la vez que se mantiene un elevado nivel de protección de los derechos fundamentales del individuo, facilitando el intercambio de datos cuando sea necesario y promoviendo la cooperación reglada entre las distintas autoridades policiales y judiciales de los Estados miembros. En ese sentido, la Declaración número 21 relativa a la protección de datos de carácter personal en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial, adoptada en la Conferencia Intergubernamental que adoptó el Tratado de Lisboa, reconocía que, en razón de la naturaleza específica de la cooperación judicial en materia penal y de la cooperación policial, podían requerirse normas específicas basadas en el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE) para la protección de

datos de carácter personal y la libre circulación de los mismos.

La legislación vigente de la Unión Europea en materia de protección de datos, la Directiva 95/46/CE, fue adoptada en el año 1995 con un doble objetivo: defender el derecho fundamental a la protección de datos y garantizar la libre circulación de datos personales entre los Estados miembros. Dicha norma se ha complementado con varios instrumentos que establecían normas específicas sobre protección de datos en el ámbito de la cooperación policial y judicial en materia penal, entre los que se incluye la Decisión Marco 2008/977/JAI. De forma paralela, el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y la Recomendación R(87) 15 del Comité de Ministros del Consejo de Europa a los Estados miembros por la que se regula el uso de datos personales en el ámbito policial han sido utilizados como marcos generales de protección de datos en los casos en los que la Directiva no era aplicable o para complementar regímenes específicos de protección de datos utilizados en mecanismos conjuntos de colaboración o en organismos de la Unión competentes en la materia. La Decisión Marco 2008/977/JAI representó sin duda un avance, aunque adolecía de un ámbito de aplicación limitado, al aplicarse únicamente al tratamiento transfronterizo de datos y no a las actividades de tratamiento por parte de las autoridades policiales y judiciales a nivel puramente nacional.

A su vez, mientras algunos Estados miembros incluyeron en el ámbito de aplicación de las normas que transponían la Directiva 95/46 los tratamientos en el ámbito policial y judicial, otros adoptaron soluciones de carácter específico, lo que derivó en una remarcable falta de armonización, creando

dificultades a las autoridades policiales y otras autoridades competentes en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial.

La Decisión Marco deja por su parte un amplio margen de maniobra a los Estados miembros para transponer sus disposiciones de Derecho interno y no contiene ningún mecanismo o grupo consultivo similar al Grupo del Artículo 29 establecido por la Directiva, ni otros que pudieran garantizar un grado aceptable de armonización en su aplicación.

La propuesta de Directiva ahora en fase de aprobación definitiva se basa en el artículo 16, apartado 2, del TFUE, que es la base jurídica introducida por el Tratado de Lisboa para la adopción de normas relativas a la protección de las personas físicas con respecto al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos, y por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y de normas relativas a la libre circulación de estos datos. La propuesta, como señalaba la Comisión en el documento que acompañaba a la propuesta original presentada en 2012, «tiene por objeto garantizar un nivel uniforme y elevado de protección de los datos en este ámbito, reforzando así la confianza mutua entre las autoridades policiales y judiciales de los distintos Estados miembros y facilitando la libre circulación de datos y la cooperación entre las autoridades policiales y judiciales».

En cuanto a la justificación de la necesidad de adoptar este nuevo texto, la Comisión abundaba en la necesidad de ofrecer el mismo nivel de protección para los datos intercambiados entre autoridades de los Estados miembros y los datos tratados a nivel nacional, favoreciendo la adopción de normas claras y precisas en protección de datos. Se

señalaba igualmente como factor que justificaba la adopción la fragmentación de las legislaciones nacionales. Concluía la evaluación señalando que la propuesta de Directiva era, por consiguiente, el mejor instrumento para garantizar en este ámbito la armonización a nivel de la UE y dejar, al mismo tiempo, a los Estados miembros la flexibilidad necesaria a la hora de aplicar los principios, las normas y sus excepciones a nivel nacional.

■ Ámbito de aplicación de la Directiva

La propuesta aprobada se aplica tanto al tratamiento nacional como transfronterizo de datos de carácter personal por las autoridades competentes de los Estados miembros en los ámbitos policial y judicial. Esto incluye la prevención, investigación, detección y enjuiciamiento de infracciones penales, así como la protección y la prevención de amenazas a la seguridad pública. No se aplica ni a las actividades de las instituciones, órganos y organismos de la UE –que cuentan con su propio marco legal– ni a las actividades que no estén comprendidas en el ámbito de aplicación del Derecho de la UE.

El texto permite a los Estados miembros establecer mayores garantías que las que se fijan con carácter general en la nueva norma e incluye como obligación de los Estados que el intercambio de datos de carácter personal entre las autoridades competentes no sufra restricciones por motivos relacionados con la protección de datos.

■ Principios

Establece una serie de principios entre los que se incluye la necesidad de garantizar que los datos personales se tratan de manera lícita, sean recogidos con fines determinados, explícitos y legítimos y sean adecuados, pertinentes y no excesivos en relación con los fines para los que se traten. En

lo tocante a la finalidad del tratamiento, establece la posibilidad de que las autoridades competentes utilicen datos recogidos con una finalidad determinada en otro tipo de tratamientos, dentro del marco fijado en el artículo 1.1 y siempre que así lo autorice el Derecho de la Unión o el del Estado miembro.

■ Distinción entre categorías de interesados y calidad de los datos

El responsable del tratamiento ha de establecer una distinción clara entre las diferentes categorías de interesados, como puedan ser las personas de las que existan sospechas fundadas de su participación en una infracción penal, las personas condenadas, las víctimas y otras. En este sentido, la propuesta sigue criterios presentes en otras normativas del sector, como la Decisión Europol o la Decisión Eurojust, ambas en trámite de modificación. Se establece también la obligación por parte de los Estados de distinguir aquella información basada en hechos de la que tenga como origen las apreciaciones personales.

■ Derechos de los titulares de los datos

Los Estados miembros tienen que ofrecer información de fácil comprensión y accesible por parte del usuario, así como a garantizar el derecho de acceso, rectificación, supresión o limitación del tratamiento de datos. No obstante, se establecen limitaciones, permitiendo a los Estados miembros adoptar medidas legislativas que limiten el ejercicio de esos derechos en casos justificados.

La Directiva establece que los derechos del individuo se pueden llevar a cabo de conformidad con la legislación del Estado miembro cuando los datos personales figuren en una resolución judicial o en un registro o expediente tratado en el curso de investigaciones y procedimientos penales.

■ Cumplimiento

Se establecen las obligaciones del responsable del tratamiento, entre las que se incluye llevar un registro de tratamiento de datos personales con una descripción de las políticas de protección de datos aplicadas. Se incorpora la figura del delegado de protección de datos que ayude a las autoridades competentes a garantizar el cumplimiento de las normas en materia de protección de datos. Igualmente, se establece la obligación conservar un registro de las operaciones de tratamiento en sistemas automatizados con la finalidad de comprobar la licitud del tratamiento, registro que estará a disposición de la autoridad de control.

■ Privacidad desde el diseño y por defecto

Se establece la protección de datos desde el diseño y por defecto como principios generales que han de ser aplicados por los responsables del tratamiento en el ámbito de la Directiva.

Otro instrumento para velar por el cumplimiento es el requisito de realizar una evaluación del impacto potencial cuando un tipo de tratamiento tenga probabilidades de generar un riesgo alto sobre los derechos del individuo, así como someter a consulta previa con la autoridad de control aquellos tratamientos que presenten un riesgo alto, en particular aquellos basados en el uso de nuevas tecnologías.

■ Quiebras de seguridad

Se establecen mecanismos de notificación de quiebras de seguridad tanto a la autoridad de control como a los individuos afectados, pudiendo restringirse esta última en casos específicos y justificados.

■ Supervisión

Las autoridades de control pueden ser las mismas que las establecidas en virtud del Reglamento ge-

neral de protección de datos. El texto establece normas relativas a la asistencia mutua obligatoria así como una obligación general de cooperar. Establece igualmente que el Comité Europeo de Protección de Datos ejerza sus funciones en el ámbito de aplicación de la Directiva.

Se incorpora también el derecho de los interesados a ser indemnizados si hubieran sufrido perjuicios como consecuencia de un tratamiento no conforme a las normas.

■ Transferencias a terceros países

Las transferencias a terceros países podrán llevarse a cabo cuando sean necesarias a los efectos de la norma y cuando la Comisión haya adoptado una decisión de adecuación favorable sobre el nivel de protección de datos que ofrece el país o la organización internacional de que se trate. Cuando no exista una decisión de adecuación, se pueden llevar a cabo transferencias con arreglo a garantías adecuadas, que han de ser justificadas por el responsable mediante decisión expresa y documentada a disposición de la autoridad de control. Existe una tercera posibilidad para circunstancias específicas y excepcionales que requieren justificación y documentación, con sujeción igualmente a control posterior por parte de la autoridad de control. Por último, bajo ciertas condiciones específicas, se podrá transferir de forma directa datos de carácter personal a destinatarios específicos establecidos en terceros países.

■ Acuerdos previos

Los acuerdos internacionales en vigor a la fecha de comienzo de aplicación de la Directiva seguirán siendo válidos mientras no se modifiquen, sustituyan o se revoquen.

B - ACTUACIÓN COORDINADA EN RELACIÓN CON LA NUEVA POLÍTICA DE PRIVACIDAD DE GOOGLE

En febrero de 2012 se inició un procedimiento coordinado entre las Autoridades de Protección de Datos de Alemania –Hamburgo–, España, Francia, Holanda, Italia y Reino Unido en relación a la nueva política de privacidad de Google que culminó en, el caso de la AEPD, con la resolución de un procedimiento sancionador en diciembre de 2013 y fue seguido por otros procedimientos cerrados en Francia y Holanda a lo largo de 2014.

La Autoridad Italiana emitió una orden el 20 de julio de 2014 en relación a las infracciones detectadas y en febrero de 2015 acordó un Protocolo de Verificación del cumplimiento de dicha orden con Google. Alemania cerró su procedimiento nacional en abril de 2015 y en el mismo reclamó a Google la limitación en el tratamiento y en la combinación de datos entre servicios, con la obligación de pedir, en su caso, un consentimiento válido; resolución que la compañía ha apelado a los tribunales y está pendiente de resolución. La Autoridad inglesa llegó, en función de su procedimiento, a un acuerdo de compromiso con Google en enero de 2015 para que corrijan las infracciones detectadas en línea con las recomendaciones aprobadas por el Grupo de Trabajo del artículo 29 en el plenario del mes de septiembre de 2014.

En el caso del procedimiento en España, Google hizo efectivo el pago de los 900.000 euros de sanción y desistió de presentar recurso contencioso-administrativo en diciembre de 2014. Sin embargo, en la resolución sancionadora también se establecía un requerimiento para que Google corrígiera la situación en relación a las infracciones detectadas, requerimiento que prescribiría el 18 de diciembre de 2015, por lo que las actuaciones de inspección continuaron a lo largo de dicho año.

Aunque los contenidos concretos de los procedimientos de los distintos países varían en función de los distintos marcos legales, las decisiones en todos los países coincidían en establecer que Google ha vulnerado las respectivas leyes de protección de datos y que esas vulneraciones afectan a la capacidad de los ciudadanos de saber qué se hace con sus datos personales y de ejercer un control eficaz sobre ellos. Por lo tanto, las acciones de seguimiento en el marco de los procedimientos nacionales también se coordinaron a lo largo de 2015 entre las distintas Autoridades.

El GT29, por su parte, aprobó en su reunión plenaria de septiembre de 2014 un conjunto de recomendaciones dirigidas a Google con el fin de precisar las ya formuladas en la carta remitida a Google en octubre de 2012. Google respondió al Grupo en diciembre de 2014 y, al mismo tiempo, siguió manteniendo contactos con todas las autoridades integrantes del grupo de trabajo y con éste como tal a lo largo de 2015. En concreto, la Task Force se reunió con representantes de Google en París el 25 de marzo. En esta reunión, la compañía presentó, con carácter confidencial y como continuación a la carta de diciembre de 2014, un catálogo de propuestas relacionadas tanto con las recomendaciones de la carta enviada por el GT29 como con los requerimientos contenidos en las resoluciones nacionales.

En respuesta a esta acción coordinada, Google puso en marcha una serie de iniciativas de cara a modificar su política de privacidad, ampliar la información a los usuarios y desarrollar nuevas herramientas para el control de la información personal por los sujetos de los datos. La iniciativa se plasmó en un ofrecimiento al Grupo de Trabajo de forma general, y directamente a las autoridades de forma individual, de sucesivos planes para el despliegue de las mejoras de forma cuatrimestral aproximadamente.

Durante el primer cuatrimestre de 2015 se celebraron con Google diversas reuniones de seguimiento en las que se trataron los cambios implantados y los propuestos en la Política de Privacidad, tanto con la AEPD como en el marco del grupo de Autoridades coordinadas, y entre otros se trató la necesidad de mejorar la colaboración que Google debía manifestar a la hora de proporcionar información detallada, en particular a la AEPD como autoridad de control.

En este marco, el 4 de mayo de 2015 se abrieron actuaciones de investigación para verificar el cumplimiento de medidas y la ampliación de la información a la AEPD sobre los procesos internos de tratamiento de datos personales. Estas actuaciones se concretaron en un primer requerimiento a Google para que proporcionase información detallada de qué datos se estaban recogiendo, cómo se comunicaban entre las aplicaciones, en qué ficheros se almacenaban y cuánto tiempo se retenían, descripción de los ejercicios de los derechos, etc., para así tener suficiente información para determinar el grado de cumplimiento de la resolución. A su vez, se reclamó a Google la presencia en la sede de la AEPD de su personal técnico para realizar un desarrollo y una explicación detallada de la información proporcionada a los Servicios de Inspección de esta Agencia.

Durante estas actuaciones se constató un avance real desde la resolución sancionadora en numerosos aspectos. Como ejemplos, puede destacarse que entre la información proporcionada a los usuarios se incluyó en la política de privacidad y aviso legal de YouTube el aviso de que se trata de una empresa del grupo Google, que se ha habilitado el centro «información personal y privacidad» a partir del enlace «Mi cuenta» a los usuarios con cuenta en Google, donde se ofrece información adicional y mayor posibilidad de gestión de la información recogida

por Google, que es accesible también a usuarios no autenticados aunque con una menor funcionalidad. Además, Google ha lanzado una campaña de recordatorios online cuando un usuario pretende hacer uso de sus servicios, orientada tanto para usuarios autenticados como no autenticados, que obliga a acceder a la información de privacidad y fijar los parámetros de configuración de privacidad.

En relación a la obtención del consentimiento para tratamiento de datos, en particular para la comunicación de datos entre servicios, el usuario tiene ahora la capacidad de desconectar selectivamente servicios que antes tenía activados de forma obligatoria y a los que se comunicaban datos de su actividad, incluyendo la posibilidad de eliminar completamente su cuenta. Google ha desactivado recientemente la capacidad de limitar el uso de cuentas abiertas por un mismo usuario. De esta forma, un usuario puede tener distintas cuentas y evitar la comunicación de datos entre las mismas, se han cifrado las cookies en el lado del cliente, y el contenido de la información recogida con las mismas en el lado del servidor.

En cuanto a la información recogida de usuarios pasivos, se han iniciado acciones dirigidas a los editores que utilizan la red publicitaria de Google con notificaciones intra-producto y correos electrónicos para que actualicen la política de consentimiento en la Unión Europea. Se está auditando a los editores que utilizan cookies publicitarias de Google en España, y se han tomado medidas en aquellos casos en los que se ha detectado un no cumplimiento. En el mismo sentido se ha creado la página «Cookiechoices.org», que ofrece herramientas para que los editores puedan cumplir la política de consentimiento.

En lo relativo a la conservación de datos, se han establecido herramientas para gestionar los datos de

los usuarios autenticados distinguiendo entre Contenidos, ligados al servicio en que se genera el contenido, y Actividad, relacionado con los metadatos de dicho contenido. Además, se han detallado y clarificado a la AEPD los procesos de conservación y eliminación para datos de contenido y datos de actividad tanto de usuarios autenticados como no autenticados y pasivos.

En el caso del ejercicio de derechos, Google ha incluido un formulario para solicitud de acceso a datos accesible desde la Política de Privacidad, así como un enlace para ponerse en contacto con la compañía, herramientas para acceder a los históricos de actividad y varias formas de acceder al formulario para ejercer el derecho al olvido.

Más allá de estas acciones constatadas, Google ha adoptado formalmente una serie de compromisos en una carta dirigida a la Directora de la Agencia Española de Protección de Datos, para seguir progresando en los cuatro aspectos anteriores, con varias acciones específicas entre las que destacan dar una mayor visibilidad del aviso de YouTube como empresa de Google, aumentar la lista de servicios con políticas específicas de privacidad o extender las campañas de recordatorio de privacidad a otros productos de Google y a los usuarios de Android. Una parte importante de los compromisos adquiridos es la de colaborar con la AEPD para ofrecer una mayor visibilidad (accountability) sobre el cumplimiento de la normativa de privacidad e informar del progreso de las auditorías dirigidas a los editores para implementar las políticas orientadas a usuarios pasivos, y de la efectividad de los formularios de ejercicio de derechos.

Esos progresos, si bien han determinado el archivo de las actuaciones en curso, siguiendo la línea de las actuaciones realizadas por el resto de Autoridades de Protección de Datos dentro del pro-

cedimiento coordinado, no constituyen un final al seguimiento de la implementación de la política de privacidad de Google, tanto a nivel de la AEPD como del procedimiento coordinado, sino que estas acciones continúan y se extienden a 2016.

C - LA SENTENCIA DEL TJUE DE 6 DE OCTUBRE SOBRE LA DECISIÓN DE PUERTO SEGURO (DECISIÓN 2000/520/CE)

El día 6 de octubre de 2015 se publicó el fallo de la Corte de Justicia de la Unión Europea (TJUE) en el caso Maximilian Schrems vs. Comisionado de Protección de Datos (C-362-14).

Se planteaba al Tribunal si en caso de presentarse ante una autoridad de protección de datos una reclamación en que se afirma que el tratamiento de datos llevado a cabo por una entidad importadora ubicada en un Estado respecto del que la Comisión hubiera declarado un nivel adecuado de protección la autoridad está vinculada «en términos absolutos» por la Decisión de la Comisión o si, en caso contrario, puede o debe realizar su propia investigación del asunto a la luz de la evolución de los hechos que haya tenido lugar desde que se publicó la Decisión de adecuación.

La sentencia parte del principio de que la finalidad de la Directiva 95/46/CE es asegurar un elevado nivel de protección de las libertades y derechos fundamentales, no debiendo ser interpretadas sus disposiciones de un modo restrictivo. A partir de ahí, y en cuanto al ámbito de competencias de las autoridades de protección de datos, el Tribunal aclara que «sería contrario al sistema establecido por la Directiva 95/46 y a la finalidad de sus artículos 25 y 28 que una decisión de la Comisión adoptada en virtud del artículo 25, apartado 6, de dicha Directiva tuviera el efecto de impedir que una autoridad nacional de control examine la solicitud

de una persona para la protección de sus derechos y libertades frente al tratamiento de sus datos personales que hayan sido o pudieran ser transferidos desde un Estado miembro a un tercer país al que se refiere esa decisión de la Comisión» (apartado 56), de modo que «las autoridades nacionales de control, a las que una persona haya presentado una solicitud de protección de sus derechos y libertades frente al tratamiento de datos personales que la conciernen, deben poder apreciar con toda independencia si la transferencia de esos datos cumple las exigencias establecidas por la referida Directiva» (apartado 57).

De este modo si planteada la reclamación fuese desestimada por la autoridad, los ciudadanos gozarían de la posibilidad de impugnar su cesión ante los tribunales del Estado miembro. Si por el contrario, la autoridad considera fundada la pretensión del interesado debería contar con la posibilidad de poner esta circunstancia en conocimiento de los órganos jurisdiccionales, en virtud de lo establecido en el artículo 28.3 de la Directiva.

El Tribunal, aun no siendo esta la cuestión planteada, entra a valorar la validez de la Decisión de adecuación de las transferencias internacionales de datos a las empresas adheridas a los principios de Puerto Seguro (Decisión 2000/520/CE). A tal efecto, clarifica (apartado 73) que «debe entenderse la expresión «nivel de protección adecuado» en el sentido de que exige que ese tercer país garantice efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión por la Directiva 95/46, entendida a la luz de la Carta».

Sentado este criterio, analiza el alcance de la Decisión, teniendo en cuenta que la aplicabilidad de

los principios de Puerto Seguro puede limitarse, en especial, por «las exigencias de seguridad nacional, interés público y cumplimiento de la ley [de Estados Unidos]», así como por «disposición legal o reglamentaria, o jurisprudencia, que originen conflictos de obligaciones o autorizaciones [explícitas], siempre que las entidades que recurran a tales autorizaciones puedan demostrar que el incumplimiento de los principios se limita a las medidas necesarias para garantizar los intereses legítimos esenciales contemplados por las mencionadas autorizaciones». De este modo, entiende que la Decisión reconoce la primacía de las exigencias establecidas por la normativa estadounidense, sin que conste en modo alguno «la existencia en Estados Unidos de reglas estatales destinadas a limitar las posibles injerencias en los derechos fundamentales de las personas cuyos datos se transfieren desde la Unión a Estados Unidos, injerencias que estuvieran autorizadas a llevar a cabo entidades estatales de ese país cuando persigan fines legítimos, como la seguridad nacional» (apartado 88), sino que, por el contrario, la Comisión constató que las autoridades de Estado Unidos podían acceder a los datos «y tratarlos de manera incompatible con las finalidades de esa transferencia» (apartado 90). Entiende el Tribunal que estas circunstancias suponen una lesión del derecho fundamental y que, al propio tiempo, el sistema «no prevé posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión no respecta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconoce el artículo 47 de la Carta» (apartado 95).

El Tribunal analiza igualmente el artículo 3 de la Decisión, que habilitaría la suspensión por los Estados Miembros de las transferencias realizadas a su amparo, entendiendo que dado lo limitado de los supuestos en que los Estados estarían legitimados

para acordar la suspensión, el artículo «priva a las autoridades nacionales de control de las facultades que les atribuye el artículo 28 de la Directiva 95/46, en el supuesto de que una persona alegue, con ocasión de una solicitud basada en esa disposición, factores que puedan afectar a la compatibilidad de una decisión de la Comisión, que haya constatado con fundamento en el artículo 25, apartado 6, de esa Directiva que un tercer país garantiza un nivel de protección adecuado, con la protección de la vida privada y de las libertades y derechos fundamentales de las personas» (apartado 102).

Por todo ello, el Tribunal considera «inválida» la Decisión 2000/520/CE.

El GT29 acogió positivamente la sentencia, en la medida en que refuerza las potestades de supervisión de las autoridades de protección de datos, pero se vio obligado a intervenir con el objetivo de buscar una respuesta coordinada de todas las autoridades europeas y ante la situación creada con la anulación del principal instrumento de transferencias a EEUU.

El Grupo estudió estas consecuencias en un Plenario extraordinario ad hoc celebrado el 16 de octubre. El resultado de la reunión fue una Declaración en la que se concluye que, lógicamente, las transferencias procedentes de la Unión Europea a EEUU ya no se pueden amparar en la Decisión de Puerto Seguro. Por ello, se hace un llamamiento a los Estados miembros y a las Instituciones europeas para iniciar conversaciones con las autoridades de EEUU a fin de encontrar soluciones políticas, jurídicas y técnicas que permitan transferencias de datos al territorio de EEUU respetando los derechos fundamentales. En definitiva, se pide la rápida adopción de algún tipo de instrumento que proporcione mayores garantías a los interesados en la UE o una versión mejorada de la Decisión de Puerto Seguro

que tenga en cuenta los requisitos fijados por el Tribunal.

El documento señala que, en cualquier caso, estas soluciones deberían ir siempre acompañadas por mecanismos claros y vinculantes e incluir, al menos, obligaciones sobre la necesaria supervisión del acceso por parte de las autoridades públicas, sobre transparencia, proporcionalidad, mecanismos de reparación y derechos recogidos en la legislación de protección de datos.

Según la Declaración, si a finales de enero de 2016 no se hubiera encontrado una solución adecuada con las autoridades estadounidenses, y en función de la evaluación de las herramientas de transferencia por parte del Grupo de Trabajo, las Autoridades de protección de datos de la UE se comprometían a adoptar las medidas necesarias y apropiadas, que podrían incluir acciones coordinadas de aplicación de la ley (enforcement).

Por otro lado, el Grupo inició los análisis del impacto en los otros instrumentos de transferencia mencionados contando con la participación de hasta cuatro de sus subgrupos sectoriales. El Grupo señalaba expresamente que en tanto este análisis no estuviera finalizado, las SCC y las BCR pueden seguir siendo utilizadas con carácter general, sin perjuicio de que deban investigar casos particulares, por ejemplo, a partir de denuncias, y ejerzan sus poderes con el fin de proteger a las personas.

El anuncio, el día 2 de enero de 2016, ya fuera del ámbito que corresponde a esta Memoria, de que la Comisión Europea y representantes de la Administración estadounidense habían alcanzado un acuerdo que permitiría a la Comisión poder adoptar una nueva decisión de adecuación sobre el esquema acordado –que recibirá el nombre de Privacy Shield- hizo necesario reordenar el trabajo

del Grupo a fin de poder tomar en consideración los nuevos elementos. El Grupo emitió una nueva Declaración en ese sentido, aunque sin entrar en el análisis del nuevo sistema, dado que en esos momentos no existía documentación disponible sobre el mismo.

El impacto que supuso la sentencia para los responsables de ficheros que hasta esa fecha confiaban en el marco legal establecido para realizar las transferencias internacionales motivó que la Agencia, en línea con lo acordado por las Autoridades de protección de datos de la Unión Europea (Grupo del 29), se dirigiera a los 1.648 responsables de 3.222 ficheros de titularidad privada que habían notificado transferencias internacionales de datos a entidades estadounidenses adheridas al acuerdo de Puerto Seguro informándoles de las consecuencias de la sentencia y solicitándoles que antes del 29 de enero de 2016, en concordancia con el plazo que el Grupo del 29 había establecido para encontrar una solución apropiada con las Autoridades de EEUU, comunicaran sus previsiones respecto a dichas transferencias.

La Agencia les transmitió que los instrumentos contractuales que incluyen las cláusulas tipo y las BCR mantenían su validez para realizar transferencias internacionales de datos a EEUU, así como, en su caso y cuando procedieran, las excepciones previstas en el artículo 34 de la LOPD.

Las acciones llevadas a cabo por los responsables que ya han contestado han consistido fundamentalmente en suprimir las transferencias, solicitar la correspondiente autorización al amparo de las cláusulas contractuales tipo adoptadas por las distintas Decisiones de la Comisión Europea y, en su caso, notificar las transferencias amparándolas en las excepciones a la autorización previstas en la Directiva 95/46 y en la LOPD.

D - INSPECCIÓN CONJUNTA SOBRE EL USO DE COOKIES - COOKIE SWEEP

La reforma de la Directiva 2002/58/EC, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), que entró en vigor en el año 2009, incluía una modificación en su artículo 5.3 que obliga a que la utilización de dispositivos que permitan el almacenamiento de información, el acceso a la información ya almacenada en el equipo terminal de un abonado o usuario, sólo pueda producirse a condición de que dicho abonado o usuario haya dado su consentimiento después de que se le haya facilitado información clara y completa. Esta disposición afecta singularmente al uso de cookies, pieza clave en el seguimiento de la navegación de los usuarios en internet.

Tras la entrada en vigor de la Directiva y su trasposición a los ordenamientos nacionales, tanto las autoridades de protección de datos de los Estados miembros como el Grupo de Trabajo del Artículo 29 adoptaron diversas medidas orientadas a facilitar el cumplimiento de estas disposiciones. Por lo que se refiere al Grupo del Artículo 29 se han aprobado hasta tres dictámenes con análisis y directrices sobre la aplicación práctica del artículo 5.3 en relación con el uso de cookies, más otro en que se analiza su aplicabilidad al seguimiento los dispositivos de seguimiento de la huella de los dispositivos electrónicos (device fingerprinting).

Al cumplirse los cinco años de su entrada en vigor, y con el fin de obtener indicadores sobre el cumplimiento efectivo de esta obligación, se decidió organizar una acción de inspección simultánea en varios Estados miembros, orientada al análisis de la situación en tres sectores específicos: comercio electrónico, medios de comunicación y sector pú-

blico. La Agencia Española de Protección de Datos participó en este estudio junto con autoridades de otros Estados miembros como Francia, Reino Unido o Países Bajos.

El objetivo del estudio era, fundamentalmente, obtener una visión transversal de la aplicación de la Directiva en toda la Unión Europea, identificando posibles pautas de incumplimiento o buenas prácticas que pudieran servir para desarrollar acciones de mejora a nivel nacional.

La inspección se llevó a cabo en dos fases. En una primera aproximación al problema se realizó una revisión estadística de las cookies utilizadas por cada uno de los sitios web incluidos en la muestra objeto de análisis, así como sus características técnicas. En la segunda fase, se revisó con detalle la información ofrecida por cada sitio web acerca del uso de cookies así como los mecanismos implantados para la obtención del consentimiento del usuario.

Los resultados de esta inspección fueron publicados por el Grupo del Artículo 29 en febrero de 2015, utilizando datos agregados por sector y a nivel global, incluyendo además un documento de conclusiones.

Las conclusiones señalaban que, con carácter general, los responsables de los sitios web objeto de análisis habían puesto en marcha medidas para informar a sus usuarios sobre la instalación y uso de cookies en los dispositivos utilizados para acceder a sus servicios. No obstante, también se señalaba que había margen de mejora en lo tocante a la obtención del consentimiento necesario para el uso de las cookies.

Entre los datos obtenidos se destacaban los siguientes:

- Se analizaron 478 sitios web de diferentes entidades pertenecientes a los sectores objeto de análisis.

- Los sitios web analizados instalaban en total 16.555 cookies, con una media de 34,6 cookies.

- El 70% de las cookies encontradas eran de tercera parte, y más de la mitad de ese porcentaje eran instaladas por sólo 25 proveedores de servicios de publicidad electrónica.

- 22 de los sitios web examinados instalaban más de 100 cookies en el momento en que el usuario accedía a la página principal. Por el contrario, en siete de los sitios web analizados no se procedía a la instalación de cookies cuando el usuario visitaba su página principal.

- La caducidad media de las cookies analizadas era con carácter general de entre uno y dos años, aunque tres de ellas llegaba a prolongar su vigencia hasta el 31 de diciembre del año 9999.

- El 26% de los sitios web analizados no ofrecía información sobre el uso de cookies. En los que sí facilitaban información, se llegó a la conclusión de que su visibilidad hacia el usuario podía ser mejorada en un 39% de los casos.

- Aproximadamente la mitad de los sitios web limitaba su actividad a informar a sus usuarios sobre el uso de cookies, sin requerir el consentimiento para su instalación de acuerdo a lo establecido en la normativa. Además, tan sólo el 16% de los sitios web analizados ofrecía un nivel granular de control sobre la instalación de estos dispositivos.

Los resultados del estudio ponen de manifiesto una situación que ofrece margen para la mejora, tanto en los mecanismos para proporcionar al usuario información previa, clara y completa, sobre el uso de cookies, como en los que se ocupan de la obtención del consentimiento.

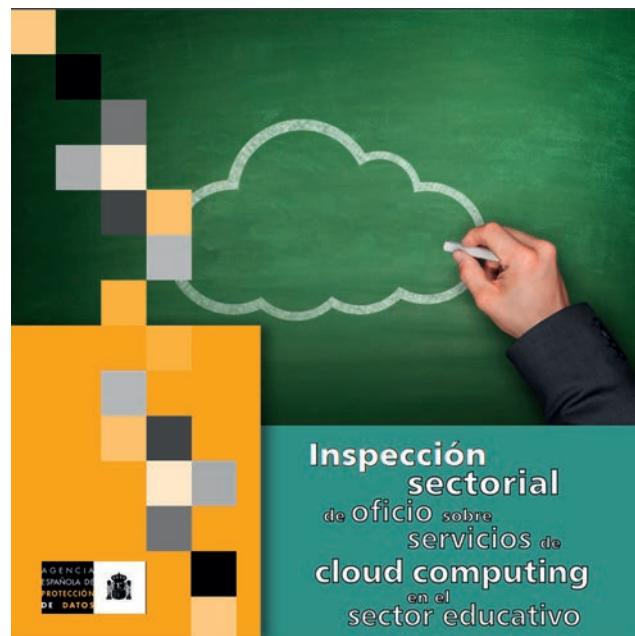
Por lo que se refiere a los proveedores de servicios, este estudio muestra que el ofrecer al usuario la información que necesita para poder decidir con conocimiento si otorga o no el consentimiento para la instalación de las cookies es un buen indicador del esfuerzo por parte del proveedor a la hora de respetar los derechos de los individuos recogidos en la normativa, así como un signo positivo de cara al usuario que ha de otorgar su confianza a un producto o servicio.

En el caso de la AEPD, la información proporcionada por el sweep ha conducido, junto con otros factores, a la decisión de actualizar y completar las guías sobre el uso de cookies que se recoge en su Plan Estratégico, actuación que, como la guía anterior, se desarrollará en colaboración con la industria.

E - LA INSPECCIÓN DE LOS SERVICIOS DE CLOUD COMPUTING EN EL SECTOR EDUCATIVO

La AEPD realizó la primera inspección a nivel europeo de servicios de cloud computing asociados a las plataformas de gestión educativa y de aprendizaje en centros de enseñanza secundaria.

La importancia de esta inspección, que se enmarca en las actividades preventivas de la Agencia, se deriva del volumen de datos objeto de tratamiento asociado a los más de ocho millones de alumnos escolarizados la tipología de los datos tratados -como los perfiles de aprendizaje de los alumnos o la gestión de datos especialmente protegidos de menores-, la pluralidad de agentes que intervienen en su tratamiento (centros educativos, profesores, prestadores externos de servicios y editoriales de libros digitales), así como del rápido desarrollo tecnológico aplicado en los procesos de enseñanza de los alumnos.



La aplicación de nuevas tecnologías en el ámbito educativo aporta perspectivas innovadoras para mejorar los procesos de enseñanza y aprendizaje que, no obstante, pueden implicar importantes riesgos para la privacidad. Es necesario abordar estos riesgos para facilitar el cambio hacia un entorno digital en la enseñanza que contribuya al desarrollo de estos nuevos modelos en un marco respetuoso con los derechos de los afectados y, en particular, de los alumnos, dadas las posibilidades que ofrece la tecnología para obtener perfiles personalizados desde muy temprana edad.

El informe de la inspección recoge tres apartados de conclusiones y 22 recomendaciones orientadas a subsanar las deficiencias detectadas en la protección de datos personales. Las más relevantes son las siguientes:

- La difusión pública de imágenes de los alumnos, especialmente en internet, exige la presta-

ción previa del consentimiento informado de ellos o de sus representantes legales.

- Las empresas que prestan a los centros educativos servicios relacionados con la gestión o plataformas de aprendizaje sólo podrán remitir comunicaciones comerciales a los usuarios de los centros educativos cuando han obtenido su consentimiento, que debe ser expreso si dichas comunicaciones se realizan mediante comunicaciones electrónicas.
- Los centros educativos deben asegurarse de la existencia del consentimiento de los usuarios de los sistemas de correo electrónico para permitir la visualización de datos por parte de otros usuarios del correo.
- Los contenidos que los alumnos publican en las aulas virtuales deberían ser supervisados por los educadores con objeto de evitar contenidos malintencionados. Para ello, la Agencia recomienda la revisión y autorización de los contenidos de acceso público por parte del profesor, la acreditación de esta autorización y adopción de sistemas que permitan la identificación del usuario que los publica.
- Se ha constatado la existencia de aplicaciones utilizadas por los profesores en sus dispositivos personales (tableta, móvil, etc.) para organizar las clases con los alumnos registrando sus datos personales, incluyendo imágenes y calificaciones académicas.

Los centros educativos deben elaborar normas internas para el uso de estas aplicaciones que garanticen su utilización de conformidad con la normativa de protección de datos personales.

- Los docentes suelen compartir documentos o servicios de almacenamiento en servicios de

cloud computing distintos de las plataformas educativas contratadas por los centros.

La utilización de estas plataformas debe ser autorizada previamente por el centro, que debe establecer normas internas que aseguren el cumplimiento de la LOPD.

- La prestación de servicios de cloud computing implica frecuentemente la intervención de subcontratistas ubicados en países en los que no existe una normativa de protección de datos personales que ofrezca el nivel de garantías exigido por la normativa europea y española. En consecuencia los centros educativos a la hora de contratar estos servicios deberán:

- Ser diligentes para obtener información sobre las garantías jurídicamente exigibles que ofrecen los distintos agentes que intervienen en la prestación de estos servicios para respetar el derecho a la protección de datos personales.
- Conocer, en particular, si la prestación de estos servicios implica la realización de transferencias internacionales de datos a países que no ofrecen garantías adecuadas, exigiéndolas contractualmente en los términos previstos por la normativa europea.

A este respecto debe señalarse que, con posterioridad a la inspección sectorial de la Agencia y como ya se ha mencionado en un apartado anterior de esta Memoria, la sentencia del Tribunal de Justicia de la Unión Europea de fecha 6 de octubre de 2015 ha declarado inválida la Decisión de la Comisión de 26 de Julio de 2000 2000/520/CE sobre Puerto Seguro, que declaraba adecuadas las transferencias internacionales de datos a EEUU amparadas en el acuerdo de Puerto Seguro.

■ Las plataformas de gestión educativa y de aprendizaje utilizan servicios de infraestructura de cloud computing que son suministrados por terceras entidades. Es por ello que los centros escolares que contratan los servicios de las citadas plataformas deben ser diligentes para conocer las medidas de seguridad que les ofrecen, teniendo en cuenta que son responsables del tratamiento de datos sensibles (datos de salud y psicopedagógicos) y de perfiles de alumnos.

En particular, deben garantizar que dichas plataformas dispongan de una certificación de seguridad apropiada, que sean auditadas por un tercero independiente de acuerdo con estándares de seguridad reconocidos y que sean puntualmente informados de las incidencias de seguridad que se produzcan y de las medidas adoptadas para resolverlas.

Asimismo, deben adoptar las medidas necesarias para que los usuarios del sistema conozcan las políticas del centro en materia de seguridad.

■ Las editoriales que facilitan libros digitales ponen a disposición de los usuarios plataformas

que permiten que los alumnos accedan al contenido de los libros y realicen los ejercicios. Por su parte, los profesores interactúan con los libros digitales de sus alumnos y comprueban los resultados obtenidos de los ejercicios.

En ocasiones, estos resultados no se integran en las plataformas educativas de los centros sino que se conservan en la editorial. En estos casos, las editoriales no tienen legitimación para el tratamiento de datos de los alumnos para fines distintos de los previstos en las licencias para el uso de los libros digitales.

Para evitar posibles usos indebidos de la información, debe promoverse la anonimización de los datos identificativos de los usuarios que acceden a los libros digitales, impidiendo su identificación por parte de la editorial.

Con el fin de promover la aplicación de estas recomendaciones en el ámbito de la educación gestionada por las administraciones públicas la Agencia, en colaboración con el Ministerio de Educación, Cultura y Deporte participó en la reunión de la Comisión General de la Conferencia de Educación.

A-ACTUALIZACIÓN DEL CONVENIO 108 DEL CONSEJO DE EUROPA

Aunque su impacto directo en el derecho español de protección de datos sea aparentemente menor, dada la influencia prioritaria del derecho de la Unión, no puede desconocerse la importancia del segundo de los instrumentos europeos actualmente en proceso de revisión. Se trata del Convenio 108 del Consejo de Europa, cuya reforma se abordó al cumplirse los 30 años de su adopción en 1981.

A lo largo de 2015 no se han producido otros avances significativos. El Comité ad hoc establecido para estudiar la propuesta hecha por el Comité Consultivo del Consejo elevó un texto al Comité de Ministros, que tomó conocimiento de él en abril de 2015. A partir de ese momento, la cuestión se ha seguido debatiendo en los distintos comités del Consejo de Europa y finalmente en el Grupo de Relatores Jurídicos, pero no se ha llegado a acuerdos que permitan avanzar el proceso.

Como ya se destacó en anteriores Memorias, un elemento clave de la revisión es que la Unión Europea ha reivindicado formalmente que su competencia en materia de protección de datos debe extenderse a la negociación y adopción de la nueva Convención. Para ello, el Consejo otorgó un mandato de negociación a la Comisión, que ha participado en las reuniones del CAHDATA, planteando reservas al texto final relacionadas con la compatibilidad de éste con los contenidos de la revisión del marco legal de la Unión que, paralelamente, se desarrollaba en Bruselas. Es de esperar que la conclusión de este último proceso permita finalizar también en un futuro próximo las negociaciones para la modernización del Convenio.

B-LA ACTIVIDAD DEL GRUPO DE TRABAJO DEL ARTÍCULO 29

Durante el año 2015 el Grupo de Trabajo del Artículo 29 (GT29) ha celebrado cinco reuniones plenarias ordinarias más una extraordinaria dedicada a analizar las consecuencias de la Sentencia del Tribunal de Justicia de la Unión Europea (TJUE) en el caso Schrems (Asunto C-362-14).

A lo largo de este periodo el Grupo ha adoptado dos dictámenes, así como dos documentos de posición sobre temas clave en las propuestas de Reglamento y Directiva de cara a la negociación en los trílogos. También se han redactado y remitido varias cartas que reflejan la posición del Grupo en cuestiones de relevancia actual, incluidas una sobre la Directiva de PNR europeo y otra sobre el PNR de México. Igualmente se ha publicado una declaración del Grupo sobre la aplicación de la Sentencia Schrems. Por otro lado, se ha continuado la actuación coordinada en relación con la nueva política de privacidad de Google. El Grupo ha tomado igualmente conocimiento del inicio de acciones a nivel nacional por parte de varias Autoridades de protección de datos en relación con los nuevos términos de uso de Facebook.

Como novedad dentro del funcionamiento del GT29 debe señalarse la creación de un nuevo subgrupo, el de Cooperación. Este subgrupo, tiene como objetivo concentrar y coordinar las actividades que el Grupo viene desarrollando, y desarrollará en el futuro, de cara a facilitar y promover una más intensa cooperación práctica de las Autoridades europeas, especialmente en todo lo relativo al desarrollo de sus funciones de supervisión y de reacción ante posibles infracciones.

■ Dictamen sobre cuestiones de protección de datos y privacidad relacionadas con el uso de drones (WP 231)

El Dictamen 01/2015 responde a la creciente presencia de drones en el espacio aéreo europeo y a la también creciente variedad de aplicaciones de este tipo de aparatos. Desde la perspectiva de la protección de datos lo relevante no es tanto el uso de drones como la amplia gama de sensores que estos aparatos pueden trasportar. La capacidad de esos sensores de captar datos personales y procesarlos o comunicarlos para su posterior tratamiento, unida a la versatilidad y maniobrabilidad de los drones, plantea riesgos para la privacidad que, aunque se pueden asimilar a los que presentan las cámaras de videovigilancia, los exceden en términos cuantitativos y cualitativos.



El Dictamen identifica una serie de riesgos específicamente vinculados al uso de drones equipados con sensores. Entre ellos, la falta de transparencia de estos tratamientos, derivada de la dificultad de localizar los drones y de saber qué datos se pueden estar captando, para qué finalidades y por quién. Son igualmente relevantes la facilidad que los dro-

nes tienen para sortear obstáculos que en principio protegerían frente a una recogida de datos por medios más tradicionales, la posibilidad de cubrir grandes espacios de forma sistemática y la de realizar seguimientos basados en determinadas informaciones obtenidas del propio objeto o persona a seguir.

Desde el punto de vista legal, el Dictamen afirma la aplicabilidad de la legislación de protección de datos a los tratamientos derivados del uso de drones dotados de sensores, sin perjuicio de que el uso y manejo de estas aeronaves puedan ser igualmente objeto de regulación en el ámbito de la normativa aeronáutica tanto europea como nacional.

Al mismo tiempo, el documento analiza la posibilidad de que resulten de aplicación las excepciones derivadas del uso de los datos con finalidades estrictamente personales y domésticas, con fines periodísticos y en el marco de las actividades de las fuerzas y cuerpos de seguridad, detallando los requisitos que deben cumplirse a estos efectos.

El dictamen se centra, particularmente, en formular recomendaciones para el uso de drones equipados con sensores a sus usuarios, como responsables del tratamiento de los datos que se obtengan, a los legisladores y a los fabricantes.

■ Procedimiento de cooperación para emitir opiniones comunes sobre cláusulas contractuales consideradas equiparables a las cláusulas tipo de la Comisión Europea

En 2014 el GT29 se pronunció sobre la adecuación de las cláusulas contractuales para transferencias internacionales empleadas por algunas grandes compañías como complemento a las cláusulas tipo adoptadas mediante decisiones de la Comisión. Esta intervención del Grupo fue consecuencia de un intento de armonizar las respuestas de todas las

autoridades nacionales a las que una empresa concreta había dirigido previamente sus peticiones. El objeto del análisis sería determinar hasta qué punto las cláusulas empleadas por estas grandes compañías en servicios tales como el cloud computing, que en teoría se inspiran en las aprobadas por la Comisión, son verdaderamente compatibles con ellas.

Ante la eventualidad de que este tipo de evaluaciones pudiera generalizarse, el Grupo decidió dotarse de un procedimiento que delimitase con claridad los roles respectivos del Grupo como tal y de las autoridades afectadas por las solicitudes y establezca cuáles han de ser las actuaciones de cada nivel, para evitar duplicación de trabajo y garantizar resultados consistentes en toda la UE. Este procedimiento se plasmó en un documento de trabajo (WP 226) aprobado en diciembre de 2014.

Para poner en práctica el procedimiento, el GT29 ha adoptado un modelo de declaración de «reconocimiento mutuo» basado en la que en su momento se utilizó en el contexto de las BCR. El proceso de adhesión al sistema se iniciará con una carta de la Presidencia del GT29 a todos los miembros pidiéndoles que expresen su intención de adherirse a esta declaración de reconocimiento mutuo. La lista de miembros que se adhieran al sistema será incluida en la página web del GT29.

■ **Carta al Comité LIBE del Parlamento Europeo sobre el PNR de la Unión Europea**

La Comisión Europea presentó en febrero de 2011 una propuesta de Directiva estableciendo un sistema de PNR (Listado de Nombres de Pasajeros) en la Unión Europea. Esta propuesta fue bloqueada en el Parlamento Europeo en abril de 2013 y no se produjeron avances significativos sobre el texto desde esa fecha.

Los atentados cometidos en París en enero de 2015 y el hecho de que los autores mantuvieran contactos con enclaves terroristas en Oriente Medio y hubieran viajado allí para recibir entrenamiento hicieron que varios responsables políticos europeos se plantearan reforzar los sistemas de control fronterizo y, en particular, retomar y concluir rápidamente el proceso de negociación de la Directiva de PNR.

Ante esta evolución, el GT29, que ya en 2011 había adoptado un dictamen en que manifestaba sus dudas sobre la iniciativa, decidió reiterar sus argumentos en una carta dirigida al presidente del Comité LIBE del Parlamento Europeo.

El Grupo reconoce en la carta que las nuevas propuestas presentadas por el relator encargado del proyecto en el Comité LIBE suponen una mejora en el texto. Sin embargo, constata que hay cuestiones todavía pendientes. La principal es que el Grupo sigue sin tener noticia de evidencias que avalen la necesidad de este instrumento para alcanzar los fines perseguidos y expliquen las razones por las que otros instrumentos ya existentes y menos intrusivos no pueden, en su configuración actual o con modificaciones, alcanzar los mismos objetivos. Por otro lado, el Grupo recuerda que hay un tratamiento de una gran cantidad de datos de todos los pasajeros en todos los vuelos, incluidos, según la nueva propuesta del relator, los intracomunitarios. Por ello, recomienda limitar esta recogida de datos atendiendo a criterios concretos como pueden ser zonas geográficas o períodos temporales limitados. Por otra parte, se vuelve a insistir en la necesidad de definir con mayor precisión los delitos cubiertos y de justificar y reducir los períodos de retención. Finalmente, el Grupo considera necesario que, caso de que el sistema se pusiera en funcionamiento, debiera preverse una evaluación detallada de su eficacia en un plazo lo más corto posible.

■ Carta a la Comisión sobre el PNR de México

Desde hace varios años tanto la AEPD como otras autoridades de protección de datos europeas han recibido informaciones indicando que las autoridades mexicanas habrían decidido comenzar a solicitar datos PNR a las compañías europeas que vuelan a y desde México. Esas informaciones señalaban, también, que la Comisión Europea habría estado negociando con las autoridades mexicanas y habría obtenido sucesivos aplazamientos de la puesta en marcha del esquema de PNR. A este respecto hay que indicar que en esta materia la competencia corresponde a la UE, y que es la Comisión Europea la encargada de mantener las negociaciones previas a la eventual firma de algún tipo de acuerdo bilateral.

A principios de 2015 varias compañías aéreas europeas contactaron con sus respectivas autoridades nacionales, entre ellas las de protección de datos, para informar de que comunicaciones oficiales mexicanas confirmaban la obligatoriedad de transmitir los datos PNR requeridos a partir del 1 de abril de 2015. El incumplimiento de estas obligaciones conllevaría fuertes sanciones económicas.

Las compañías aéreas se enfrentaban a una situación de conflicto de legislaciones. Por un lado, estarían obligadas a suministrar los datos para eludir posibles sanciones de las autoridades mexicanas. Por otro, deberían respetar el derecho de los Estados miembros de la Unión Europea, que prohíbe estos envíos en ausencia de bases legales suficientes y adecuadas.

Las distintas autoridades nacionales emprendieron iniciativas en el plano interno para intentar responder a esta situación. Sin embargo, y conscientes de que estas medidas no permitían resolver eficaz y permanentemente el problema, el GT29 remitió

en febrero de 2015 una carta a la Comisión Europea instándole a encontrar soluciones adecuadas y recordándole las consecuencias que podría tener para las compañías aéreas la entrada en vigor de la obligación de remisión de datos PNR sin que se hubiera establecido una base legal adecuada.

En respuesta a estas demandas, así como a los requerimientos de compañías aéreas y de los propios gobiernos de los Estados miembros, la Comisión solicitó al Consejo de Ministros mandato para establecer negociaciones con México con el objeto de concluir un tratado bilateral sobre comunicación de datos PNR, en línea con los ya existentes para EEUU, Canadá y Australia. No obstante, la Comisión también manifestó que estas negociaciones no comenzarían hasta que el Tribunal de Justicia de la Unión Europea no se pronuncie sobre la cuestión que el Parlamento Europeo le ha planteado en relación con la adecuación al derecho de la Unión del Acuerdo con Canadá.

La imposibilidad material de que el acuerdo con México pudiera concluirse y entrar en vigor antes del 1 de abril hizo que la Comisión solicitara y obtuviera de las autoridades mexicanas una nueva moratoria en su aplicación, que se pospuso al 1 de julio. Aunque no se tienen noticias formales de que este plazo se haya extendido, las negociaciones no han comenzado aún y no se está aplicando el esquema.

La importancia de esta cuestión no se limita solo al caso mexicano. Hay otros países terceros que con mayor o menor intensidad han expresado su interés de establecer sistemas nacionales de PNR que incluirían a los vuelos desde o hacia la Unión Europea. Es por ello que el modo en que se gestione por las partes implicadas el PNR de México puede resultar importante como precedente en el abordaje de futuras iniciativas de este tipo.

■ Actualización del Dictamen 8/2010 sobre Ley Aplicable a la luz de la Sentencia del TJUE en el caso Google-Spain

La Sentencia del Tribunal de Justicia de la Unión Europea (TJUE) de mayo de 2014 sobre el caso Google vs. AEPD resolvía diversas cuestiones planteadas por la Audiencia Nacional española. Entre ellas, la relativa a la aplicabilidad de la legislación española a Google como responsable de los tratamientos realizados por el motor de búsqueda.

El TJUE concluyó que podía considerarse que entre Google Inc. y Google Spain, filial española dedicada principalmente a la venta de publicidad, existe una asociación indisociable, en la medida en que los ingresos de la primera por la actividad del buscador dependen de la venta de publicidad que hace la segunda y en que esa venta de publicidad no podría llevarse a cabo si no existiera el servicio de búsqueda en el que se inserta. En definitiva, la sentencia concluía que a este tipo de relación se incluye en lo previsto en el artículo 4.1.a de la Directiva 95/46, según el cual la legislación de un Estado miembro, en este caso España, es aplicable cuando el tratamiento se lleva a cabo en el contexto de las actividades de un establecimiento de ese responsable en el territorio de ese Estado.

Esta conclusión supone una nueva interpretación del correspondiente artículo de la Directiva que no pudo tenerse en cuenta cuando en 2010 se redactó el Dictamen del GT29 sobre los criterios de determinación de la legislación aplicable. Por ello, el Grupo consideró necesario actualizar ese Dictamen e incorporar nuevos ejemplos que ilustren el razonamiento seguido por el Tribunal.

El nuevo Dictamen se presenta como «adenda» al anterior y analiza de forma muy resumida el contenido de la Sentencia. Su contenido, básicamente, gira en torno a la idea de que puede haber otro

tipo de relaciones entre un responsable y sus establecimientos que también podrían estar comprendidas en el ámbito del artículo 4.1.a. Al mismo tiempo, el nuevo texto señala también que la Sentencia del TJUE se limita a analizar el alcance de esa frase del artículo, sin entrar en otras cuestiones como podría ser qué sucede si uno de los establecimientos es más importante que otros o en qué medida los establecimientos son tales o más exactamente entidades diferenciadas que funcionarían, según los casos, como encargados de tratamiento.

C-ÁREA DE COOPERACIÓN POLICIAL Y JUDICIAL

SCHENGEN

■ Nuevo sistema de evaluación Schengen

En 2015 se ha completado la nueva estructura de supervisión en protección de datos del Área Schengen con la puesta en marcha efectiva del nuevo sistema de evaluación aplicable a los Estados miembros, en el que la Comisión Europea juega un papel relevante en colaboración con ellos. El nuevo sistema está regulado en el Reglamento 1053/2013 del Consejo, que establece un programa plurianual de actuaciones de evaluación de los Estados miembros, incluyendo un estudio detallado en el ámbito de la protección de datos de carácter personal, en particular la normativa aplicable al Sistema de Información Schengen de segunda generación (SIS II).

En las evaluaciones de protección de datos participan equipos de expertos nombrados por los Estados miembros y por la Comisión Europea. Se trata de inspecciones *in situ* con una duración efectiva de cinco días. El resultado de la evaluación, recogido en un informe de inspección y un documento de recomendaciones, es sometido a la consideración

del Consejo y del Parlamento Europeo. La Comisión Europea, por su parte, coordina las actividades y es la encargada del seguimiento y verificación de cumplimiento de las recomendaciones. De acuerdo a la planificación establecida, la evaluación correspondiente a España tendría lugar en 2017.

La Agencia Española de Protección de Datos desarrolla un papel activo en estos procedimientos, principalmente mediante el envío de expertos a las misiones de evaluación. En el año 2015 se ha participado en las evaluaciones de Austria y Alemania y se ha confirmado la participación en la de Croacia, prevista para febrero de 2016. En este último caso, se trata de una evaluación pre-acceso, por lo que tiene características diferenciadas respecto de las evaluaciones que se llevan a cabo en países ya integrados.

Por último, de cara al procedimiento de evaluación de España, previsto para 2017, la AEPD ha iniciado los trabajos preparatorios con la elaboración de un plan de acción y la constitución de un grupo de trabajo específico.

■ Incorporación de Reino Unido

Tras el resultado favorable de la evaluación pre-acceso realizada a Reino Unido en 2014, en la que la Agencia Española de Protección de Datos tuvo participación activa, Reino Unido formalizó la petición de incorporación al Sistema de Información Schengen de acuerdo a lo establecido en la Decisión 2000/365/CE.

Como resultado de lo anterior, la Decisión de Ejecución 2015/215 del Consejo estableció un calendario de actuaciones que culminó con el comienzo efectivo de la introducción de datos en el sistema por parte de Reino Unido el 1 de abril de 2015. Es de interés señalar que la incorporación al sistema no es completa, ya que Reino Unido no participa

en la parte del sistema relativo a las alertas relacionadas con prohibición de entrada reguladas en el artículo 26 del Reglamento 1987/2006.

■ Supervisión coordinada

El Grupo de Supervisión Coordinada del Sistema de Información Schengen, formado por representantes de las Autoridades de protección de datos de los Estados miembros y del Supervisor Europeo de Protección de Datos (EDPS), prosigue sus actividades de acuerdo al programa de trabajo bianual acordado por sus miembros. En ese sentido, es relevante señalar las actividades realizadas con el fin de acordar un marco conjunto de supervisión y auditoría de las alertas introducidas en el SIS II, del que este año se ha aprobado la parte correspondiente a la auditoría de seguridad y sistemas de información.

El Grupo también ha llevado a cabo una revisión exhaustiva de los procedimientos de ejercicio del derecho de acceso a los datos incluidos en el Sistema de Información Schengen con el fin de facilitar a los ciudadanos el ejercicio efectivo del mismo, tarea que ha culminado con la publicación de una guía actualizada a fecha octubre de 2015.

EUROPOL

■ Nuevo Reglamento Europol

La discusión de la propuesta de nuevo Reglamento Europol ha llegado a su fin con el acuerdo sobre un texto que aún requiere la aprobación formal del Parlamento Europeo y del Consejo, lo que se espera ocurra en abril de 2016, demorando su aplicación hasta abril de 2017.

El texto aprobado supone la creación de un régimen de protección de datos específico aplicable a Europol, que incluye un modelo de supervisión basado en el de supervisión coordinada existente

para los sistemas de información SIS, VIS y Eurodac, pero reforzado para adaptarse a las peculiaridades de los tratamientos de datos que lleva a cabo Europol.

En ese sentido, el responsable de supervisar la estructura central pasa a ser el Supervisor Europeo de Protección de Datos en sustitución de la Autoridad Conjunta de Control integrada por representantes de las Autoridades de protección de datos de los Estados miembros, mientras que los tratamientos realizados a nivel de Estado miembro serían responsabilidad de cada una de las Autoridades de protección de datos, incluyendo en ese ámbito a las oficinas de enlace de cada Estado miembro presentes en la sede central de Europol.

El texto establece la creación de un grupo de supervisión coordinada con un conjunto de competencias específicas centradas en la creación de procedimientos comunes de supervisión y la elaboración de criterios comunes, así como la elaboración de propuestas de consenso en caso de discrepancias. El Reglamento prevé también la participación de expertos nacionales en las actividades de inspección realizadas por el Supervisor Europeo de Protección de Datos en la sede central de Europol.

Es importante señalar que ese modelo va a ser, en principio, utilizado tanto para Eurojust como para la futura Fiscalía Europea y, por otro, que la posible integración a medio plazo de esas estructuras de supervisión en el Comité Europeo de Protección de Datos previsto en el nuevo Reglamento Europeo ha sido incluida a través de una petición expresa a la Comisión para que estudie esa posibilidad una vez que los diferentes reglamentos estén en vigor.

La Agencia ha asesorado a las autoridades españolas en aspectos técnicos relacionados con la tramitación de este Reglamento.

■ Autoridad Común de Control

En el marco de las actividades de la Autoridad Conjunta de Control de Europol, la Agencia ha participado tanto en la auditoría anual que tuvo lugar el pasado mes de marzo como en la de cumplimiento de las disposiciones del Acuerdo entre la Unión Europea y EEUU relativo Acuerdo TFTPII (Tratamiento y transferencia de datos de mensajería financiera de la Unión Europea a EEUU a efectos del Programa de seguimiento de la financiación del terrorismo), que tuvo lugar en mayo de 2015, y cuyas conclusiones fueron adoptadas en septiembre. Dichas conclusiones, aunque presentaban un resultado global positivo, no dejaban de hacer mención a la tensión que crea la realización de transferencias de gran volumen a las autoridades de EEUU con la idea de que dichos envíos de datos se realicen de forma limitada y ajustada en la mayor medida posible a las necesidades específicas en el tiempo derivadas de la lucha contra el terrorismo y el crimen organizado.

Por último, es necesario hacer una referencia al informe sobre las víctimas de actividades delictivas de trata de seres humanos y su impacto desde el punto de vista de la protección de datos de carácter personal. Basado en la experiencia de supervisión de las actividades de Europol, el informe presenta un conjunto de condiciones y buenas prácticas que permitan que las autoridades que lleven a cabo tratamiento de datos en ese ámbito lo hagan de forma apropiada y con pleno respeto de los derechos de los individuos afectados.

EUROJUST

■ Nuevo Reglamento Eurojust

La tramitación legislativa del nuevo Reglamento de Eurojust, que vendrá a sustituir a la Decisión 2002/187/JHA, enmendada en 2009, ha avanzado a lo largo de este año, sin que al final

del mismo se haya finalizado. El texto presenta numerosas novedades, incluyendo una reforma del régimen de protección de datos, en línea con el ya aprobado para Europol pero manteniendo elementos particulares en consideración de lo específico de la ubicación de Eurojust como instrumento de intercambio de información en el ámbito judicial.

La Agencia Española de Protección de Datos está asesorando a los organismos competentes en aspectos técnicos relacionados con la tramitación de esta norma legal.

■ Autoridad Común de Control

La Agencia participa regularmente en las actividades de supervisión de los tratamientos de datos realizados por la Oficina Europea de Justicia (Eurojust) tanto en el ámbito de su participación como miembro nacional en la autoridad común de control como aportando expertos para la realización de auditorías técnicas. En ese último aspecto, personal de la Agencia participó en la auditoría realizada en marzo de 2015 así como en las actividades de asesoramiento relativas a la implementación técnica de las recomendaciones derivadas de la misma. Conviene señalar, en ese mismo sentido, que la Ley 16/2015, de 7 de julio, por la que se regula el estatuto del miembro nacional de España en Eurojust, los conflictos de jurisdicción, las redes judiciales de cooperación internacional y el personal dependiente del Ministerio de Justicia en el Exterior, ha confirmado la representación por parte de España de la Directora de la Agencia Española de Protección de Datos en la Autoridad Común de Control.

EURODAC

■ Aplicación del nuevo marco legal

El 20 de julio de 2015 comenzó la aplicación efectiva del Reglamento (UE) número 603/2013 del

Parlamento Europeo y del Consejo, relativo a la creación del sistema Eurodac para la comparación de las impresiones dactilares en aplicación del Reglamento (UE) 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional.

En el marco de la adaptación a esta norma, se ha desarrollado un nuevo sistema de información a nivel central, responsabilidad de la Comisión Europea a través de la Agencia de Gestión de Grandes Sistemas de Información en el Área de Libertad, Seguridad y Justicia (EU-LISA), a la vez que los Estados miembros se han ocupado del desarrollo del sistema a nivel nacional.

■ Supervisión coordinada

El grupo de supervisión coordinada de Eurodac ha seguido de cerca el proceso de puesta en marcha de los nuevos sistemas, en particular las incidencias con diversos Estados miembros en los que se daban circunstancias que ponían en riesgo que, tal y como establece el Reglamento, el sistema a nivel nacional hubiera completado su adaptación y pudiera funcionar de acuerdo con los requisitos establecidos en la nueva norma antes de su fecha de aplicación efectiva. Además, el Grupo realizó una visita de estudio a la sede de EU-LISA para obtener información relativa al proceso de transición y a la puesta en marcha del nuevo sistema.

SISTEMA DE INFORMACIÓN DE VISADOS

■ Despliegue del sistema

El Sistema de Información de Visados culminó en 2015 el despliegue mundial que, según la planificación por zonas diseñada por la Comisión Europea, se inició en 2014.

■ Supervisión coordinada

Las actividades de supervisión conjunta estuvieron centradas en el análisis de las autoridades nacionales con acceso al sistema, incluyendo el acceso al sistema con fines de cumplimiento de la ley así como el relativo al ejercicio de los derechos reconocidos a los afectados. De la misma forma, se han analizado las actividades de las empresas que actúan como agentes de las representaciones diplomáticas en el extranjero y que se ocupan de la recogida de la documentación de los solicitantes y su transmisión a los Consulados.

Se ha avanzado notablemente en el desarrollo de un marco de supervisión común para las auditorías del sistema, incluyendo la posibilidad de realizar inspecciones conjuntas en aquellos países terceros donde una misma empresa se encargue de la solicitudes de visado correspondientes a varios Estados miembros.

D - CONFERENCIA DE PRIMAVERA DE AUTORIDADES EUROPEAS DE PROTECCIÓN DE DATOS

Los días 18 y 19 de mayo se celebró en Manchester la Conferencia de Primavera de Autoridades Europeas de Protección de Datos, organizada por la autoridad británica, el Information Commissioner's Office (ICO).

La Conferencia giró en torno al tema «Protección de Datos en la Práctica» y pretendía pasar revista a los diversos factores que deben contribuir a que las autoridades de protección de datos europeas puedan ofrecer a los ciudadanos el nivel y el tipo de protección que éstos esperan.

Desde esa perspectiva, uno de los elementos centrales de la Conferencia fue la presentación por

parte del comisionado británico de un estudio realizado por el propio ICO titulado «Derecho a la protección de datos: qué quieren los ciudadanos y qué quieren los ciudadanos de sus autoridades de protección de datos». El estudio recoge estudios europeos recientes sobre las actitudes de los ciudadanos respecto al derecho a la protección de datos a los que añade un también reciente estudio realizado en Reino Unido sobre control de los usuarios y privacidad en internet.

Las sesiones de la Conferencia respondieron a esa voluntad de analizar cómo ofrecer una protección real en la práctica desde las tres perspectivas de los instrumentos que pueden ponerse a disposición de los ciudadanos, de las medidas que pueden adoptar las entidades que tratan datos personales y de la actividad de las autoridades de protección de datos. Estos mismos planteamientos se reflejaron en una resolución adoptada por la Conferencia, con el título «Meeting data protection expectations in the digital future».

El Grupo de Trabajo de Cooperación en materia de Cumplimiento de la Ley (enforcement), creado en la Conferencia de 2014 y que tenía como objetivo el desarrollo de mecanismos de cooperación entre los miembros de la Conferencia (lo que incluye tanto a estados de la UE como de fuera de ella) en temas de inspección y sanción presentó un informe de su actividad. Entre sus propuestas se encuentra la de disponer del sistema CIRCABC, gestionado por la Comisión Europea, como plataforma para el intercambio de información entre las autoridades miembros de la Conferencia. La Comisión se ha mostrado favorable a crear este espacio dedicado dentro del CIRCABC y ya se ha iniciado su implantación.

La Conferencia aceptó como nuevo miembro a la Autoridad de protección de datos de Andorra,

que anteriormente había asistido regularmente a las reuniones anuales, si bien con el estatuto de observador.

E - CONFERENCIA INTERNACIONAL DE COMISIONADOS DE PROTECCIÓN DE DATOS Y PRIVACIDAD

Entre los días 26 y 29 de octubre se celebró en Ámsterdam la 37.^a Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, bajo el lema «Construyendo Puentes».

En esta edición, nuevamente, y siguiendo una línea ya consolidada a partir de los criterios adoptados en la Conferencia de México, la Sesión Cerrada tuvo un elevado peso específico en el conjunto de la Conferencia, dedicando un día completo al estudio y debates sobre dos temas: «Datos genéticos y de salud» y «Supervisión de Protección de Datos de la seguridad y la inteligencia: el papel de las APD en una sociedad cambiante». El resultado de estos debates se ha plasmado, como ya comienza a ser tradicional en este nuevo formato de la Sesión Cerrada, en la «Declaración de Ámsterdam».

La Conferencia adoptó también una serie de resoluciones, entre las que puede destacarse una relativa a «Informes de Transparencia», en la que la Conferencia subraya la importancia de que los responsables de tratamiento mantengan una política de información abierta sobre las peticiones de acceso que puedan recibir por parte de autoridades públicas.

Sin embargo, desde la perspectiva de la AEPD, la principal resolución adoptada fue la relativa a «Privacidad y Acción Internacional Humanitaria». Esta resolución fue promovida conjuntamente por la Red Iberoamericana de Protección de Datos y la Asociación Francófona de Autoridades de Protec-

ción de Datos, que actuaron bajo la coordinación de sus respectivas secretarías permanentes, la AEPD y la francesa CNIL. Como se indica en la exposición de motivos, el tema es de la máxima actualidad. La acción internacional humanitaria conlleva en muchos casos el tratamiento de datos personales, con frecuencia sensibles, de los beneficiarios. Esos tratamientos se están intensificando y ampliando mediante el uso de las TIC. Al mismo tiempo, el estatuto legal de los diversos actores humanitarios es heterogéneo y no todos ellos están protegidos en el desarrollo de su actividad por privilegios o inmunidades que garanticen una adecuada protección de los datos que manejan, muy especialmente frente a los accesos por parte de autoridades de estados involucrados en situaciones de persecución o conflicto armado.

La Resolución insta a la Conferencia a incluir estas cuestiones de relación entre privacidad y acción internacional humanitaria, y crea un Grupo de Trabajo que deberá estudiarlas y presentar sus conclusiones ante la próxima edición, desarrollando sus trabajos en estrecha colaboración con los actores humanitarios interesados. La AEPD y la Autoridad suiza de protección de datos actuarán como coordinadores de ese Grupo de Trabajo.

En la Sesión Cerrada se incluyó también una intervención del nuevo rapporteur Especial de Naciones Unidas para el Derecho a la Privacidad, Joe Cannati, y se adoptó una Resolución apoyando el trabajo del rapporteur.

En esta Conferencia fueron reconocidas como nuevos miembros las Autoridades de protección de datos de Benín, Georgia, Estado de México, Cantón de Basilea y Ucrania.

El Comité Ejecutivo ha visto modificada su composición. La Federal Trade Commission, que finalizaba su mandato, ha sido sustituida por el Comisiona-

do de Información de Canadá. Nueva Zelanda fue confirmada como presidencia del Comité Ejecutivo.

Las Sesiones Abiertas de la Conferencia giraron en torno a un documento, denominado igualmente «Building Bridges», elaborado por un panel de expertos norteamericanos y europeos. Este documento parte de reconocer que entre los sistemas de protección de datos y privacidad de EEUU y Europa puede haber diferencias sustanciales que difícilmente podrán salvarse, en la medida en que reflejan planteamientos culturales, sociales, económicos y legales distintos. Sin embargo, existen elementos y valores comunes sobre los que el documento pretende identificar mecanismos prácticos que permitan la interoperabilidad de los sistemas. El documento enumera hasta diez de esos «puentes», y la Conferencia ha fijado como objetivo hasta la siguiente edición trabajar para la aplicación del primero de ellos, definido como «Profundización en las relaciones entre el GT29 y la Federal Trade Commission».

La Sesión Cerrada aceptó la candidatura de Marruecos para organizar la próxima edición de la Conferencia Internacional.

F - LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS

Respecto a las actividades de la Red hay que destacar la celebración del XIII Encuentro Iberoamericano de Protección de Datos, que tuvo lugar del 6 al 8 de mayo en Lima, organizado por la Autoridad Nacional de Protección de Datos de Perú (APDP). Participaron representantes de Argentina, Brasil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, España, Honduras, Perú, Portugal, República Dominicana y Uruguay.

En la Sesión Cerrada, que se celebró el día 8, intervinieron miembros de la RPD de México, España,

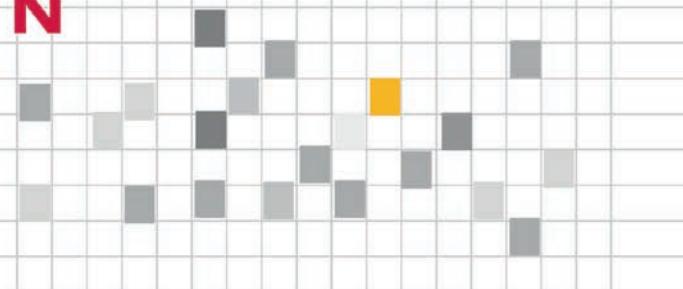
Costa Rica, Chile, Brasil, Ecuador y Honduras para informar sobre las principales novedades legislativas y el estado de la protección de datos personales en los respectivos países. Asimismo, se hizo un seguimiento del plan de trabajo aprobado en el XII Encuentro de México, y se acordó establecer una mayor coordinación entre las Autoridades integrantes de la delegación iberoamericana presentes en la 37.^a Conferencia Internacional de Autoridades de Protección de Datos. Finalmente, se aprobó la Declaración Final, la llamada «Declaración de Lima».

En cuanto a la normativa en proyecto, debe resenyarse el Seminario internacional «El anteproyecto brasileño de Protección de Datos Personales en perspectiva comparada», celebrado los días 19 y 20 de octubre en Brasilia (Brasil). Dentro de la colaboración con el programa EUROSociAL, tuvo lugar este evento organizado por la Secretaría Nacional de los Consumidores de Brasil, del Ministerio de Justicia, en apoyo a la tramitación del anteproyecto de ley de protección de datos personales, a cuya finalización se procedió a elevar a la Casa Civil de la Presidencia de la República, para su valoración, y, en su caso, remisión al Parlamento. Por parte de la RPD, participaron como expertos internacionales representantes de las Autoridades de Protección de Datos de Portugal, Uruguay, México y España. Por parte de la AEPD, asistió el Abogado del Estado-Jefe del Gabinete Jurídico.

Respecto de las restantes actividades organizadas en el marco de la RPD cabe mencionar las siguientes:

Foro «Libertad de Expresión y Protección de Datos Personales» celebrado en México DF en el mes de marzo. En el acto organizado por el INAI intervino el Director de la AEPD en la inauguración y como panelista en la Mesa 3, llamada «El Derecho al olvido en México, precedentes y retos».

RED IBEROAMERICANA DE PROTECCIÓN DE DATOS



6

Asimismo, el 26 de mayo se desarrolló el Webinario sobre el «Derecho al olvido» mediante videoconferencia en colaboración con la Fundación CEDDET, destinado a expertos de parlamentos iberoamericanos que integran la red de antiguos alumnos de CEDDET. La Conferencia fue impartida por el Abogado del Estado-Jefe del Gabinete Jurídico de la Agencia.

Los días 28-29 de mayo tuvo lugar el «III Congreso Internacional de Protección de Datos», que se celebró en Medellín (Colombia). El evento fue organizado por la Superintendencia de Industria y Comercio-Delegatura de Protección de Datos Personales de Colombia.

«Seminario-Taller Internacional de Diseño de una Normatividad de Protección de Datos Personales para la Función de Transparencia y Control Social (FTCS) de la República de Ecuador». Quito (Ecuador). Este taller internacional se celebró entre los días 29 de septiembre y 1 octubre en el marco de la colaboración entre la RPID y el Programa EUROSociAL, para la aprobación de una normativa interna en materia de protección de datos de aplicación a las ocho enti-

tidades que integran la FTCS de Ecuador (Defensoría del Pueblo, Superintendencia de Bancos, etc.). El objetivo del Taller es impulsar de nuevo el debate sobre la protección de datos en Ecuador, tras el intento frustrado hace tres años de aprobación de un proyecto de ley en la materia.

La colaboración de la Red Iberoamericana se concreta en la designación de expertos internacionales que apoyen técnicamente el proyecto. En particular, por parte de la AEPD, asistió el Adjunto a la Directora, que participó en varias mesas y ponencias.

Finalmente, dentro de la programación anual de la RPID en colaboración con la AECID, en el marco del Programa PIFTE, se celebró en el Centro de Formación de la Cooperación Española, en Montevideo (Uruguay), entre los días 3 y 5 de noviembre el Seminario «Los nuevos retos de la privacidad. El tratamiento masivo de los datos personales». Al seminario asistieron 49 representantes de autoridades de protección de datos y otras entidades públicas, así como del sector profesional y empresarial (Google, Microsoft, Mastercard, Hewlett Packard, etc.) de quince países, para intercambiar experien-

cias y conocimientos sobre el impacto de las nuevas tecnologías de tratamiento masivo de los datos personales en el ámbito de la privacidad (Big Data, Internet de las cosas, aplicaciones en dispositivos móviles, ciudades inteligentes, etc.)

Por parte de la AEPD, participó el Adjunto a la Directora, que intervino como ponente en los Paneles relativos a Internet de las cosas y Gestión de riesgos, y como moderador en el Panel correspondiente a Big Data.

En relación con las visitas institucionales a la AEPD en el marco de la colaboración entre la RIPD, la FIIAPP y CEDDET, a través del programa EUROSOCIAL, visitó la Agencia una delegación de varios miembros de diferentes instituciones de la República de Honduras, encabezada por la Comisionada-Presidenta del Instituto de Acceso a la Información Pública y por el Secretario de Estado de Derechos Humanos, Justicia Gobernación y Descentralización, junto con representantes del Congreso Nacional y del Consejo Hondureño de la Empresa Privada. Asimismo, estuvieron presentes la Directora General de Archivos y el Director General de Política Pública del Defensor del Pueblo de Ecuador.

En la reunión se expuso el papel de la Agencia en el desarrollo y aplicación de la normativa española de protección de datos, y se informó sobre el estado de situación de diversas iniciativas regulatorias, en especial del Anteproyecto de Ley de Protección de Datos Personales de Honduras, apoyado muy activamente por la cooperación española y la AEPD. Finalmente, se procedió a un debate sobre cuestiones prácticas de interés para ambas delegaciones.

Entre los días 19 y 22 de octubre visitó la Agencia el Director de la Agencia de Protección de Datos de Costa Rica (PRODHAB). El Director de la PRODHAB, Mauricio Garro, se reunió con la Directora de la

Agencia para tratar temas de interés común para ambas entidades. Asimismo, desarrolló un completo programa de reuniones con directivos y empleados de la Agencia sobre un conjunto amplio de temas: crédito y hacienda, relaciones laborales, transparencia y protección de datos, salud, menores, redes sociales, planes sectoriales de oficio, etc.

Por otro lado, el 21 octubre se produjo la visita a la Agencia de la Comisionada Presidenta del INAI y Presidenta de la RPD, Ximena Puente de la Mora. Durante dicha visita se reunió con la Directora para tratar temas que afectan a las relaciones entre ambas instituciones, así como a la Red Iberoamericana de Protección de Datos. En particular, se firmó la prórroga del vigente convenio de colaboración entre la AEPD y el INAI, con el compromiso de formalizar un nuevo convenio, de alcance más amplio, con ocasión del XIV Encuentro Iberoamericano en 2016. Asimismo, se trataron cuestiones relativas a la 37.^a Conferencia Internacional de Autoridades de Privacidad y de Protección de Datos.

En el ámbito de las actividades de formación destaca la puesta en marcha del curso online sobre protección de datos para empleados y directivos de las Autoridades y entidades integrantes de la RPD (15 octubre-15 diciembre). En el marco del programa de formación de la RPD, y en colaboración con la Fundación CEDDET, se ha desarrollado la primera edición del Curso online sobre protección de datos personales, dirigido a 35 empleados y directivos de las diferentes Autoridades y entidades públicas integrantes de la Red Iberoamericana de Protección de Datos (RIPD).

El curso incluye un completo programa de formación en protección de datos, dividido en seis módulos que abarcan los conceptos y elementos más importantes en dicha materia, impartido por personal directivo de la Agencia.

Por último se ha impulsado la presencia internacional de la Red Iberoamericana de Protección de Datos en la 37.^a Conferencia Internacional de Autoridades de Privacidad y de Protección de Datos y Privacidad (CICPDP), celebrada en Ámsterdam (Holanda) entre el 25 y el 29 de octubre.

Como antes se ha expuesto, desde la RPD se ha impulsado por primera vez una acción de coordinación efectiva entre las Autoridades iberoamericanas presentes en la CICPDP, encabezadas por las delegaciones mexicana y española, como Presidencia y Secretaría Permanente de la RPD. Por parte de la AEPD, asistieron la Directora y el responsable del Área Internacional de la Agencia.

Fruto de dicha coordinación, se ha promovido la iniciativa conjunta de resolución entre la RPD y la Asociación Francófona de Autoridades de Protección de Datos Personales (AFAPDP) sobre Privacidad y Acción Internacional Humanitaria mencionada anteriormente, que fue aprobada con el compromiso de crear un Grupo de Trabajo para el desarrollo de la misma, cuyos resultados se presentarán, para su aprobación, en la 38.^a CICPDP de Marrakech. Asimismo, se financiaron de forma conjunta entre la RPD y la AFAPDP los gastos de traducción por el uso del español y el francés en la sesión cerrada de la Conferencia Internacional, con el fin de mantener ambas lenguas como oficiales en dicha conferencia.

Durante el año 2015 se han tramitado un total de 38 asuntos instados por la Oficina del Defensor del Pueblo. Ello supone una tendencia descendente en relación con años anteriores, y en particular respecto a 2013 (59) y 2014 (53).

En cuanto a las principales materias o temas objeto de la atención del Defensor del Pueblo, hay que destacar los relativos a la morosidad, en especial los ficheros de solvencia (6); el llamado derecho al olvido (5); el tratamiento de los datos de salud (4); el uso indebido de los datos por empresas concesionarias (4); la videovigilancia (3); o el deber de secreto (3).

Respecto a las principales causas que llevan a los ciudadanos a dirigirse a la AEPD, a través de este cauce, la más destacable es la solicitud de información sobre el estado de tramitación de expedientes en curso promovidos por ellos, lo que ha tenido lugar en 22 ocasiones. También utilizan este mecanismo para exponer su disconformidad con los criterios seguidos por la Agencia a la hora de fundamentar sus decisiones, como ha sucedido en cinco ocasiones.

De otra parte, desde la oficina del Defensor del Pueblo se ha requerido información a la Agencia para proceder a un estudio o investigación más profunda sobre un tema o para conocer el criterio seguido por ésta en un determinado asunto. Así ha ocurrido en relación con los llamados «contadores inteligentes», a efectos de valorar las posibles implicaciones para la privacidad de los usuarios; el llamado derecho al olvido, para conocer los criterios de cumplimiento por los buscadores de la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014; las redes sociales, respecto al control parental sobre las fotografías de menores en Facebook, o el relativo al envío por la Dirección General de Tráfico de los datos personales de los conductores por correo postal.

En lo que se refiere al derecho al olvido en internet, el Defensor del Pueblo formuló una Recomendación en mayo de 2015 en la que se recogían diversas consideraciones sobre la necesidad de que los responsables de los buscadores en internet establecieran unos criterios claros, acordados entre todos los sujetos implicados, para la resolución de las reclamaciones de los ciudadanos; así como la determinación de un procedimiento al que los interesados pudieran acudir en caso de disconformidad con las decisiones del buscador, evitando la judicialización de estas reclamaciones.

Para ello, la Recomendación instaba a que se concretaran y publicaran los criterios seguidos por los gestores de los motores de búsqueda para la adopción de sus decisiones en esta materia y se estableciera un procedimiento concreto de reclamación previo a la vía judicial al que pudieran acogerse quienes discrepan con la decisión del responsable del buscador.

La AEPD contestó a la Recomendación en julio de 2015 informando, en primer lugar, de que no existe previsión legal que permita obligar a los gestores de motores de búsqueda a explicitar y publicar los criterios de aplicación y, en segundo lugar, de la dificultad de establecer criterios genéricos más allá de los recogidos en la STJUE de 13 de mayo de 2014, debido a que deben atender a las circunstancias de cada caso concreto para realizar la ponderación establecida por el Tribunal.

No obstante, se describían las diversas iniciativas de las Autoridades de protección de datos de la Unión Europea y del principal buscador en internet para ofrecer información sobre la aplicación de la sentencia del Tribunal de Justicia.

Al mismo tiempo se informaba sobre la existencia de un procedimiento administrativo especí-

fico para la tutela de estos derechos, previo a la vía judicial, para la tramitación con garantías de las reclamaciones presentadas ante la Agencia por quienes discrepan de las decisiones adoptadas por el buscador respecto de las solicitudes que los interesados le hubieran planteado. A partir de estas argumentaciones, la Agencia manifestó que las Recomendaciones realizadas por el Defensor del Pueblo no podían ser aceptadas.

En el mes de octubre, el Defensor del Pueblo, asumiendo la ausencia de una obligación legal para que los gestores de los motores de búsqueda publicaran los criterios que aplican, reiteró su criterio favorable a la publicación. En su escrito añadía que los derechos de los ciudadanos que reclamaban ante los buscadores deben garantizarse desde el momento de la solicitud inicial y no a posteriori una vez que hubiera sido denegada, concluyendo así que existe una ausencia de supervisión en la actuación de los motores de búsqueda y reiterando la necesidad de establecer un procedimiento administrativo concreto para la tutela de estos dere-

chos. A partir de estas consideraciones solicitaba información adicional a la Agencia.

La AEPD contestó la solicitud en el mes de diciembre ratificando la existencia de un procedimiento específico para la tutela de los derechos de oposición y cancelación que no prevé un pronunciamiento previo a la decisión del buscador sobre las reclamaciones que se le plantean. Adicionalmente, facilitó datos sobre las reclamaciones planteadas y el resultado de las resoluciones dictadas para concluir que no es posible compartir la afirmación de que exista una ausencia de supervisión en la actuación de los motores de búsqueda.

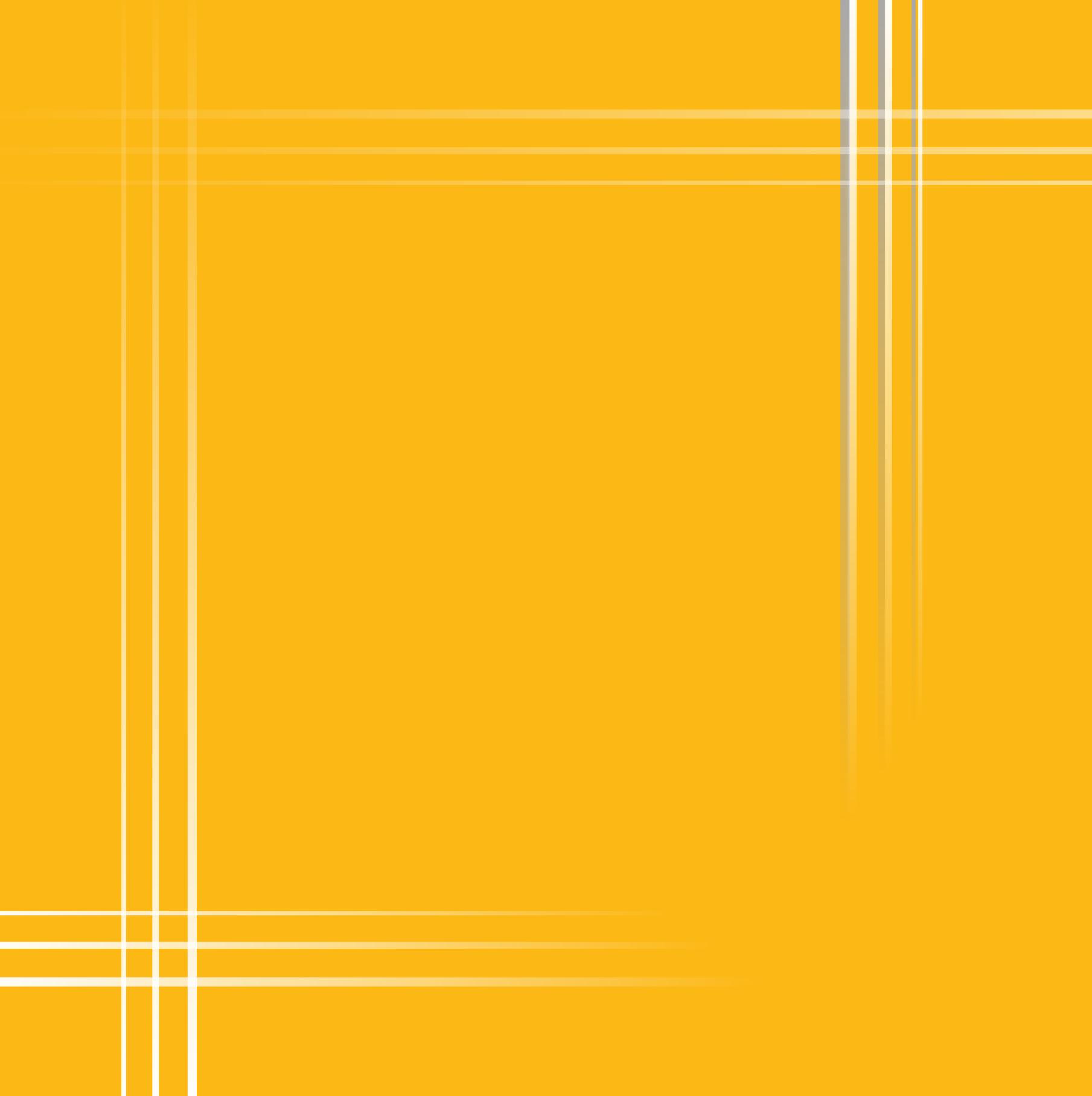
No obstante, la Agencia compartió la conveniencia de facilitar una información más amplia y detallada sobre los criterios aplicables y sobre cómo facilitar el ejercicio de sus derechos a los ciudadanos, ofreciendo diversas medidas para alcanzar ambos objetivos. En consecuencia, la respuesta al Defensor del Pueblo concluyó aceptando parcialmente su Recomendación con el compromiso de adoptar las medidas propuestas.

El Plan Estratégico de la Agencia contempla entre sus prioridades impulsar los procedimientos de cooperación con las distintas Autoridades autonómicas de protección de datos. En primer lugar, es necesario destacar la creación del Consejo de Transparencia y Protección de Datos de Andalucía, creado por el artículo 43 de la Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía, una institución que fortalecerá la aplicación de la normativa de protección de datos en dicha Comunidad Autónoma.

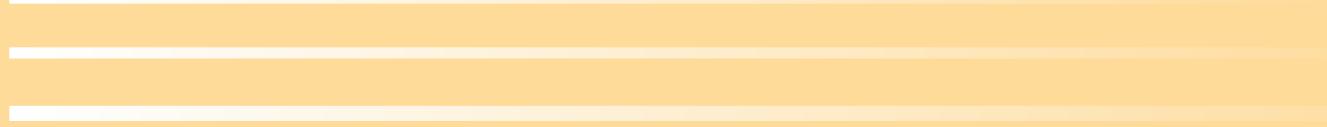
En relación con los procedimientos de cooperación celebrados con las diferentes Autoridades, en el año 2015 se han mantenido en el marco del Consejo Consultivo, detallados en el apartado Representación Institucional de esta Memoria, y la Reunión de Directores/as.

Durante 2015 se ha mantenido la cooperación entre los Registros de la Agencia Española de Protección de Datos y los de la Autoridad Catalana de Protección de Datos (APDCAT) y la Agencia Vasca de Protección de datos (AVPD), que tiene por finalidad facilitar el cumplimiento de la obligación de notificación de ficheros, y conforme al protocolo de intercambio de operaciones registrales.

Los retos globales relacionados con las nuevas tecnologías a los que se enfrenta la protección de datos son otro de los temas en los que se ha desarrollado la cooperación. El 23 de enero la Agencia participó en una Jornada organizada por la Agencia Vasca de Protección de Datos con la colaboración de la AEPD y la Autoridad Catalana de Protección de Datos en la que se puso de manifiesto la visión de las autoridades de control acerca de la «Tecnología, privacidad y tratamiento de los datos personales por administraciones y empresas». El evento, celebrado en Bilbao, incluyó tres mesas redondas. La primera de ellas, moderada por el director de la AEPD, incluyó una presentación en la que se analizaron los aspectos más destacados de la Guía de evaluación de impacto sobre la privacidad, tratando aspectos de la relación entre protección de datos, transparencia y acceso a la información pública. La segunda, presidida por el director de la AVPD, se centró en la situación actual de la protección de datos en las administraciones públicas. Finalmente, la tercera estuvo dirigida por la directora de la APDCAT y se dedicó a la importancia de la prevención en las nuevas tecnologías. Con carácter previo a esta sesión, se celebró una reunión de trabajo para intercambiar criterios sobre el derecho a la protección de datos y la transparencia y acceso a la información pública.



AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



MEMORIA 2015

LA AGENCIA EN CIFRAS

INSPECCIÓN DE DATOS

DENUNCIAS Y RECLAMACIONES REGISTRADAS

TIPO	2013	2014	2015	% RELATIVO	Δ% 2014/2015
Escritos de reclamación de tutela	1.997	2.099	2.082	19,70	-0,81
Escritos de denuncia	8.607	10.074	8.489	80,30	-15,73
TOTAL	10.604	12.173	10.571	100	-13,16

DENUNCIAS Y RECLAMACIONES RESUELTA

TIPO	2013	2014	2015	% RELATIVO	Δ% 2014/2015
Reclamaciones de tutela de derechos	2.108	1.818	2.113	16,27	16,23
Denuncias	8.633	9.404	10.871	83,73	15,60
TOTAL	10.741	11.222	12.984	100	15,70

MEMORIA 2015

RESOLUCIONES – EJERCICIO DE LA POTESTAD SANCIONADORA

SEGÚN TIPO DE PROCEDIMIENTO	2013	2014	2015	% RELATIVO	Δ% 2014/2015
Archivo de denuncia sin actuaciones de investigación	5.114	5.692	6.049	67,70	6,27
Archivo de actuaciones tras no subsanarse denuncia	415	467	691	7,73	47,97
Archivo de actuaciones de investigación	1.087	1.157	1.040	11,64	-10,11
Resolución de procedimientos de apercibimiento	219	315	397	4,44	26,03
Resolución de procedimientos sancionadores	719	752	693	7,76	-7,85
Resolución de procedimientos de infracción de las AAPP	58	60	65	0,73	8,33
SEGÚN SENTIDO DE LA RESOLUCIÓN	2013	2014	2015	% RELATIVO	Δ% 2014/2015
Archivo actuaciones previas	6.616	7.316	7.780	87,07	6,34
Archivo de procedimiento de apercibimiento	13	127	216	2,42	70,08
Archivo de procedimiento sancionador	103	113	99	1,11	-12,39
Archivo de procedimiento de infracción de las AAPP	6	15	13	0,15	-13,33
TOTAL RESOLUCIONES DE ARCHIVO	6.738	7.571	8.108	90,74	7,09
Declarativa de infracción con apercibimiento	206	207	181	2,03	-12,56
Declarativa de infracción con sanción económica	616	620	594	6,65	-4,19
Declarativa de infracción de las AAPP	52	45	52	0,58	15,56
TOTAL RESOLUCIONES DECLARATIVAS DE INFRACCIÓN	874	872	827	9,26	-5,16
TOTAL RESOLUCIONES POTESTAD SANCIONADORA	7.612	8.443	8.935	100	5,83

* En cada resolución puede haberse analizado más de una infracción.

** Las cifras corresponden al número total de resoluciones dictadas en cada ejercicio en relación con denuncias que hubieran sido presentadas y de inspecciones que hubieran sido iniciadas de oficio en el mismo ejercicio o en ejercicios anteriores. Cada resolución puede tener su origen en una o en más denuncias que se han acumulado atendiendo al criterio de identidad de hechos.

EXENCIÓN DEL DEBER DE INFORMACIÓN AL INTERESADO

(Título IX, Cap. VII Reglamento de desarrollo de la LOPD)

	2013	2014	2015	Δ% 2014/2015
Procedimientos resueltos	4	2	3	50

INFRACCIONES SEGÚN LEY INFRINGIDA. SECTOR PRIVADO

	2013	2014	2015	% RELATIVO	Δ% 2014/2015
LOPD	924	896	782	87,37	-12,72
LSSI	57	95	100	11,17	5,26
LGT	3	6	13	1,45	116,67
TOTAL	984	997	895	100	-10,23

NÚMERO DE INFRACCIONES SEGÚN GRAVEDAD. SECTOR PRIVADO

	2013	2014	2015	% RELATIVO	Δ% 2014/2015
MUY GRAVE	0	2	3	0,34	50
GRAVE	894	846	759	84,80	-10,28
LEVE	90	149	133	14,86	-10,74
TOTAL	984	997	895	100	-10,23

* En este apartado se detallan cifras sobre infracciones declaradas, pudiendo haberse declarado más de una infracción en cada resolución de procedimiento sancionador o de apercibimiento.

MEMORIA2015

APLICACIÓN DE CRITERIOS DE GRADUACIÓN EN LA DECLARACIÓN DE INFRACCIONES. SECTOR PRIVADO

	2013				2014				2015				% RELATIVO 2014/2015	Δ% 2014/2015
	LOPD	LSSI	LGT	TOTAL	LOPD	LSSI	LGT	TOTAL	LOPD	LSSI	LGT	TOTAL		
Apercibimiento	216	194	27	0	221	163	24	0	187	163	24	0	20,89	-15,38
Sanción por la escala de gravedad precedente	350	442	0	0	442	464	13	0	477	464	13	0	53,30	7,92
Sanción sin atenuación	418	260	68	6	334	155	63	13	231	155	63	13	25,81	-30,84
Total infracciones	984	896	95	6	997	782	100	13	895	782	100	13	100,00	-10,23

* En este apartado se detallan cifras sobre infracciones declaradas, pudiendo haberse declarado más de una infracción en cada resolución de procedimiento sancionador o de apercibimiento.

** Desde el 11 de mayo de 2014, el artículo 39 bis de la LSSI, introducido por el apartado once de la disposición final segunda de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, prevé la moderación de las sanciones (faltas graves) y la figura del apercibimiento.

EVOLUCIÓN DE LAS INFRACCIONES CON SANCIÓN ECONÓMICA. SECTOR PRIVADO

	2013	2014	2015	Δ%	
				2014/2015	
Total sanciones	768	776	708		-8,76

* En este apartado se detallan cifras sobre infracciones declaradas, pudiendo haberse declarado más de una infracción en cada resolución de procedimiento sancionador o de apercibimiento.

DISTRIBUCIÓN DE LAS ACTUACIONES PREVIAS INICIADAS

ACTIVIDAD	2013	2014	2015	% RELATIVO	Δ% 2014/2015
Telecomunicaciones	2.256	2.220	1.926	23,68	-13,24
Entidades financieras	1.566	1.540	1.729	21,26	12,27
Videovigilancia	918	966	1.157	14,23	19,77
Servicios de Internet (excepto spam)	424	447	427	5,25	-4,47
Publicidad y prospección comercial (excepto spam)	270	314	398	4,89	26,75
Comunicaciones electrónicas comerciales – spam (LSSI)	344	353	321	3,95	-9,07
Administración pública	360	311	292	3,59	-6,11
Suministro y comercialización de energía/agua	346	237	260	3,20	9,70
Comunidades propietarios, admón. fincas, otros profesionales	204	232	250	3,07	7,76
Sanidad	139	225	206	2,53	-8,44
Comercio, transporte, hostelería	162	145	189	2,32	30,34
Recursos humanos, asuntos laborales	160	147	177	2,18	20,41
Seguros	67	81	114	1,40	40,74
Organizaciones asociativas (excepto partidos políticos y sindicatos)	100	105	103	1,27	-1,90
Partidos políticos	40	56	88	1,08	57,14
Medios de comunicación	98	75	76	0,93	1,33
Inscripción de ficheros / Información artículo 5	94	101	74	0,91	-26,73
Seguridad privada	8	161	67	0,82	-58,39
Cookies (LSSI)	16	58	57	0,70	-1,72
Sindicatos	48	44	53	0,65	20,45
Fuerzas y cuerpos de seguridad	47	49	52	0,64	6,12
Enseñanza	50	53	47	0,58	-11,32
Asuntos relacionados con procedimientos judiciales	62	56	40	0,49	-28,57
Documentación desechada sin destruir o borrar	29	39	20	0,25	-48,72
Comunicaciones comerciales por fax (LGT)	9	16	2	0,02	-87,50
Otros	40	37	7	0,09	-81,08
TOTAL ACTUACIONES PREVIAS INICIADAS	7.857	8.068	8.132	100	0,79

NOTA: Las actuaciones previas incluyen: las actuaciones de investigación incoadas por denuncia o de oficio (EI), las solicitudes de documentación adicional que no son subsanadas por el denunciante (AT) y el análisis de denuncias que finalmente no se admiten a trámite (IT).

DISTRIBUCIÓN DE LOS PROCEDIMIENTOS SANCIONADORES RESUELTOS

ACTIVIDAD	2013	2014	2015	% RELATIVO	Δ% 2014/2015
Telecomunicaciones	377	310	270	38,96	-12,90
Entidades financieras	74	124	101	14,57	-18,55
Comunicaciones electrónicas comerciales – spam (LSSI)	67	75	89	12,84	18,67
Videovigilancia	57	39	51	7,36	30,77
Suministro y comercialización de energía/agua	54	63	47	6,78	-25,40
Servicios de Internet (excepto spam)	29	36	30	4,33	-16,67
Publicidad y prospección comercial (excepto spam)	24	32	24	3,46	-25
Comercio, transporte, hostelería	6	15	11	1,59	-26,67
Seguros	7	8	13	1,88	62,50
Seguridad privada	–	–	13	1,88	–
Sanidad	1	3	10	1,44	233,33
Documentación desechada sin destruir o borrar	–	3	7	1,01	–
Inscripción de ficheros / Información artículo 5	1	5	5	0,72	0
Comunicaciones comerciales por fax (LGT)	4	1	5	0,72	400
Cookies (LSSI)	–	19	4	0,58	-78,95
Organizaciones asociativas, excepto partidos políticos y sindicatos	5	4	4	0,58	0
Recursos humanos, asuntos laborales	2	7	4	0,58	-42,86
Comunidades propietarios, admón. fincas, otros profesionales	2	1	3	0,43	200
Partidos políticos	3	1	–	–	–
Otros	6	6	2	0,29	-66,67
TOTAL RESOLUCIONES (PS)	719	752	693	100	-7,85

* Se incluyen tanto las resoluciones declarativas de infracción como las de archivo del procedimiento.

**DISTRIBUCIÓN DE LOS PROCEDIMIENTOS
DE APERCIBIMIENTO RESUELTOS. SECTOR PRIVADO**

ACTIVIDAD	2013	2014	2015	% RELATIVO	Δ% 2014/2015
Videovigilancia	131	176	234	58,94	32,95
Comunicaciones electrónicas comerciales – <i>spam</i> (LSSI)	–	14	34	8,56	142,86
Servicios de Internet (excepto <i>spam</i>)	19	34	28	7,05	-17,65
Cookies (LSSI)	–	5	21	5,29	320
Comunidades propietarios, admón. fincas, otros profesionales	11	18	15	3,78	-16,67
Comercio, transporte, hostelería	13	8	11	2,77	37,50
Sanidad	4	4	11	2,77	175
Organizaciones asociativas, excepto partidos políticos y sindicatos	14	9	10	2,52	11,11
Documentación desechada sin destruir o borrar	4	12	8	2,02	-33,33
Partidos políticos	2	2	5	1,26	150
Sindicatos	–	–	4	1,01	–
Enseñanza	–	5	3	0,76	-40
Publicidad y prospección comercial (excepto <i>spam</i>)	5	5	3	0,76	-40
Recursos humanos, asuntos laborales	10	4	3	0,76	-25
Inscripción de ficheros / Información artículo 5	–	2	2	0,50	0
Otros	6	17	5	1,26	-54,55
TOTAL RESOLUCIONES (A)	219	315	397	100	26,03

* Se incluyen tanto las resoluciones de apercibimiento como las de archivo del procedimiento.

MEMORIA 2015

RESOLUCIONES DECLARATIVAS DE INFRACCIÓN. SECTOR PRIVADO

ACTIVIDAD	2013	2014	2015	% RELATIVO	Δ% 2013/2014
Telecomunicaciones	317	270	234	30,19	-13,33
Videovigilancia	176	158	158	20,39	0,00
Entidades financieras	62	98	91	11,74	-7,14
Comunicaciones electrónicas comerciales – spam (LSSI)	59	74	88	11,35	18,92
Suministro y comercialización de energía/agua	48	52	39	5,03	-25
Servicios de Internet (excepto spam)	44	50	35	4,52	-30
Publicidad y prospección comercial (excepto spam)	29	30	22	2,84	-26,67
Cookies	–	20	16	2,06	-20
Seguros	6	8	13	1,68	62,50
Comercio, transporte, hostelería	15	17	12	1,55	-29,41
Sanidad	5	3	11	1,42	266,67
Seguridad privada	–	–	11	1,42	–
Comunidades propietarios, admón. fincas, otros profesionales	11	8	10	1,29	25
Organizaciones asociativas, excepto partidos políticos y sindicatos	19	7	10	1,29	42,86
Documentación desechada sin destruir o borrar	4	3	6	0,77	100
Inscripción de ficheros / Información artículo 5 LGT (fax y otros)	1	5	5	0,65	0
Recursos humanos, asuntos laborales	10	9	3	0,39	-66,67
Enseñanza	0	2	2	0,26	0
Medios de comunicación	1	1	2	0,26	100
Sindicatos	–	–	2	0,26	–
Partidos políticos	5	3	–	–	–
Administración pública (entidades Derecho privado)	0	2	–	–	–
Otros	6	7	1	0,13	-85,71
TOTAL RESOLUCIONES DECL. INFRACCIÓN (PS, A)	822	827	775	100	-6,29

* En cada resolución de procedimiento sancionador o de apercibimiento puede haberse declarado más de una infracción.

SANCIONES ECONÓMICAS IMPUESTAS

	2012	2013	2014	2015	Δ% 2014/2015
TOTAL SANCIONES	21.054.656,02	22.339.440	17.002.622	13.712.621	-19,35

ÁREAS CON MAYOR IMPORTE GLOBAL DE SANCIONES

ACTIVIDAD	2012	2013	2014	2015	% RELATIVO DEL TOTAL 2015	Δ% 2014/2015
Telecomunicaciones	15.368.938	15.035.008	10.750.502	7.090.004	51,70	-34,05
Entidades financieras	2.853.004	1.811.501	2.018.501	2.395.902	17,47	18,70
Suministro y comercialización de energía/agua	1.270.001	2.084.901	1.862.900	1.205.002	8,79	-35,32
Comunicaciones electrónicas comerciales – <i>spam</i> (LSSI)	541.507	526.010	645.506	897.403	6,54	39,02
Organizaciones asociativas incluyendo partidos políticos y sindicatos	147.202	40.400	19.800	525.500	3,83	2.554,04*
Publicidad (excepto <i>spam</i>)	137.000	481.004	751.411	502.108	3,66	-33,18
TOTAL DE LAS 6 PRIMERAS ACTIVIDADES	20.317.652	19.978.824	16.048.620	12.615.919	92	-21,39

* El incremento obedece a la tramitación de un procedimiento sancionador en el que se impusieron sanciones con un importe total de 440.000 euros.

MEMORIA 2015

PROCEDIMIENTOS DE INFRACCIÓN DE LAS ADMINISTRACIONES PÚBLICAS RESUELTOS

TIPO ADMINISTRACIÓN	2013	2014	2015	% RELATIVO	Δ% 2014/2015
Local	28	32	38	48,72	18,75
Autonómica	20	12	25	32,05	108,33
General del Estado	9	14	12	15,38	-14,29
Otras Entidades de Derecho Público	1	2	3	3,85	50
TOTAL RESOLUCIONES	58	60	78	100	30

* En un mismo procedimiento de infracción pueden figurar investigados de distintas administraciones territoriales, computándose tales procedimientos en una sola de las administraciones afectadas.

** Se incluyen tanto las resoluciones que declaran infracción como las de archivo del procedimiento.

INFRACCIONES DECLARADAS DE LAS ADMINISTRACIONES PÚBLICAS

TIPO ADMINISTRACIÓN	2013	2014	2015	% RELATIVO	Δ% 2014/2015
Local	26	27	32	56,14	18,52
Autonómica	21	12	17	29,82	41,67
General del Estado	9	11	7	12,28	-36,36
Otras Entidades de Derecho Público	1	1	1	1,75	0
TOTAL INFRACCIONES	57	51	57	100	11,76

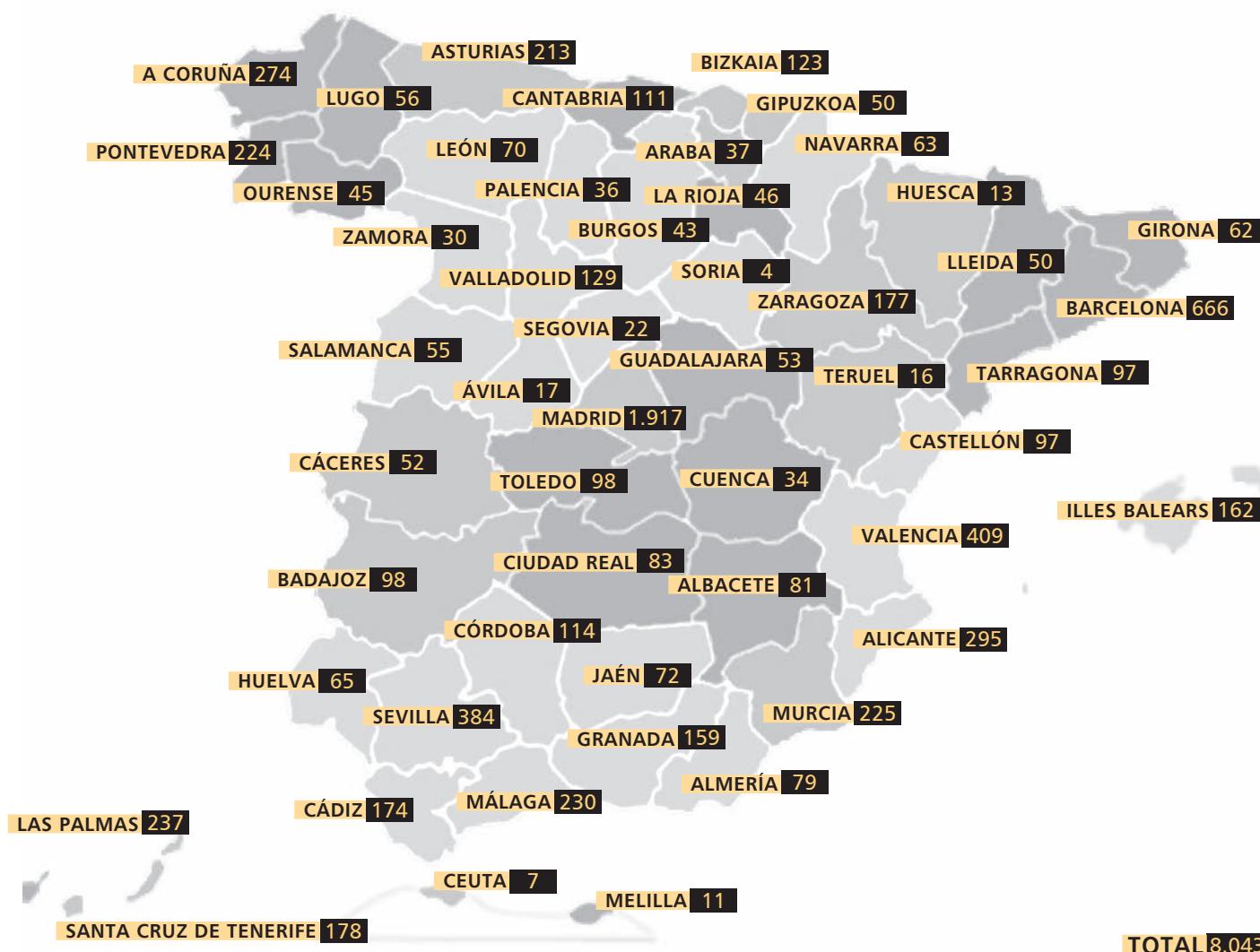
* En cada resolución puede haberse declarado más de una infracción.

PROCEDIMIENTOS DE TUTELA DE DERECHOS RESUELTOS

	ESTIMATORIA	ESTIMATORIA FORMAL O PARCIAL	DESESTIMATORIA	ARCHIVO POR INADMISIÓN O DESISTIMIENTO	TOTAL
Cancelación	274	92	217	746	1.329
Acceso	145	135	99	229	608
Rectificación	17	14	12	54	97
Oposición/exclusión	32	11	19	68	130
TOTAL	468	252	347	1.097	2.164

* En cada procedimiento resuelto puede haberse tutelado más de un derecho ARCO.

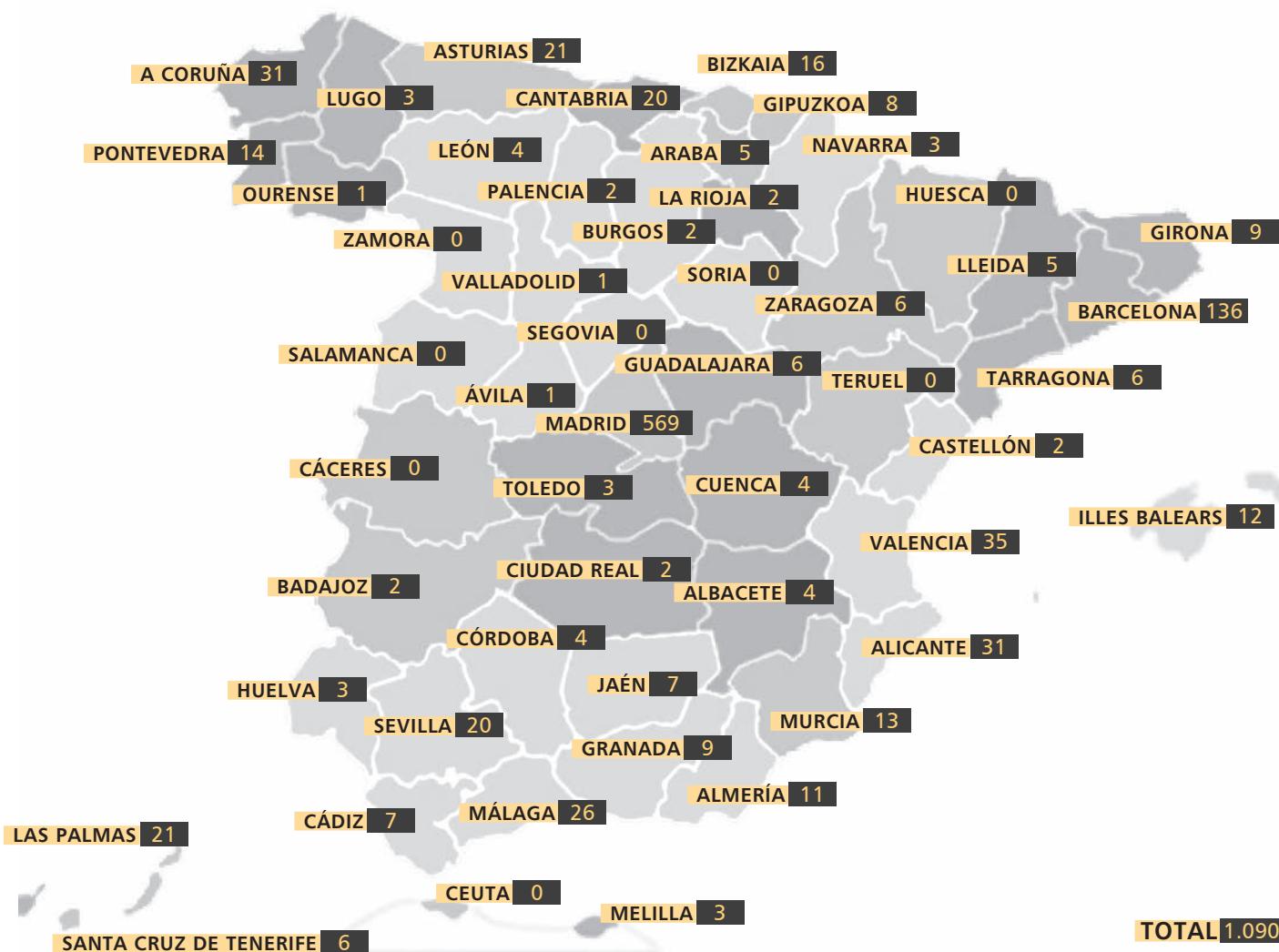
**DISTRIBUCIÓN GEOGRÁFICA DE LAS ACTUACIONES PREVIAS INICIADAS EN 2015
(PROVINCIA DEL DENUNCIANTE)**

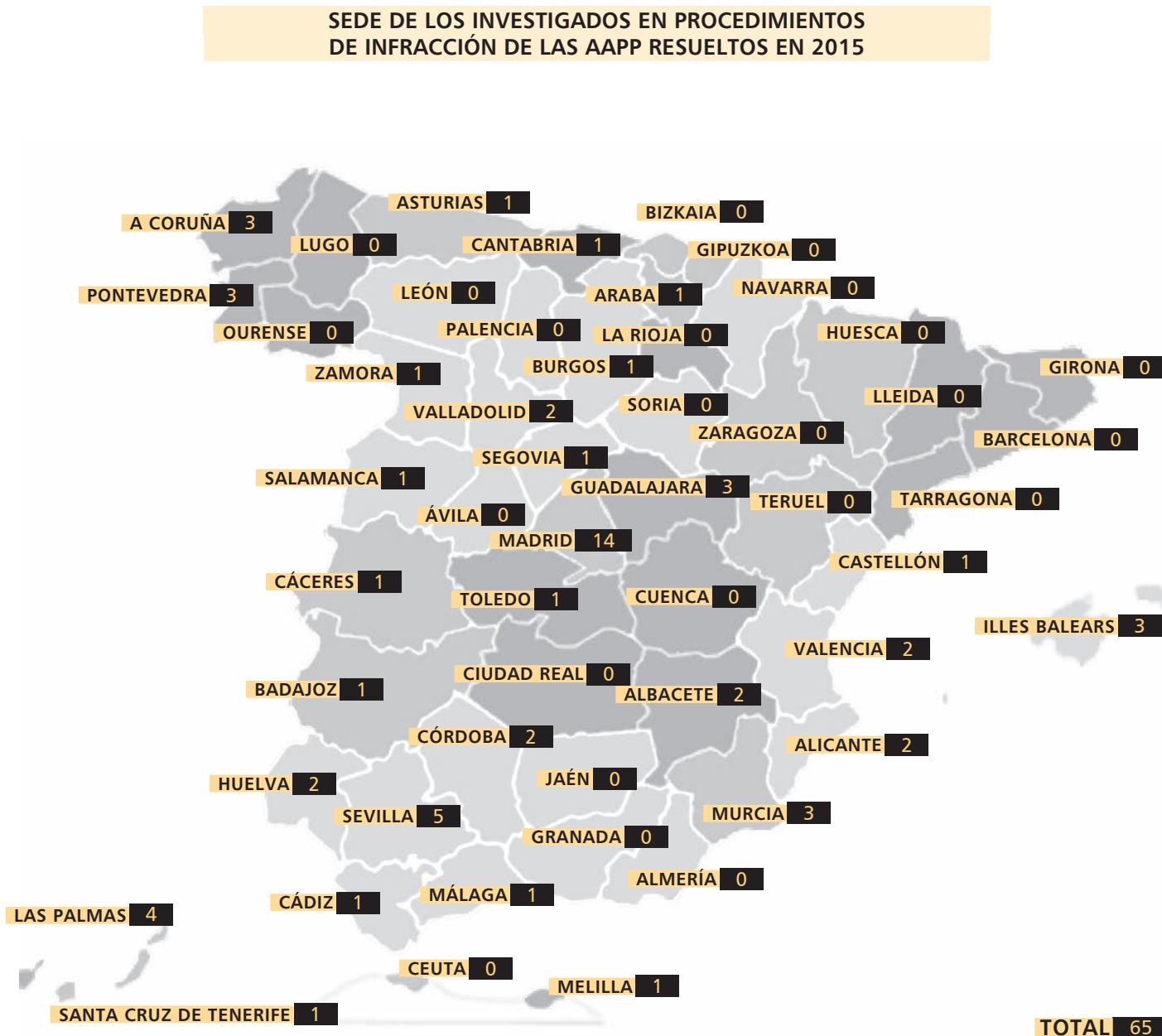


* Se incluyen denuncias archivadas sin actuaciones (expedientes IT), denuncias no subsanadas (AT) y expedientes de investigación previa (EI).

** No se consideran las actuaciones previas iniciadas de oficio a iniciativa de la dirección o las iniciadas por solicitud de colaboración de otras autoridades de protección de datos.

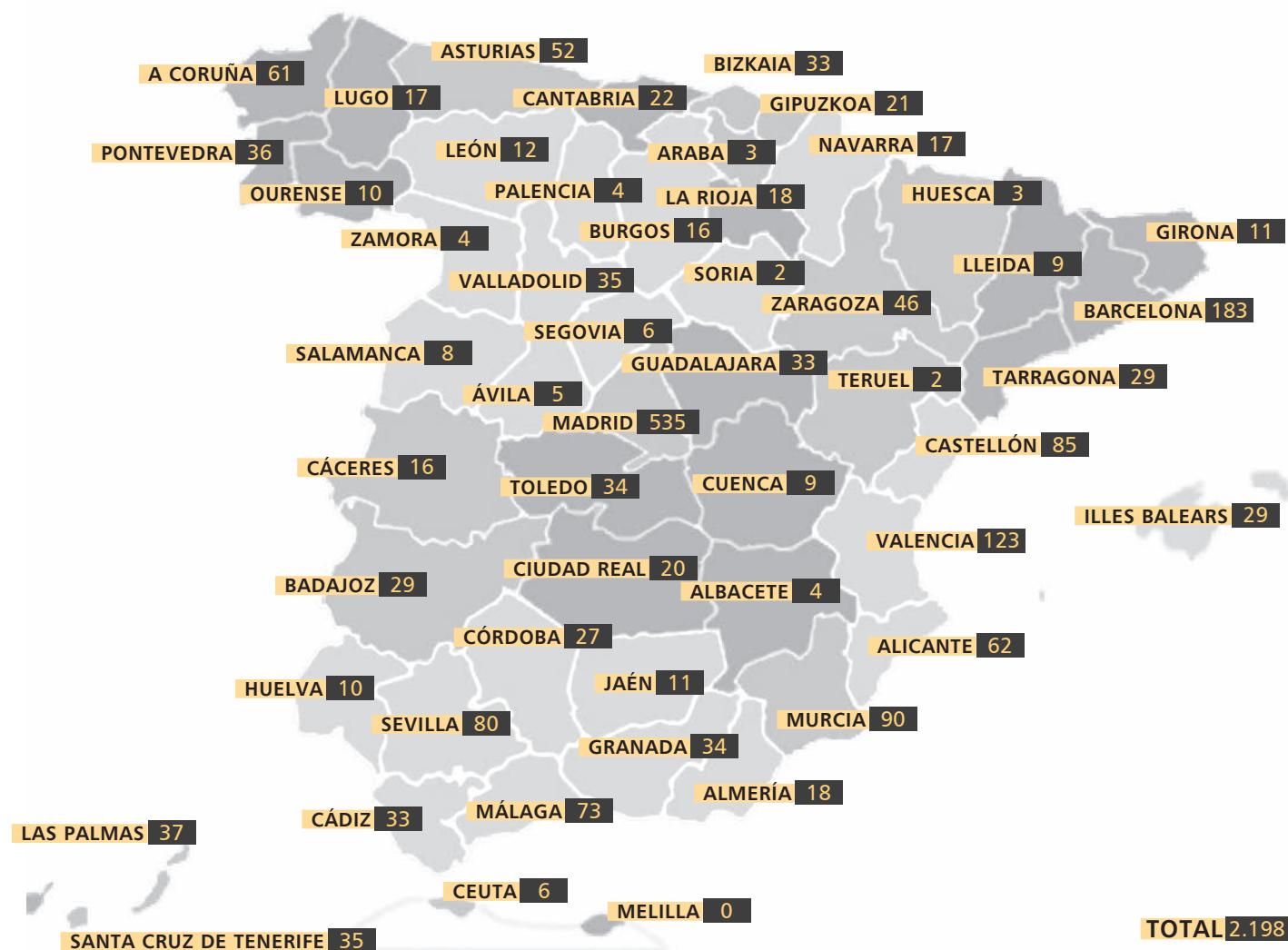
ESTABLECIMIENTO DE INVESTIGADOS EN PROCEDIMIENTOS SANCIONADORES Y DE APERCIBIMIENTO RESUELTO EN 2015





MEMORIA 2015

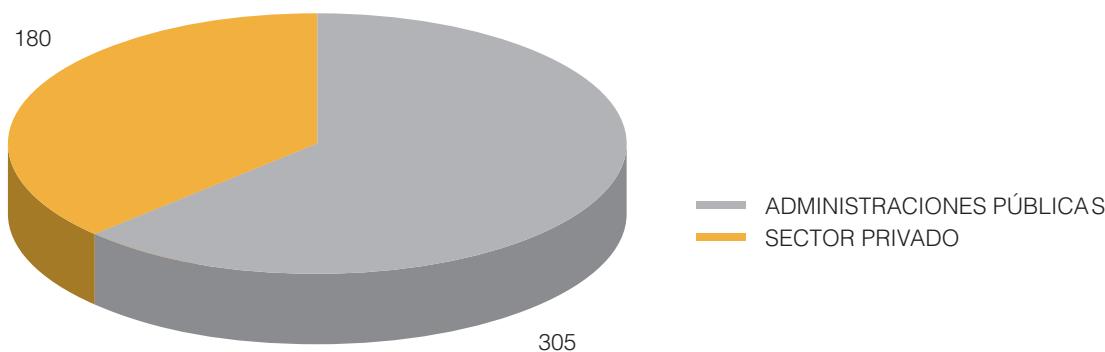
DISTRIBUCIÓN GEOGRÁFICA DE LOS PROCEDIMIENTOS DE TUTELA DE DERECHOS INICIADOS EN 2015 (PROVINCIA DEL RECLAMANTE)



CONSULTAS

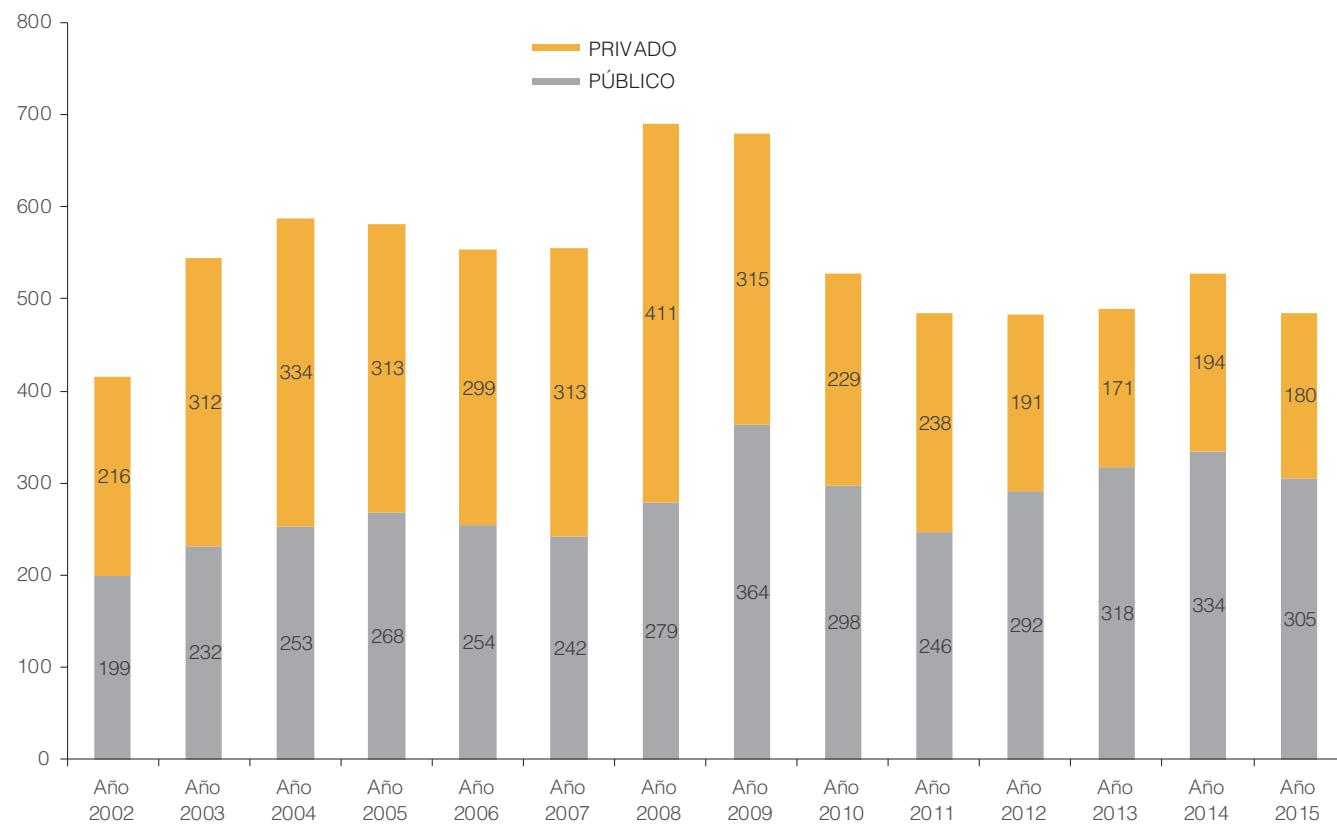
ADMINISTRACIONES PÚBLICAS		305
Administración general del Estado		141
Comunidades Autónomas		72
Entidades Locales		49
Otros Organismos Públicos		43
CONSULTAS PRIVADAS		180
Empresas		103
Particulares		49
Asociaciones/Fundaciones		21
Sindicatos/Partidos políticos		7
TOTAL		485

DISTRIBUCIÓN 2015 DE CONSULTAS PÚBLICAS/PRIVADAS

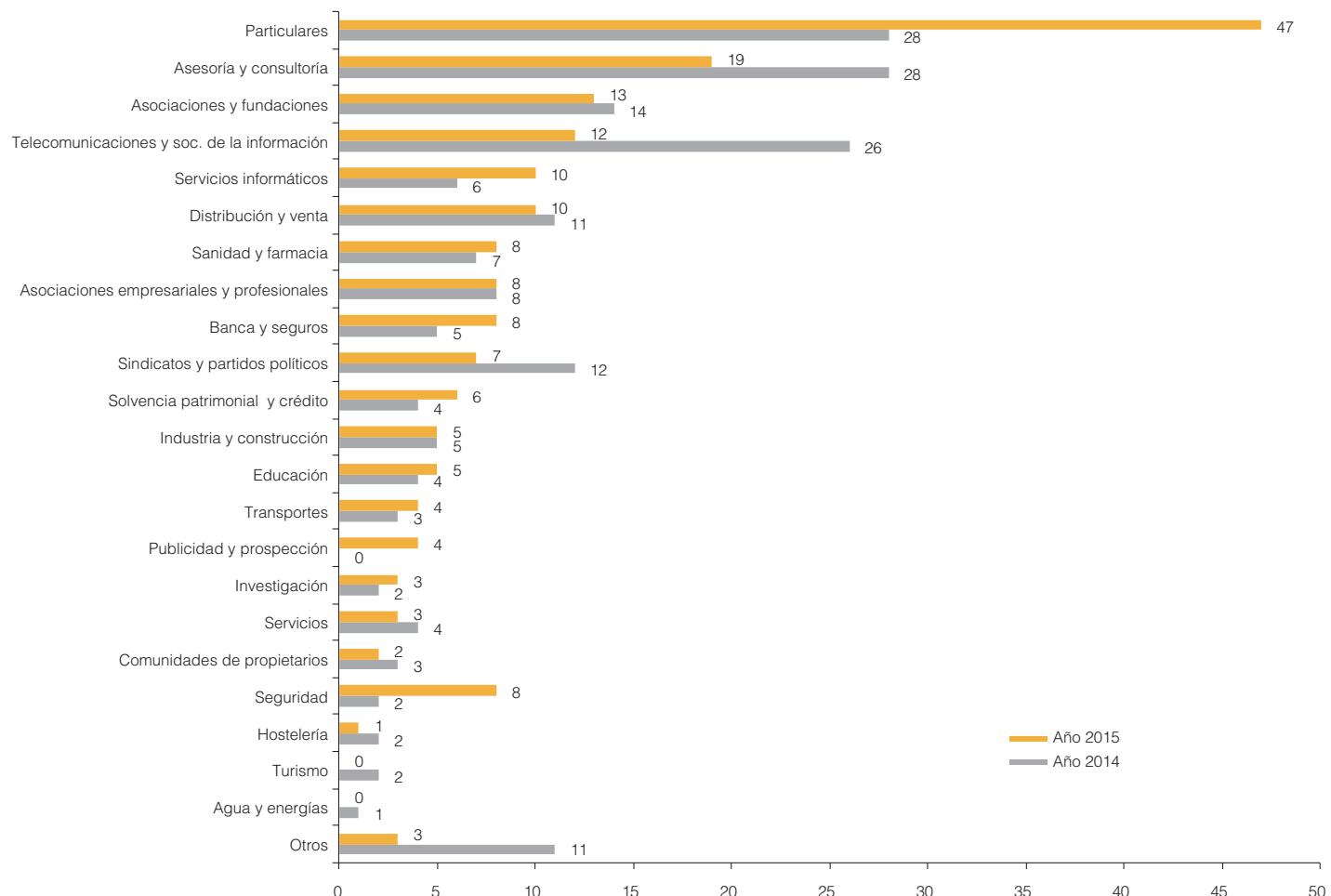


MEMORIA 2015

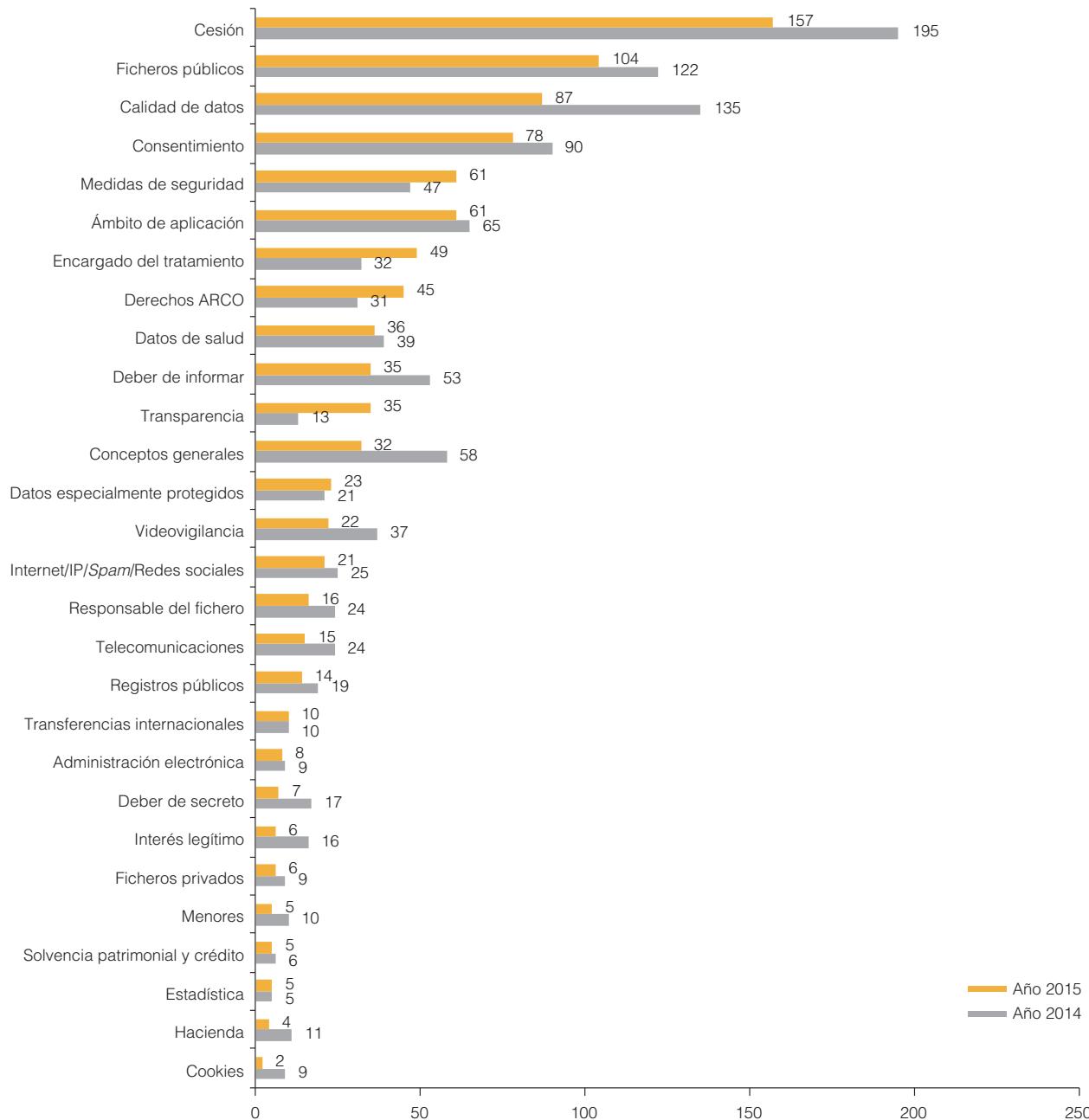
EVOLUCIÓN DE LAS CONSULTAS (2002-2015)



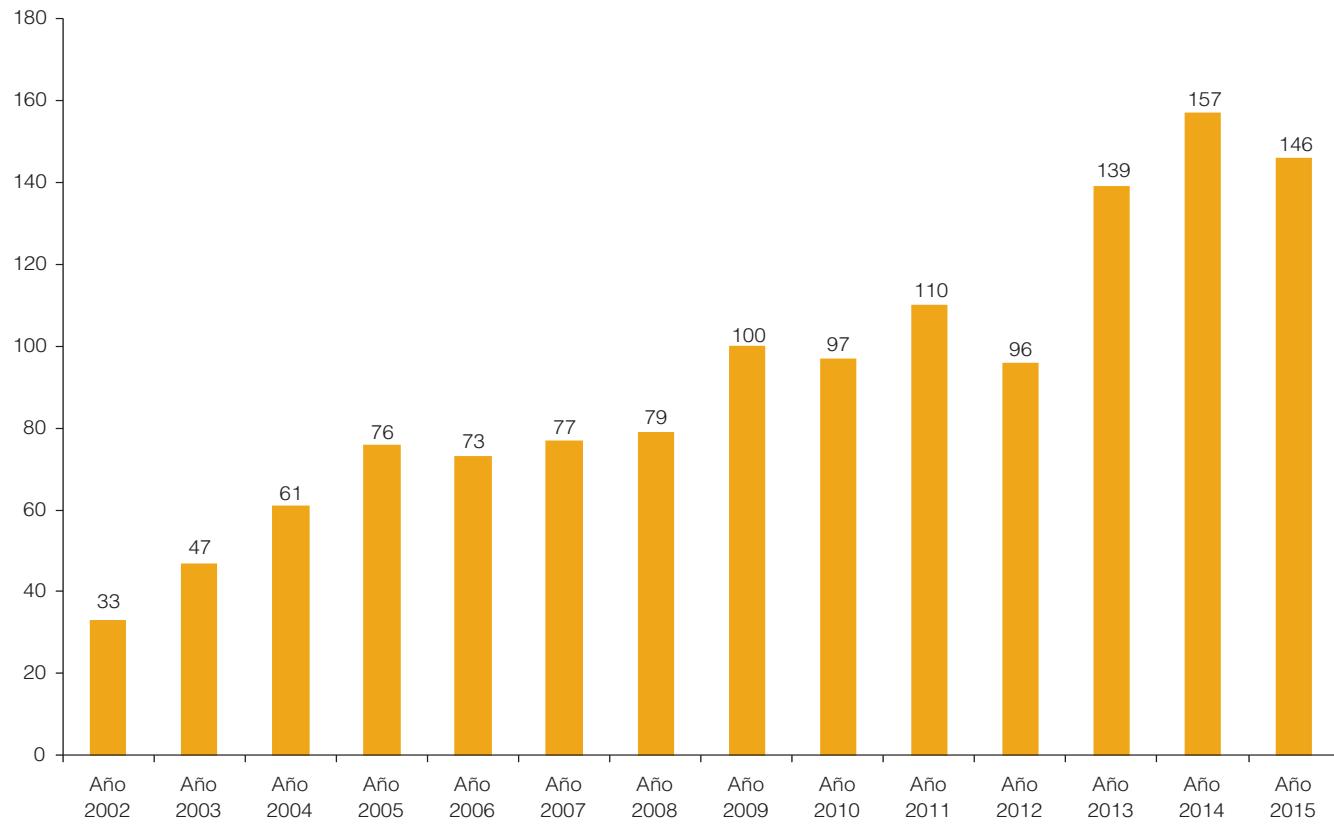
EVOLUCIÓN DE CONSULTAS POR SECTORES (2014-2015)



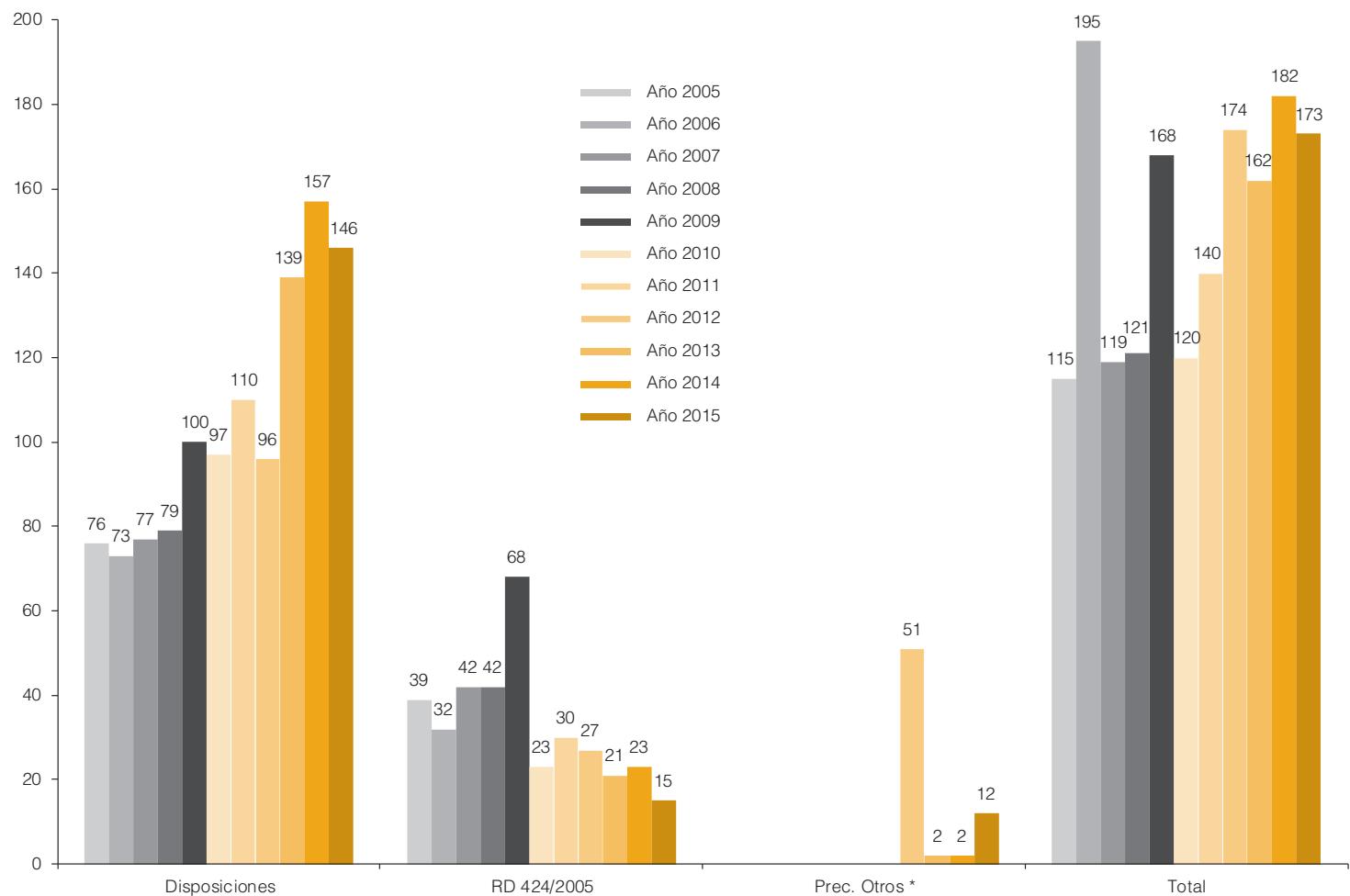
EVOLUCIÓN CONSULTAS POR MATERIAS (2014-2015)



EVOLUCIÓN DE INFORMES PRECEPTIVOS A DISPOSICIONES GENERALES (2002-2015)

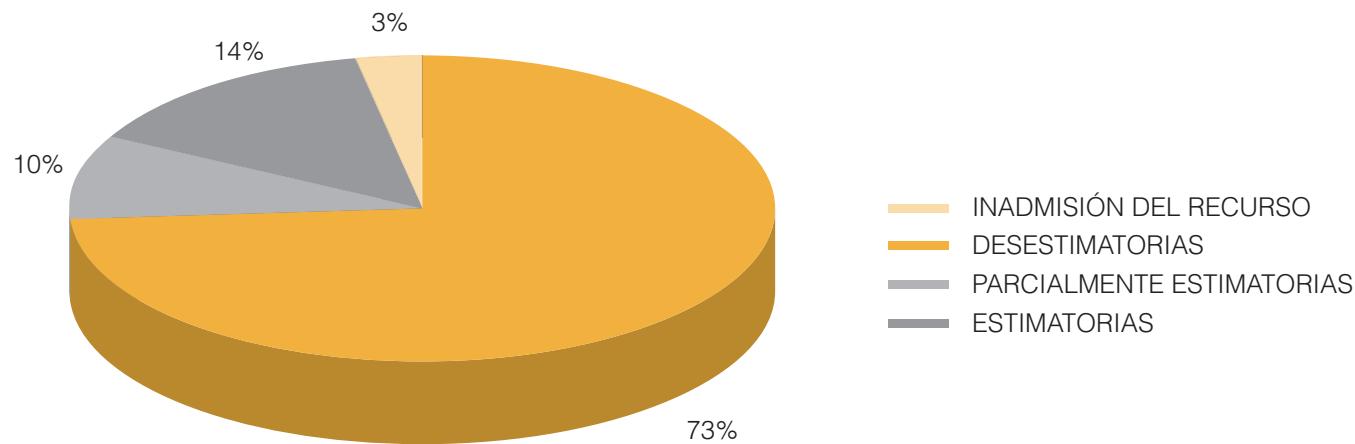


EVOLUCIÓN DE INFORMES PRECEPTIVOS (2005-2015)



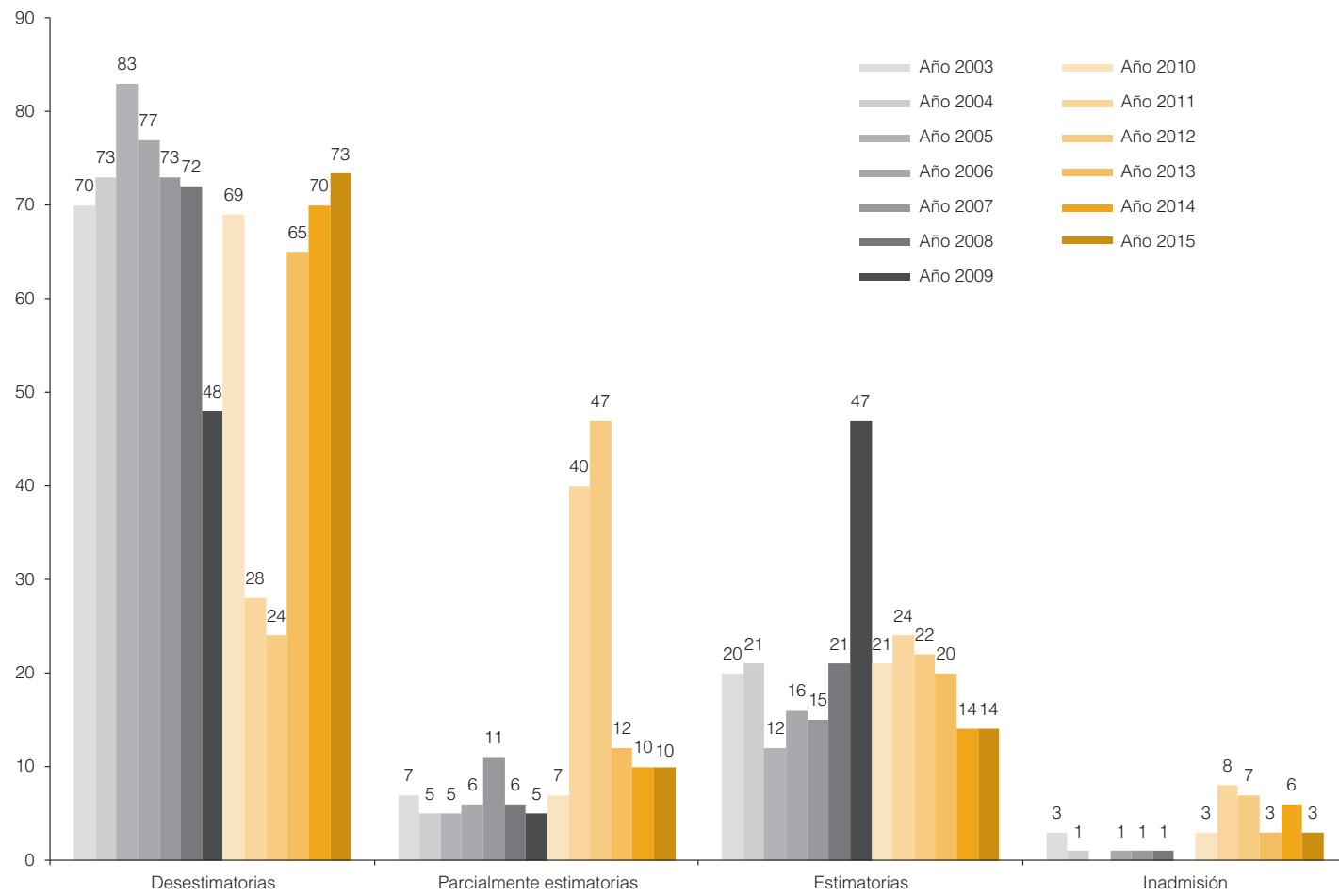
* Derivados de la Ley de Regulación del juego y la Ley de Prevención del blanqueo de capitales y de la financiación del terrorismo.

SENTENCIAS DE LA AUDIENCIA NACIONAL 2015

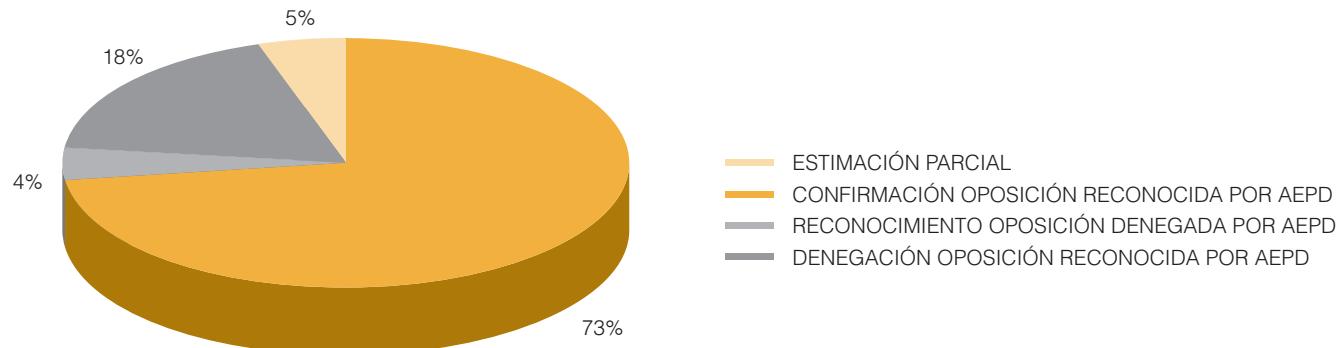


2

EVOLUCIÓN DEL SENTIDO DE FALLO EN PORCENTAJES (2003-2015)

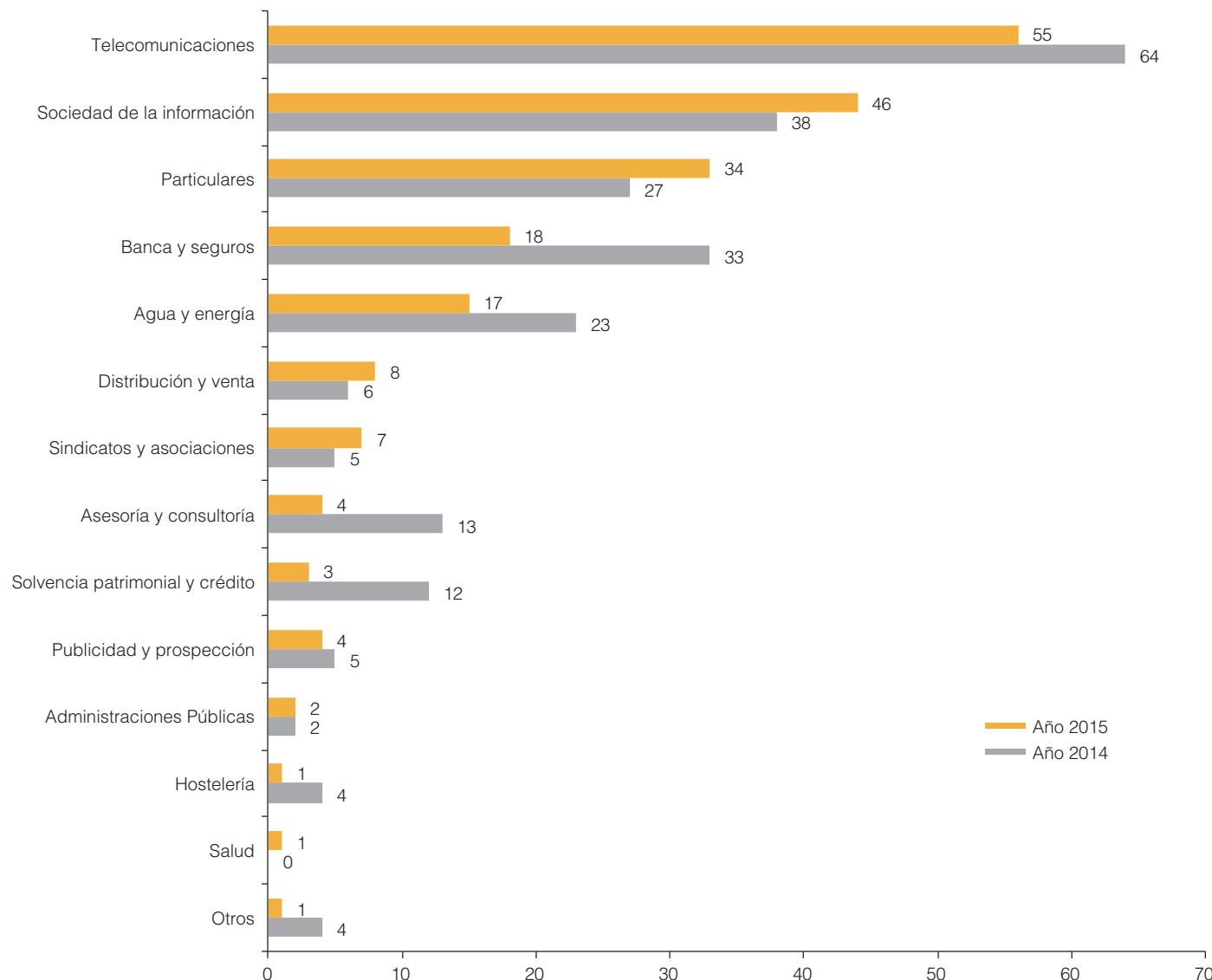


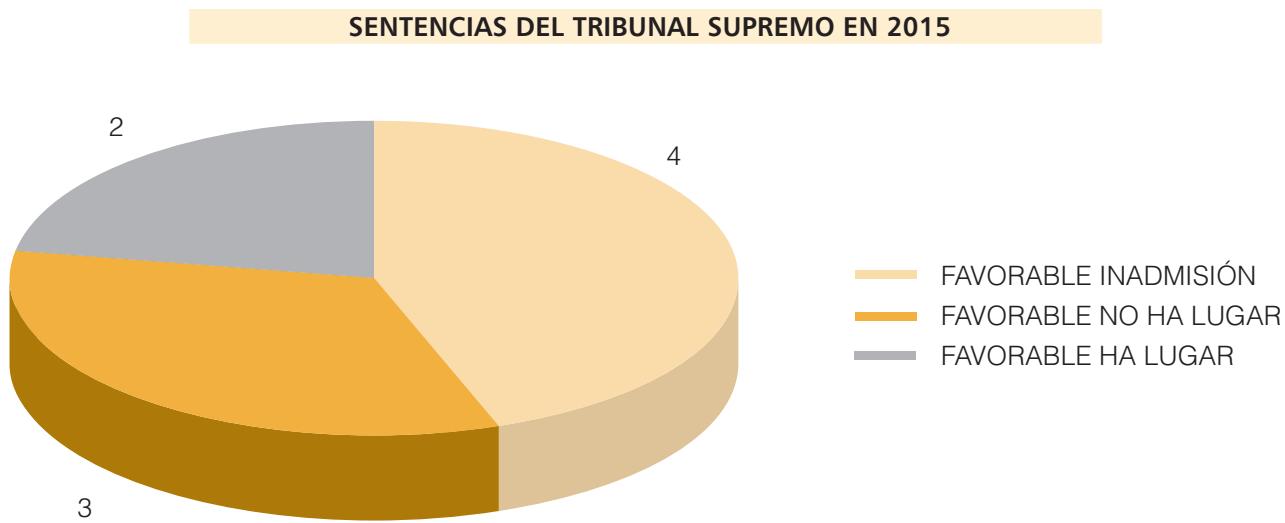
SENTENCIAS AUDIENCIA NACIONAL SOBRE 'DERECHO AL OLVIDO'



* Este gráfico no incluye los 136 casos en los que un motor de búsqueda desistió del recurso presentado.

COMPARATIVA POR SECTOR DEL RECURRENTE (2014-2015)





2

CONSULTAS TOTALES PLANTEADAS ANTE EL ÁREA DE ATENCIÓN AL CIUDADANO

	Atención presencial	Atención telefónica	Atención por escrito	Atención por sede electrónica	Respuesta automática - FAQs	TOTAL
AÑO 2013	3.817	92.942	668	4.637	105.092	207.156
AÑO 2014	3.361	89.868	592	5.703	97.854	197.378
AÑO 2015	3.767	74.260	550	7.054	132.704	218.335
% INCREMENTO	12,08	-17,37	-7,09	23,69	35,61	10,62

COMPARATIVA DE VISITAS A LA WEB (www.agpd.es)

AÑO	2013	2014	2015
Visitas	4.985.648	5.706.488	4.952.945
Promedio diario	6.842	7.816	6.766

ACCESOS AL PORTAL DE VÍDEOS 'PROTEGE TUS DATOS EN INTERNET'

Accesos al canal	32.396
Visualizaciones de vídeos	43.330*

*Se puede acceder a los vídeos directamente sin pasar por el canal, entrando desde la web www.tudecideseninternet.es.

ACCESOS AL PORTAL 'TÚ DECIDES'

VISITANTES DISTINTOS*	NÚMERO DE VISITAS**
28.606	51.998

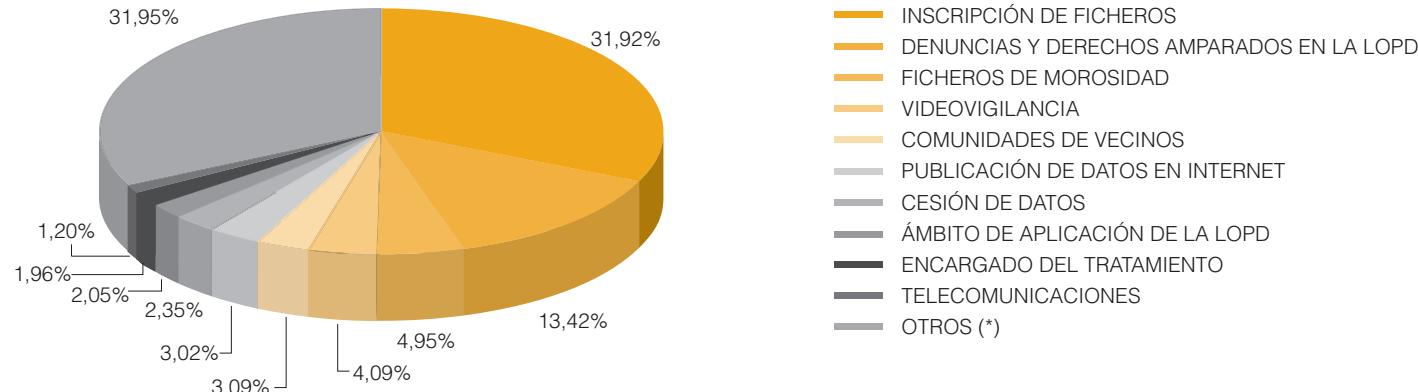
* Visitantes distintos: se refiere a una visita que ha solicitado al menos una página. Si este visitante ingresa numerosas veces, solo contará como una.

** Visitas: número de visitas realizadas por todos los visitantes. Si cada visitante tiene una sesión, cada visita que realice aumentará este contador.

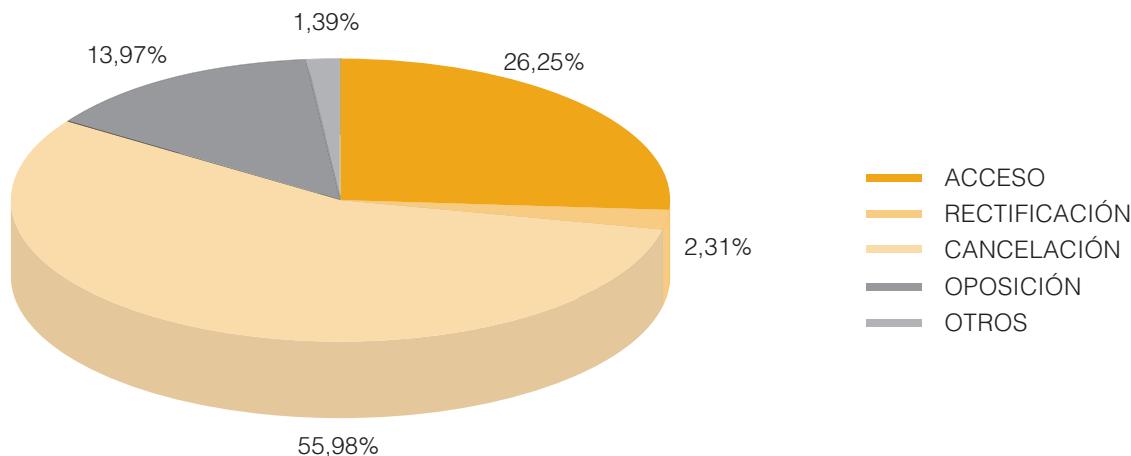
TEMAS MÁS CONSULTADOS EN EL CATÁLOGO DE PREGUNTAS FRECUENTES

ORDEN	TEMA DE CONSULTA	ACCESOS
1	Ficheros de morosos y recobro de deudas	16.059
2	Inscripción, modificación y supresión de ficheros	13.442
3	Ámbito de aplicación de la LOPD	12.874
4	Videocámaras	9.428
5	Comunidades de vecinos	9.303
6	Obligaciones de los responsables de los ficheros	9.080
7	Denuncias/reclamaciones	6.841
8	Cuestiones técnicas de la sede electrónica	6.164
9	Publicación de datos en Internet	4.777
10	Niveles de seguridad	2.720

TEMAS MÁS CONSULTADOS EN ATENCIÓN PRESENCIAL Y TELEFÓNICA



* Incluye temas como medidas de seguridad, información general sobre la LOPD y sobre la AEPD (direcciones, teléfonos, horarios, etc.).



EVOLUCIÓN DEL REGISTRO DE ENTRADA / SALIDA DE DOCUMENTOS

	2013	2014	2015
ENTRADA	527.022	520.286	506.670
SALIDA	346.597	346.694	328.830
TOTAL	873.619	866.980	835.500

DISTRIBUCIÓN DE LOS DOCUMENTOS REGISTRADOS EN 2015 SEGÚN EL MEDIO UTILIZADO

REGISTRO DE ENTRADAS	2015	%
Por medios electrónicos	473.854	93,53
<i>Con certificado electrónico</i>	240.041	
<i>Sin certificado electrónico</i>	233.813	
Por otros medios *	32.816	6,47
TOTAL ENTRADAS	506.670	100,00

REGISTRO DE SALIDAS	2015	%
Por medios electrónicos	53.537	16,28
<i>Comparecencia en sede</i>	5.468	
<i>Dirección Electrónica Habilitada</i>	40.629	
<i>Otros medios electrónicos</i>	7.440	
Por otros medios *	275.293	83,72
TOTAL SALIDAS	328.830	100,00

* Correo postal, en mano, mensajero, etc.

MEMORIA 2015

USO DE MEDIOS ELECTRÓNICOS EN LA PRESENTACIÓN DE DOCUMENTOS

TIPO DE PROCEDIMIENTO	2013	2014	2015	% (2014-15)
Entradas con certificado de firma electrónica	7.618	8.051	10.863	34,93
Entradas sin certificado de firma electrónica	11.509	14.240	16.273	14,28
TOTAL	19.127	22.291	27.136	21,74

SOLICITUDES DE ACCESO A INFORMACIÓN PÚBLICA

RECIBIDAS	INADMITIDAS *	CONCEDIDAS	DESISTIMIENTO
54	17	35	2

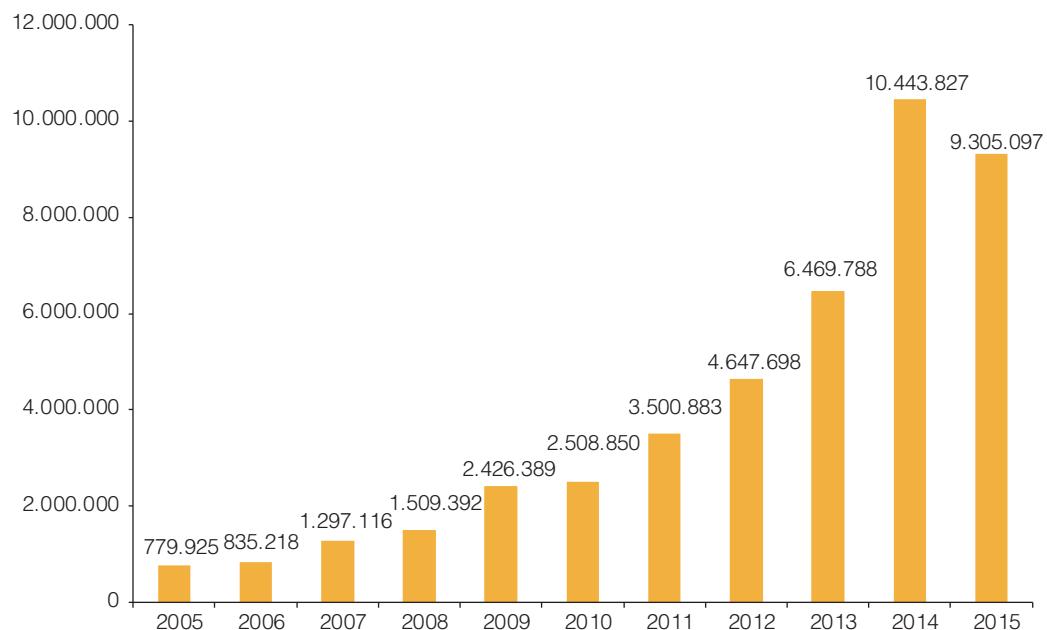
* Causas de inadmisión (Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno):
18.1 a) información en curso de elaboración o de publicación general (1 solicitud)
18.1 e) repetitiva o de carácter abusivo (9 solicitudes)
Disposición adicional 1.^a 2 regida por su normativa específica (7 solicitudes)

CONTENIDOS ELECTRÓNICOS

	2015
Accesos web	4.952.945
Accesos a la sección Transparencia	503.075
Denuncias recibidas	8.489
Reclamaciones de tutela recibidas	2.066
Consultas FAQs	132.704
Consultas electrónicas de ciudadanos	7.054
NOTA. Notificación de ficheros a la Agencia	449.632
Solicitud de copias de contenido de ficheros	13.279
Test Evalúa LOPD	4.901
Test Evalúa Medidas de seguridad	1.986
Accesos DISPONE	4.780
Consulta y/o descarga de la Guía de seguridad	16.572
Descarga del modelo de documento de seguridad	25.898
Guía del ciudadano	108.041
Guía del responsable	10.403
Guías de videovigilancia	45.247
Guía de relaciones laborales	97.428
Guía para clientes que contraten servicios de <i>cloud computing</i>	144.720
Orientaciones para prestadores de servicios de <i>cloud computing</i>	22.965
Guía sobre el uso de las cookies	497.747
Guía RFID	63.533
Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)	111.017
Documentos Plan estratégico AEPD 2015-2019 (noviembre 2015)	2.149
Inspección sectorial de oficio sobre servicios de <i>cloud computing</i> en el sector educativo (julio 2015)	3.432

DERECHO DE CONSULTA AL REGISTRO

TITULARIDAD	2014	2015
Privada	4.484.549	6.804.638
Pública	5.959.278	2.500.459
TOTAL	10.443.827	9.305.097

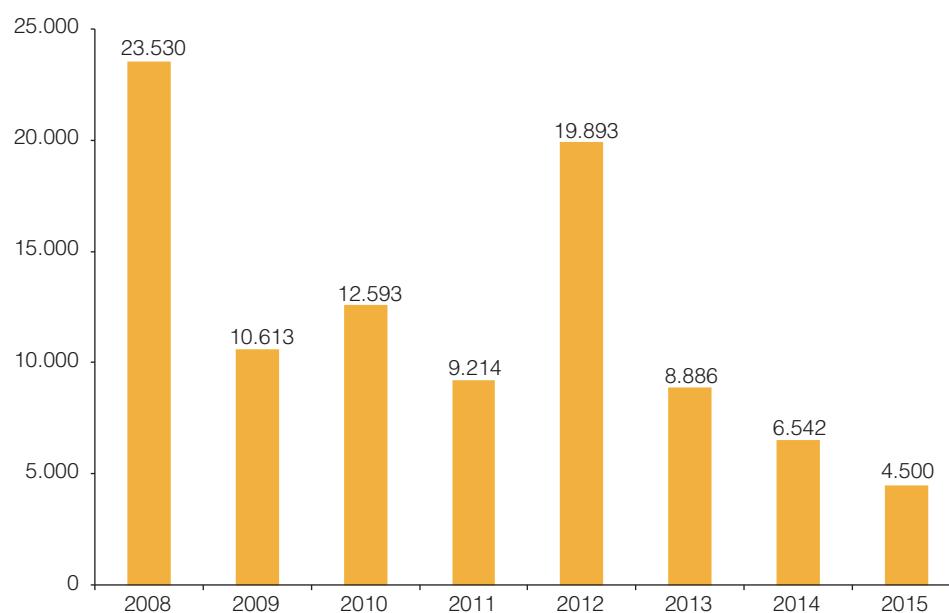


4

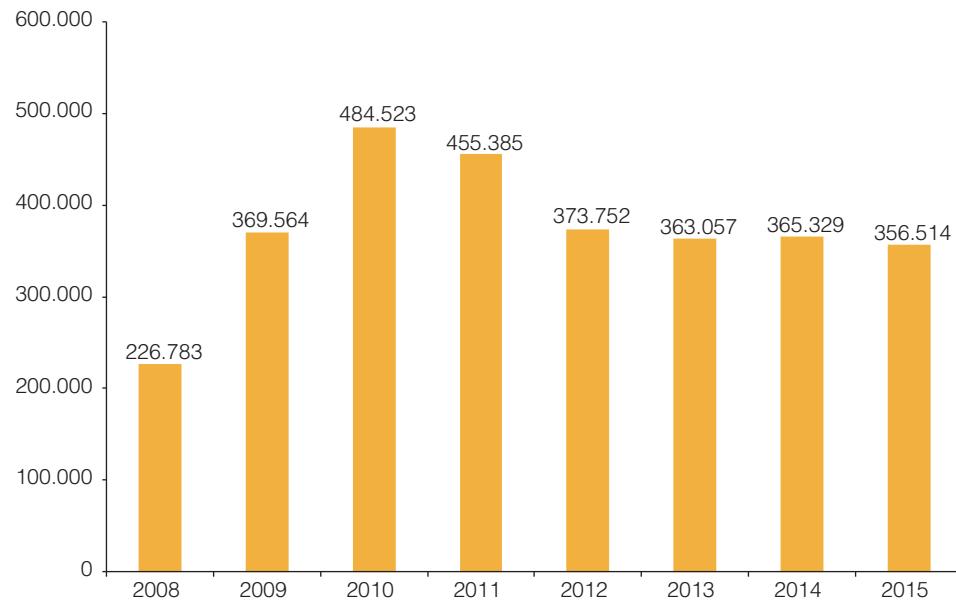
EVOLUCIÓN DE LA INSCRIPCIÓN DE FICHEROS EN EL RGPD

A 31 DE DIC.	2008	2009	2010	2011	2012	2013	2014	2015
Tit. Pública	85.083	95.696	108.289	117.503	137.396	146.282	152.824	157.324
Tit. Privada	1.182.496	1.552.060	2.036.583	2.491.968	2.865.720	3.228.777	3.594.106	3.950.620
TOTAL	1.267.579	1.647.756	2.144.872	2.609.471	3.003.116	3.375.059	3.746.930	4.107.944

INCREMENTO ANUAL DE FICHEROS TITULARIDAD PÚBLICA



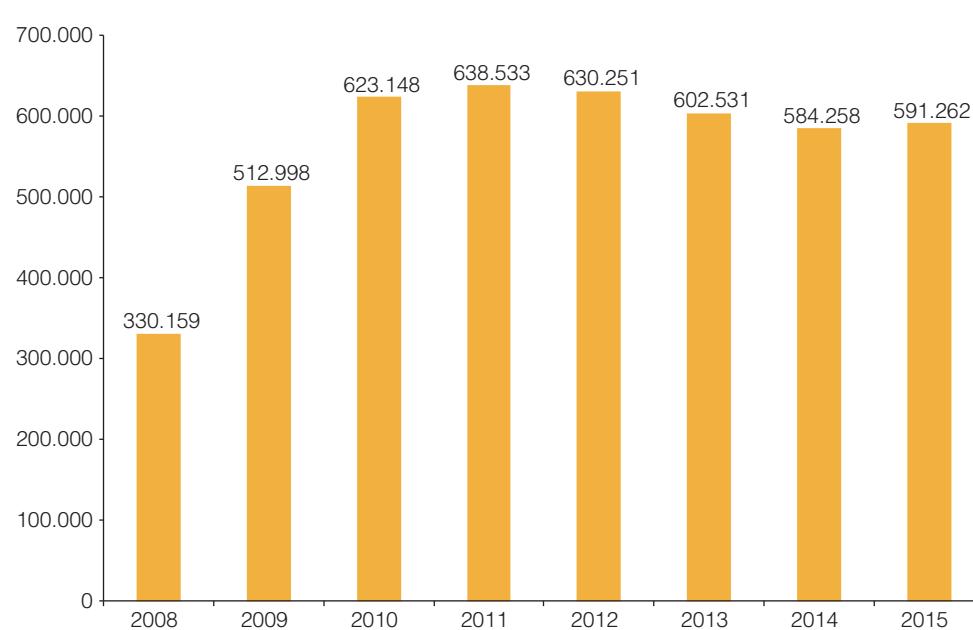
INCREMENTO ANUAL DE FICHEROS TITULARIDAD PRIVADA



OPERACIONES DE INSCRIPCIÓN

	2014	2015	MEDIA DIARIA EN 2014	MEDIA DIARIA EN 2015
Operaciones de inscripción	584.258	591.262	2.434	2.464
Total de ficheros inscritos	3.746.930	4.107.944	1.549	1.504

EVOLUCIÓN ANUAL DE LAS OPERACIONES DE INSCRIPCIÓN



MEMORIA 2015

INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN TERRITORIAL DE FICHEROS	RESPONSABLES		FICHEROS	
	2015	TOTAL	2015	TOTAL
Comunidad Autónoma de Andalucía	34.054	202.795	84.810	623.995
Almería	3.478	18.995	8.731	61.795
Cádiz	5.011	25.696	13.532	79.834
Córdoba	3.097	18.622	7.197	57.601
Granada	4.256	26.954	10.896	87.068
Huelva	1.333	8.800	3.112	26.155
Jaén	2.393	15.430	6.168	52.415
Málaga	7.837	46.410	20.887	140.787
Sevilla	6.683	42.721	14.287	118.340
Comunidad Autónoma de Aragón	5.438	45.737	11.410	114.332
Huesca	878	8.749	1.821	21.133
Teruel	610	4.102	1.486	11.245
Zaragoza	3.950	32.948	8.103	81.954
Comunidad Autónoma del Principado de Asturias	6.159	41.521	15.429	124.861
Comunidad Autónoma de Canarias	7.323	43.637	16.987	141.784
Las Palmas	3.614	20.730	9.138	68.758
Santa Cruz de Tenerife	3.714	22.987	7.849	73.026
Comunidad Autónoma de Cantabria	2.970	16.776	5.902	43.655
Comunidad Autónoma de Castilla y León	9.421	69.131	21.480	193.019
Ávila	540	4.480	1.226	11.335
Burgos	1.252	10.719	2.463	26.412
León	1.866	13.110	4.122	36.230
Palencia	688	5.064	1.595	14.740
Salamanca	980	8.544	2.304	23.170
Segovia	969	5.797	2.915	18.488

DISTRIBUCIÓN TERRITORIAL DE FICHEROS	RESPONSABLES		FICHEROS	
	2015	TOTAL	2015	TOTAL
Soria	406	2.935	781	8.333
Valladolid	1.823	14.237	4.358	40.530
Zamora	902	4.404	1.716	13.781
Comunidad Autónoma de Castilla-La Mancha	8.112	50.636	18.648	151.218
Albacete	2.562	13.205	5.190	41.078
Ciudad Real	1.884	11.634	4.336	35.487
Cuenca	693	4.962	1.800	13.942
Guadalajara	827	5.583	1.921	14.856
Toledo	2.151	15.340	5.401	45.855
Comunidad Autónoma de Cataluña	30.682	251.793	72.403	671.431
Barcelona	23.589	187.807	53.692	492.829
Girona	2.513	29.105	6.983	80.550
Lleida	1.464	12.959	3.788	33.883
Tarragona	3.129	22.329	7.940	64.169
Comunidad de Madrid	36.772	231.764	83.925	606.274
Comunitat Valenciana	26.170	165.478	60.695	451.117
Alicante / Alacant	10.048	58.654	24.899	155.655
Castellón / Castelló	2.762	19.088	6.210	54.235
Valencia / València	13.373	87.917	29.586	241.227
Comunidad Autónoma de Extremadura	3.153	24.275	7.483	71.271
Badajoz	2.022	15.161	4.629	44.377
Cáceres	1.132	9.150	2.854	26.894
Comunidad Autónoma de Galicia	15.056	98.537	30.333	280.935
A Coruña	6.725	43.221	13.782	122.167
Lugo	1.650	12.465	3.420	34.457
Ourense	1.533	10.612	2.875	28.620
Pontevedra	5.158	32.485	10.256	95.691

MEMORIA 2015

DISTRIBUCIÓN TERRITORIAL DE FICHEROS	RESPONSABLES		FICHEROS	
	2015	TOTAL	2015	TOTAL
Comunidad Autónoma de las Illes Balears	5.634	32.313	15.299	113.835
Comunidad Foral de Navarra	2.091	15.342	5.142	45.396
Comunidad Autónoma del País Vasco	9.167	57.900	20.166	158.304
Araba / Álava	1.222	8.044	2.513	20.884
Gipuzkoa	2.717	18.289	7.253	53.948
Bizkaia	5.232	31.665	10.400	83.472
Comunidad Autónoma de La Rioja	1.277	12.006	2.696	30.924
Comunidad Autónoma de la Región de Murcia	7.132	43.188	16.110	120.743
Ciudad Autónoma de Ceuta	148	924	363	2.531
Ciudad Autónoma de Melilla	148	947	454	4.694

INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN DE FICHEROS SEGÚN TIPOS DE DATOS	2015	TOTAL
Datos especialmente protegidos (ideología, creencias, religión y afiliación sindical)	5.206	87.534
Otros datos especialmente protegidos (origen racial, salud y vida sexual)	33.798	434.887
Datos de carácter identificativo	413.313	3.950.620
Datos de características personales	170.621	1.763.424
Datos de circunstancias sociales	113.644	1.044.820
Datos académicos y profesionales	94.516	995.852
Detalles de empleo y carrera administrativa	104.462	1.199.646
Datos de información comercial	116.340	1.117.600
Datos económico-financieros	220.079	2.232.957
Datos de transacciones	163.604	1.672.304
Otros tipos de datos	21.910	177.812

INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN DE FICHEROS SEGÚN SU FINALIDAD	2015	TOTAL	2014-2015 % VARIACIÓN
Gestión de clientes, contable, fiscal y administrativa	221.536	2.309.864	+9,59
Recursos humanos	81.109	881.850	+9,20
Gestión de nóminas	56.347	650.004	+8,67
Publicidad y prospección comercial	53.361	359.381	+14,85
Videovigilancia	41.492	243.388	+17,05
Prevención de riesgos laborales	40.253	351.224	+11,46
Comercio electrónico	24.821	124.131	+20,00
Gestión y control sanitario	14.434	156.402	+9,23
Historial clínico	10.321	111.310	+9,27
Seguridad y control de acceso a edificios	10.252	65.220	+15,72
Análisis de perfiles	9.291	58.291	+15,94
Gestión de actividades asociativas, culturales, recreativas, deportivas y sociales	4.816	57.336	+8,40
Educación	4.551	48.228	+9,44
Fines estadísticos, históricos o científicos	4.297	91.422	+4,70
Cumplimiento/incumplimiento de obligaciones dinerarias	4.238	51.281	+8,26
Servicios económicos-financieros y seguros	3.794	71.374	+5,32
Seguridad privada	3.422	26.413	+12,96
Prestación de servicios de comunicaciones electrónicas	3.252	24.556	+13,24
Guías/repertorios de servicios de comunicaciones electrónicas	2.109	17.506	+12,05
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	1.970	21.132	+9,32
Gestión de asistencia social	1.230	15.512	+7,93
Prestación de servicios de solvencia patrimonial y crédito	864	9.103	+9,49
Investigación epidemiológica y actividades análogas	627	9.644	+6,50
Prestación de servicios de certificación electrónica	466	3.746	+12,44
Otras finalidades	71.422	635.710	+11,23

INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN DE FICHEROS SEGÚN EL SECTOR DE ACTIVIDAD	2015	TOTAL	2014-2015 % VARIACIÓN
Comunidades de propietarios	77.716	517.711	+15,01
Comercio	44.898	466.131	+9,63
Sanidad	32.791	296.009	+11,08
Turismo y hostelería	23.222	196.915	+11,79
Contabilidad, auditoria y asesoría fiscal	11.006	162.799	+6,76
Actividades inmobiliarias	10.860	118.119	+9,19
Educación	10.037	96.869	+10,36
Construcción	9.201	139.469	+6,60
Asociaciones y clubes	8.262	84.819	+9,74
Actividades jurídicas, notarios y registradores	8.002	94.683	+8,45
Transporte	6.463	85.491	+7,56
Activ. de organizaciones empresariales, profesionales y patronales	4.887	23.497	+20,80
Servicios informáticos	4.762	56.074	+8,49
Agricultura, ganadería, explotación forestal, caza, pesca	4.335	43.595	+9,94
Comercio y servicios electrónicos	3.920	23.801	+16,47
Activ. relacionadas con los productos alimenticios, bebidas y tabacos	3.492	47.951	+7,28
Industria química y farmacéutica	3.406	56.464	+6,03
Actividades diversas de servicios personales	3.247	39.250	+8,27
Maquinaria y medios de transporte	2.413	46.948	+5,14
Seguros privados	2.209	34.310	+6,44
Actividades de servicios sociales	2.150	30.030	+7,16
Actividades políticas, sindicales o religiosas	1.996	21.502	+9,28
Producción de bienes de consumo	1.947	29.073	+6,70
Sector energético	1.634	24.763	+6,60
Servicios de telecomunicaciones	1.546	17.031	+9,08
Actividades relacionadas con los juegos de azar y apuestas	930	10.059	+9,25

DISTRIBUCIÓN DE FICHEROS SEGÚN EL SECTOR DE ACTIVIDAD	2015	TOTAL	2014-2015 % VARIACIÓN
Publicidad directa	881	12.559	+7,01
Entidades bancarias y financieras	609	13.560	+4,49
Seguridad	602	8.764	+6,87
Organización de ferias, exhibiciones, congresos y otras activ. relac.	417	4.794	+8,70
Inspección técnica de vehículos y otros análisis técnicos	406	4.297	+9,45
Investigación y desarrollo (i+d)	391	4.989	+7,84
Selección de personal	311	4.931	+6,31
Activ. postales y de correo (oper. postales, serv. post., transport.)	251	3.377	+7,43
Solvencia patrimonial y crédito	79	1.152	+6,86
Mutualidades colaboradoras de los organismos de la seguridad social	29	872	+3,33
Otras actividades	124.005	1.096.169	+11,31

INSCRIPCIÓN DE TITULARIDAD PÚBLICA

DISTRIBUCIÓN DE FICHEROS POR TIPO DE ADMINISTRACIÓN	2015	TOTAL
Administración General	538	8.442
Administración CC.AA.	1.282	29.546
Administración Local	4.320	91.520
Otras personas jurídico-públicas	680	27.816
TOTAL	6.820	157.324

DISTRIBUCIÓN DE FICHEROS DE LA ADMINISTRACIÓN GENERAL

	FICHEROS
Presidencia del Gobierno	9
Ministerio de Asuntos Exteriores y de Cooperación	551
Ministerio de Justicia	149
Ministerio de Defensa	2.129
Ministerio de Hacienda y Administraciones Públicas	1.043
Ministerio del Interior	229
Ministerio de Fomento	593
Ministerio de Educación, Cultura y Deporte	289
Ministerio de Empleo y Seguridad Social	1.675
Ministerio de Industria, Energía y Turismo	201
Ministerio de Agricultura, Alimentación y Medio Ambiente	446
Ministerio de la Presidencia	70
Ministerio de Economía y Competitividad	478
Ministerio de Sanidad, Servicios Sociales e Igualdad	580
TOTAL	8.442

DISTRIBUCIÓN DE FICHEROS DE TITULARIDAD PÚBLICA – CC.AA.

	2015	TOTAL
Comunidad Autónoma de Andalucía	71	1.898
Comunidad Autónoma de Aragón	28	404
Comunidad Autónoma del Principado de Asturias	20	526
Comunidad Autónoma de Canarias	48	464
Comunidad Autónoma de Cantabria	6	235
Comunidad Autónoma de Castilla y León	56	883
Comunidad Autónoma de Castilla-La Mancha	149	927
Comunidad Autónoma de Cataluña	292	10.268
Comunidad de Madrid	476	9.579
Comunitat Valenciana	13	579
Comunidad Autónoma de Extremadura	25	521
Comunidad Autónoma de Galicia	33	331
Comunidad Autónoma de las Illes Balears	27	591
Comunidad Foral de Navarra	8	179
Comunidad Autónoma del País Vasco	0	1.341
Comunidad Autónoma de La Rioja	12	237
Comunidad Autónoma de la Región de Murcia	3	441
Ciudad Autónoma de Ceuta	12	50
Ciudad Autónoma de Melilla	3	92
TOTAL	1.282	29.546

DISTRIBUCIÓN DE FICHEROS DE TITULARIDAD PÚBLICA - ADMINISTRACIÓN LOCAL

	2015	TOTAL
Comunidad Autónoma de Andalucía	871	11.076
Almería	112	1.271
Cádiz	50	774
Córdoba	95	950
Granada	195	1.589
Huelva	88	1.286
Jaén	92	829
Málaga	112	2.334
Sevilla	127	2.043
Comunidad Autónoma de Aragón	584	5.878
Huesca	197	1.750
Teruel	78	552
Zaragoza	310	3.576
Comunidad Autónoma del Principado de Asturias	95	1.675
Comunidad Autónoma de Canarias	116	1.981
Las Palmas	51	985
Santa Cruz de Tenerife	65	996
Comunidad Autónoma de Cantabria	70	941
Comunidad Autónoma de Castilla y León	1.207	10.560
Ávila	98	1.123
Burgos	345	2.567
León	209	1.369
Palencia	122	1.298
Salamanca	93	555
Segovia	68	778
Soria	17	97
Valladolid	208	2.486
Zamora	47	287

	2015	TOTAL
Comunidad Autónoma de Castilla-La Mancha	559	7.791
Albacete	101	3.473
Ciudad Real	110	871
Cuenca	187	1.564
Guadalajara	33	457
Toledo	128	1.426
Comunidad Autónoma de Cataluña	1.069	12.938
Barcelona	446	5.910
Girona	228	2.937
Lleida	220	2.204
Tarragona	176	1.887
Comunidad de Madrid	237	4.770
Comunitat Valenciana	520	7.359
Alicante / Alacant	164	2.468
Castellón / Castelló	109	1.161
Valencia / València	248	3.730
Comunidad Autónoma de Extremadura	327	7.965
Badajoz	195	6.174
Cáceres	132	1.791
Comunidad Autónoma de Galicia	331	4.669
A Coruña	100	1.760
Lugo	70	812
Ourense	91	1.056
Pontevedra	70	1.041
Comunidad Autónoma de las Illes Balears	86	1.664
Comunidad Foral de Navarra	253	2.785
Comunidad Autónoma del País Vasco	359	7.664
Araba / Álava	62	741
Gipuzkoa	128	2.240
Bizkaia	169	4.683
Comunidad Autónoma de La Rioja	44	431
Comunidad Autónoma de la Región de Murcia	56	1.373

MEMORIA 2015

DISTRIBUCIÓN DE FICHEROS DE TITULARIDAD PÚBLICA. OTRAS PERSONAS JURÍDICO-PUBLICAS

	TOTAL
Cámaras Oficiales de Comercio e Industria	501
Notariado	8.224
Universidades	1.520
Colegios Profesionales	2.782
Otros	14.789
TOTAL	27.816

DISTRIBUCIÓN DE FICHEROS SEGÚN TIPO DE DATOS. TITULARIDAD PÚBLICA

	2015	TOTAL
Datos especialmente protegidos (ideología, creencias, religión y afiliación sindical)	337	19.611
Otros datos especialmente protegidos (origen racial, salud y vida sexual)	1.306	38.714
Datos relativos a infracciones	836	27.281
Datos de carácter identificativo	6.820	157.324
Datos de características personales	3.504	81.359
Datos de circunstancias sociales	2.048	43.363
Datos académicos y profesionales	2.431	51.944
Detalles de empleo y carrera administrativa	2.123	46.585
Datos de información comercial	898	20.231
Datos económico-financieros	2.733	69.345
Datos de transacciones	880	30.101
Otros tipos de datos	948	23.468

DISTRIBUCIÓN DE FICHEROS CON DATOS SENSIBLES. TITULARIDAD PÚBLICA

	2015	TOTAL
Datos especialmente protegidos	337	19.611
Ideología	125	9.513
Creencias	77	8.670
Religión	98	9.061
Afiliación Sindical	205	17.987
Otros datos especialmente protegidos	1.306	38.714
Origen Racial	287	12.159
Salud	1.296	38.533
Vida Sexual	114	9.753
Datos relativos a infracciones	836	27.281
Infracciones Penales	429	18.321
Infracciones Administrativas	781	26.374

DISTRIBUCIÓN DE FICHEROS SEGÚN SU FINALIDAD. TITULARIDAD PÚBLICA

	2015	TOTAL	2014-2015 % VARIACIÓN
Procedimiento administrativo	1.764	51.234	+3,44
Educación y cultura	1.095	17.216	+6,36
Recursos humanos	871	27.316	+3,19
Gestión contable, fiscal y administrativa	791	22.868	+3,46
Servicios sociales	548	10.124	+5,41
Fines históricos, estadísticos o científicos	378	19.894	+1,90
Videovigilancia	369	2.870	+12,86
Gestión de nómina	350	13.312	+2,63
Gestión sancionadora	302	6.067	+4,98
Prevención de riesgos laborales	230	3.685	+6,24
Trabajo y gestión de empleo	228	5.759	+3,96
Hacienda pública y gestión de administración tributaria	213	10.567	+2,02
Seguridad y control de acceso a edificios	199	3.872	+5,14
Padrón de habitantes	180	6.751	+2,67
Función estadística pública	179	12.685	+1,41
Seguridad pública y defensa	178	4.053	+4,39
Publicaciones	172	2.777	+6,19
Gestión económica-financiera pública	161	6.903	+2,33
Gestión y control sanitario	125	3.903	+3,20
Actuaciones de fuerzas y cuerpos de seguridad con fines policiales	109	2.617	+4,17
Justicia	62	10.638	+0,58
Historial clínico	59	2.249	+2,62
Prestación de servicios de certificación electrónica	55	1.729	+3,18
Investigación epidemiológica y actividades análogas	29	1.564	+1,85
Gestión de censo promocional	21	1.041	+2,02
Otras finalidades	2.412	44.883	+5,37

**TRANSFERENCIAS INTERNACIONALES DE DATOS
RESOLUCIONES DE AUTORIZACIÓN**

		2000-2010	2011	2012	2013	2014	2015	TOTAL AUT.
Estados Unidos (407)	EEUU	177	40	62	47	51	30	407
Iberoamérica (485)	Panamá	2	–	–	1	3	2	8
	Colombia	52	23	17	21	23	10	146
	Chile	35	7	1	–	–	2	45
	Uruguay	23	–	2	–	–	–	25
	Perú	52	30	23	23	5	5	138
	Guatemala	3	–	2	1	–	–	6
	Paraguay	11	4	2	–	–	–	17
	Brasil	5	2	2	3	1	1	14
	El Salvador	1	–	–	–	–	–	1
	Costa Rica	3	1	2	1	–	3	10
	Nicaragua	1	–	–	–	–	–	1
	México	31	12	14	7	2	6	72
	Ecuador	1	–	–	–	–	–	1
	Venezuela	–	–	–	–	1	–	1
India (271)	India	81	29	27	42	53	39	271
Otros países (312)	Marruecos	26	4	10	13	9	7	69
	Singapur	5	2	4	1	6	3	21
	Japón	4	3	4	7	7	1	26
	Malasia	6	–	2	1	5	2	16
	Tailandia	2	–	1	–	–	–	3
	Filipinas	16	5	9	8	5	6	49
	China	9	14	4	6	–	2	35
	Hong Kong	3	–	1	2	–	2	8
	Egipto	1	–	1	1	–	1	4
	Nigeria	1	–	–	–	–	–	1
	Túnez	3	–	3	–	–	2	8
	Sudáfrica	3	–	3	–	1	1	8
	Australia	8	–	3	4	3	1	19
	Canadá	1	–	1	–	2	–	4

MEMORIA 2015

		2000-2010	2011	2012	2013	2014	2015	TOTAL AUT.
Otros países (312)	Rep. Bielorrusa	3	-	-	-	-	-	3
	Mónaco	1	-	-	-	-	-	1
	Israel	7	2	-	-	-	-	9
	Vietnam	3	-	1	-	-	-	4
	Barbados	3	-	-	-	-	-	3
	Andorra	1	-	-	-	-	-	1
	Mauricio	-	1	-	-	-	-	1
	Kenia	-	-	1	-	-	-	1
	Serbia	-	-	1	-	-	1	2
	Taiwan	-	-	2	-	1	-	3
	Croacia	-	-	1	-	-	-	1
	Turquía	-	-	1	-	-	-	1
	Ucrania	-	-	1	-	-	-	1
	Bermudas	1	-	1	-	-	-	2
	Nueva Zelanda	-	-	1	-	1	-	2
	Rep. de Corea	-	-	1	-	1	-	2
	Federación Rusa	-	-	1	1	-	-	2
Internacional (25)	Emiratos Árabes	-	-	-	1	-	-	1
	Arabia Saudí	-	-	-	-	-	-	1
	Internacional	3	1	3	8	2	8	25
	Solicitudes presentadas	197	201	224	192	187	128	1.746
	Archivadas	31	16	52	15	26	29	355
	Total Autorizaciones	155	175	177	170	150	108	1.340

FICHEROS INSCRITOS CON TRANSFERENCIAS INTERNACIONALES SEGÚN TITULARIDAD

FICHEROS	
Titularidad Privada	15.849
Titularidad Pública	8.379
TOTAL	24.228

EVOLUCIÓN DE LAS AUTORIZACIONES DE TRANSFERENCIAS INTERNACIONALES SEGÚN LAS GARANTÍAS APORTADAS (TIPO DE CONTRATO Y NORMAS CORPORATIVAS VINCULANTES -BCR-)

	2010	2012	2014	2015
2001/497/CE ¹	80	167	226	246
2002/16/CE ² – 2010/87/UE ³	475	735	966	1.037
BCR	–	8	23	34
Cláusulas Encargado–Subencargado ⁴	–	2	16	22
Contrato ad hoc	–	–	1	1

¹ DECISIÓN DE LA COMISIÓN, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE.

² DECISIÓN DE LA COMISIÓN, de 27 de diciembre de 2001, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE (derogada desde 15 de mayo de 2010).

³ DECISIÓN DE LA COMISIÓN, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

⁴ RESOLUCIÓN DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS de 16 de octubre de 2012.

TRANSFERENCIAS INTERNACIONALES DE DATOS AMPARADAS EN LAS AUTORIZACIONES DE MOVIMIENTOS DE DATOS ENTRE ENCARGADOS Y SUBENCARGADOS DEL TRATAMIENTO

	2012	2013	2014	2015	TOTAL
Ficheros	1	1.561	1.625	20	3.207
Responsables	1	454	437	8	900

MEMORIA 2015

TRANSFERENCIAS INTERNACIONALES DE DATOS AMPARADAS EN LA AUTORIZACIÓN DE TRANSFERENCIAS INTERNACIONALES BASADAS EN CONTRATO AD HOC

	2014	2015	TOTAL
Ficheros	59	27	86
Responsables	14	9	23

ACTUACIONES COMO AUTORIDAD CORREVISORA DE NORMAS CORPORATIVAS VINCULANTES (BCR)

	2010	2011	2012	2013	2014	2015	TOTAL
Revisión BCR'S	1	4	7	3	9	10	34

EVOLUCIÓN DE LA INSCRIPCIÓN DE LOS FICHEROS DE VIDEOVIGILANCIA

AÑO DE INSCRIPCIÓN	TITULARIDAD PRIVADA*	TITULARIDAD PÚBLICA*
1994 - 2007	5.341	100
2008	8.337	152
2009	20.048	261
2010	29.874	755
2011	34.292	436
2012	33.983	533
2013	37.012	418
2014	38.362	462
2015	8.337	152
TOTAL	249.124	3.555

* Incluye, además de los ficheros que tienen declarada la videovigilancia como finalidad tipificada, aquellos otros en los que se desprende de su denominación o descripción. Por ejemplo, ficheros cuya finalidad tipificada es la de seguridad privada y su denominación es la de «videovigilancia» o «CCTV».

FICHEROS DE VIDEOVIGILANCIA DE TITULARIDAD PRIVADA

SECTOR DE ACTIVIDAD PRINCIPAL	2014	2015	% VARIACIÓN 2014-2015
Otras actividades	61.210	73.242	+19,64
Comercio	49.889	57.691	+15,64
Turismo y hostelería	24.830	29.347	+18,19
Comunidades de propietarios	16.106	21.354	+32,58
Sanidad	11.258	13.827	+22,82
Activ. Relacionadas con los productos alimenticios, bebidas y tabacos	4.337	4.962	+14,41
Construcción	4.265	4.797	+12,47
Transporte	3.705	4.200	+13,36
Industria química y farmacéutica	3.490	3.766	+7,91
Actividades inmobiliarias	2.656	3.249	+22,33
Educación	2.747	3.217	+17,11
Maquinaria y medios de transporte	2.278	2.543	+11,63
Servicios informáticos	2.149	2.426	+12,89
Contabilidad, auditoría y asesoría fiscal	1.982	2.361	+19,12
Agricultura, ganadería, explotación forestal, caza, pesca	1.871	2.279	+21,81
Asociaciones y clubes	1.821	2.135	+17,24
Actividades relacionadas con los juegos de azar y apuestas	1.899	2.079	+9,48
Sector energético	1.780	1.942	+9,10
Seguridad	1.672	1.794	+7,30
Producción de bienes de consumo	1.482	1.645	+11,00
Actividades diversas de servicios personales	1.247	1.435	+15,08
Servicios de telecomunicaciones	1.174	1.323	+12,69
Actividades jurídicas, notarios y registradores	977	1.252	+28,15
Actividades de servicios sociales	1.096	1.221	+11,41
Comercio y servicios electrónicos	879	1.059	+20,48

MEMORIA 2015

SECTOR DE ACTIVIDAD PRINCIPAL	2014	2015	% VARIACIÓN 2014-2015
Activ. De organizaciones empresariales, profesionales y patronales	584	887	+51,88
Entidades bancarias y financieras	674	824	+22,26
Seguros privados	461	537	+16,49
Actividades políticas, sindicales o religiosas	393	496	+26,21
Inspección técnica de vehículos y otros análisis técnicos	263	317	+20,53
Publicidad directa	215	247	+14,88
Organización de ferias, exhibiciones, congresos y otras activ. Relac.	185	210	+13,51
Investigación y desarrollo (i+d)	170	194	+14,12
Activ. Postales y de correo (oper. postales, serv. post., transport.)	129	166	+28,68
Selección de personal	47	55	+17,02
Mutualidades colaboradoras de los organismos de la seguridad social	25	29	+16,00
Solvencia patrimonial y crédito	15	16	+6,67
TOTAL	209.961	249.124	+18,65

P RESENCIA INTERNACIONAL DE LA AEPD

REUNIÓN	FECHA	LUGAR
Sesiones Plenarias del Grupo de Trabajo del Artículo 29 (GT29)	3 y 4 de febrero 14 y 15 de abril 16 y 17 de junio 22 y 23 de septiembre 15 de octubre (extraordinario) 16 de diciembre	Bruselas (Bélgica)
Reuniones de subgrupos del GT29		
Futuro de la privacidad (FoP)	20 de enero 22 de mayo 22 de julio 7 de septiembre 6 de noviembre	Bruselas (Bélgica)
Futuro de la privacidad. EDPB Governance	8 de junio	París (Francia)
Subgrupo de Tecnología (TS)	13 y 14 de enero 2 y 3 de marzo 3 de noviembre	
Financial Matters	20 de abril	
Borders, Travellers & Law Enforcement (BTLE)	12 de enero 24 de marzo 3 de septiembre 3 de noviembre	Bruselas (Bélgica)
Key Provisions	11 y 12 de mayo	
Otras reuniones		
Grupo DAPIX del Consejo	15 y 16 de enero 26 y 27 de enero 6 de febrero 23 y 24 marzo 30 de marzo 22 de abril 6 y 7 de mayo 18 y 19 de mayo 1 de julio 23 de julio 2 de septiembre 14 de octubre	Bruselas (Bélgica)

MEMORIA 2015

REUNIÓN	FECHA	LUGAR
Autoridades Comunes de Control		
Reunión JSB EUROPOL	4 de marzo 3 de junio 12 de octubre 10 y 11 de diciembre	Bruselas (Bélgica)
Reunión JSB. Subgrupo nuevos proyectos	16 de julio	La Haya (P. Bajos)
Inspección Europol	22 de enero 9, 10, 11 y 12 de marzo 6 y 7 de mayo	La Haya (P. Bajos)
Grupos de Supervisión Coordinada de los sistemas VIS, SIS II y EURODAC	25 y 26 de marzo 9 de junio 7 y 8 de octubre	Bruselas (Bélgica)
EUROJUST – Inspección – Reunión	19, 20 y 21 de enero 11 y 12 de mayo	La Haya (P. Bajos)
Comité Schengen	14 de julio 7 de septiembre	Bruselas (Bélgica)
Evaluación Schengen	16 - 20 de marzo 28 de junio - 3 de julio	Viena (Austria) Frankfurt / Berlín (Alemania)
Grupos de trabajo sectoriales		
GT Quiebras de seguridad transfronteriza (Data Breaches)	23 y 24 de junio 17 y 18 de noviembre	Ispra (Italia)
Grupo de Berlín	13 y 14 de octubre	Berlín (Alemania)
Conferencias Internacionales		
Conferencia IAPP	2, 3, 4, 5 y 6 de marzo	Washington (EEUU)
Encuentro Ibérico de Protección de Datos	8, 9 y 10 de abril	Lisboa (Portugal)

REUNIÓN	FECHA	LUGAR
Conferencia de primavera de Autoridades Europeas de Protección de Datos	18 y 19 de mayo	Manchester (Reino Unido)
Conferencia Internacional de Protección de Datos	26-29 de octubre	Amsterdam (Países Bajos)
Otras Reuniones		
Google Taskforce	26 de marzo	París (Francia)
Big Data Code of Ethics	28 y 29 de abril	AEPD Madrid
Facebook Contact Group	26 y 27 de mayo	La Haya (Países Bajos)

GESTIÓN DE RECURSOS HUMANOS

	DOTACIÓN 31/12/2015	CUBIERTOS 31/12/2015
Funcionarios	157	149
Laborales	4	2
Laborales fuera de convenio	2	2
Alto cargo	1	1
	164	154

NIVEL	30	29	28	26	24	22	20	18	17	16	15	14
Efectivos	6	3	22	46	1	15	3	12	2	7	12	20

	A1	A2	C1	C2
Efectivos 2015	32	47	22	48

MUJERES	95
HOMBRES	59

EVOLUCIÓN DEL PRESUPUESTO

	CRÉDITO EJERCICIO 2013	CRÉDITO EJERCICIO 2014	CRÉDITO EJERCICIO 2015
CAPÍTULO I	6.672.660	6.672.660	7.295.520
CAPÍTULO II	5.024.000	5.224.000	5.224.000
CAPÍTULO III	432.450	232.450	232.450
CAPÍTULO VI	1.372.160	1.316.000	1.316.000
CAPÍTULO VIII	22.800	22.800	22.800
TOTAL	13.524.070	13.467.910	14.090.770

* Los datos de todos los capítulos son siempre referidos a créditos definitivos.



MEMORIA AEPD 2015