AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

MEMORIA AEPD 2016

PRÓLOGO

La Memoria que me complace presentar expone de manera detallada las actividades más relevantes realizadas por la Agencia Española de Protección de Datos en 2016, las novedades legislativas y jurisprudenciales y el análisis de los principales retos a los que se enfrenta este derecho fundamental. Dar respuesta a esos desafíos es precisamente lo que nos llevó a elaborar, a finales de 2015, el Plan estratégico 2015-2019 de la AEPD, que ha marcado a grandes rasgos la hoja de ruta seguida por esta institución.

El impulso dado a la ejecución de las medidas recogidas en el mismo ha permitido presentar 20 iniciativas anuales y otras 74 que se mantendrán de manera continuada, focalizando las principales actuaciones en el desarrollo de nuevas vías y materiales para dar a conocer a los ciudadanos sus derechos, así como para informar a las entidades obligadas acerca del cumplimiento de la legislación. En este sentido, la aplicación del nuevo Reglamento General de Protección de Datos, que entró en vigor el 25 de mayo de 2016 y que será aplicable dos años después, está definiendo en gran medida no sólo el futuro de este derecho fundamental sino también las actuaciones de esta Agencia.

El Reglamento va a requerir la adaptación tanto del marco regulatorio vigente como de los principales actores implicados (ciudadanos, responsables y profesionales de la privacidad). La Agencia, como institución que tiene encomendada la garantía de proteger los datos de los ciudadanos, también ha puesto en marcha medidas para afrontar los cambios próximos y facilitar a estos actores, cada uno con sus peculiaridades, la transición a la nueva normativa.

La Agencia considera imprescindible afianzarse como un organismo colaborador y transparente que actúe de la manera más ágil y eficaz posible, a la vez que apostar por la concienciación en la doble vertiente antes mencionada: la de los ciudadanos, para que sean conscientes de qué derechos les amparan y cómo ejercitarlos, y la de aquellos que tratan datos, que deben abordar este asunto como un valor añadido que puede contribuir a su crecimiento y a una mejora de su competitividad. Las vías puestas en marcha para lograrlo convergen en una única finalidad: conseguir la protección efectiva de unos ciudadanos que, como indican todos los estudios, están cada vez más preocupados por la utilización de sus datos personales.

Las consultas recibidas en el área de Atención al Ciudadano han superado las 236.000, un incremento del 8% que se suma al 10% que ya se había producido en 2015 sobre 2014. A este respecto, hay que destacar que buena parte de las consultas ciudadanas más frecuentes están relacionadas con la inclusión indebida en ficheros de morosidad, una materia que, por otro lado, también es una de las principales fuentes de reclamaciones planteadas ante la Agencia. Junto con la contratación irregular de servicios, supone el grueso de las denuncias que recibe cotidianamente la Agencia, y de ahí que se haya optado por darles un tratamiento singularizado en el apartado de cifras de esta Memoria.

En cuanto a denuncias y reclamaciones, la Agencia ha recibido más de 10.500 en 2016. Las primeras se han reducido con respecto a 2015 un 6,5%, si bien las reclamaciones de tutela se han incrementado un 24,3%. En este punto es necesario mencionar que esta institución ha acometido una profunda reorganización interna que tiene como finalidad la tramitación ágil a la vez que rigurosa de los temas planteados.

Además de la actividad generada por las consultas, denuncias y reclamaciones planteadas por los ciudadanos, las cuestiones atendidas por el Gabinete Jurídico y la inscripción de ficheros, el año que recoge esta Memoria ha destacado por el incremento de las solicitudes de transferencia internacional de datos presentadas y concedidas con motivo de la sentencia del Tribunal de Justicia de la Unión Europea que declaró inválida la Decisión de Puerto Seguro.

Estas y otras cifras, que se desglosan de manera pormenorizada en las siguientes páginas, así como el análisis de otras iniciativas menos susceptibles de cuantificación, ponen de manifiesto sin ninguna duda la creciente importancia que la protección de datos ha adquirido en la sociedad actual y la indudable apuesta que se ha de realizar para mantener el nivel de protección que nos hemos otorgado. Para finalizar, debo reconocer la labor desempeñada por el personal de todos los departamentos de la Agencia, una plantilla cuyo número se mantiene intacto desde 2008 y que, sin embargo, asume un número cada vez mayor de tareas más complejas y se enfrenta a nuevos retos derivados de la implementación del Reglamento.

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

MEMORIA **AEPD**

2016

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

1 EL PLAN ESTRATÉGICO 2015 – 2019. BALANCE DEL PRIMER AÑO DE EJECUCIÓN

En el año 2016, la Agencia Española de Protección de Datos (AEPD), además de la actividad ordinaria generada por las denuncias y reclamaciones de tutela de derechos presentadas por los ciudadanos, las consultas planteadas ante el Gabinete Jurídico y Atención al Ciudadano, y la inscripción de ficheros, destacó por las siguientes actuaciones novedosas:

- El impulso dado a la puesta en marcha y la ejecución del 67% de las actuaciones previstas en el Plan Estratégico 2015-2019, entre ellas las iniciativas preparatorias para la implementación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD, Reglamento Europeo de Protección de Datos).
- El incremento de las autorizaciones de transferencia internacional de datos presentadas y concedidas, con motivo de la sentencia del Tribunal de Justicia de la Unión Europea (TJUE) de fecha 6 de octubre del 2015 por la que se declaró inválida la Decisión 2000/520/CE, conocida como Decisión de Puerto Seguro.

La Memoria 2015 ya recogía las líneas de actuación del Plan Estratégico de la Agencia, concretando las acciones previstas durante su vigencia (2015 – 2019), con un total de 113 iniciativas.

La presente Memoria recoge las iniciativas que han sido puestas en marcha desde la presentación del mismo –en noviembre de 2015– al cierre del ámbito temporal de este documento. Las dos cuya realización estaba prevista en el Plan para 2015 fueron ejecutadas. En 2016, de las 84 actuaciones previstas en el Plan, se han puesto en marcha un total de 74. Un 27% (20) de estas iniciativas finalizaron en 2016, encontrándose las 54 restantes en proceso de ejecución al tratarse de acciones plurianuales o continuas. En consecuencia, el grado de cumplimiento del plan durante 2015 ha sido del 100%, situándose en 2016 en un 88%. El 12% restante se debe a acciones cuya ejecución se ha reformulado a 2017 o a la fusión de diferentes acciones. En cuanto a los medios empleados para la realización de las iniciativas, cabe destacar que la práctica totalidad de las mismas se ha realizado con los medios propios de la Agencia. El gasto imputable a la ejecución de estas 22 actuaciones y la puesta en marcha de las otras 54 se sitúa por debajo de los 85.000 euros, correspondiendo esta cifra fundamentalmente a la necesidad de asistencia técnica para la digitalización de la Agencia y a la elaboración de materiales orientados a la protección de los menores.

Del conjunto de iniciativas realizadas en 2016 hay que destacar la publicación de siete guías sobre diversas materias; las actuaciones realizadas para sensibilizar a los menores sobre la importancia de proteger su información personal en internet; la actualización de contenidos prácticos de diversa temática para orientar al ciudadano en temas como el ejercicio del derecho al olvido o cómo solicitar la eliminación de fotos y vídeos publicados en internet; o la optimización de los recursos de la Agencia, entre otros.

El grueso de las iniciativas que contempla el Plan Estratégico responde a lo que pretende ser un cambio de tendencia de la actividad de la Agencia en los próximos años, desde un enfoque tradicional principalmente reactivo hacia otro caracterizado por la prevención. El contexto actual exige que aquellos que tratan datos personales apuesten por la implantación de políticas y herramientas proactivas de cumplimiento en un entorno en el que los responsables del tratamiento de los datos perso-

nales deben asumir el compromiso de garantizar diligentemente los derechos de los ciudadanos.

En esa línea, la AEPD ha considerado la prevención y la concienciación de los menores, un colectivo especialmente vulnerable que puede verse involucrado en situaciones de alto riesgo en internet, como una de las líneas prioritarias para difundir el derecho a la protección de datos. No hay que olvidar que la Comisión Europea hace ya tiempo que señaló que los jóvenes empiezan a navegar en internet a los 7 años, y algunos estudios reducen aún más esa edad de inicio. Sin poner en duda las oportunidades y beneficios que proporciona internet, también hay que tener en cuenta que, como ocurre en la vida real, internet no está exento de riesgos que, en el caso de los menores, pueden tener graves consecuencias para su desarrollo.

Otro de los objetivos prioritarios de la Agencia es garantizar los derechos de los ciudadanos en caso de contratación irregular de servicios o inclusión indebida en ficheros de morosidad, áreas que constituyen dos de las principales fuentes de reclamaciones ante la Agencia y que suponen el mayor volumen de sanciones.

El incremento de la competencia en sectores liberalizados como las telecomunicaciones o la energía han contribuido al desarrollo de prácticas comerciales más agresivas por parte de los prestadores de servicios esenciales para los ciudadanos. En este marco se ha incrementado la falta de una identificación inequívoca de los clientes que contratan estos servicios y prácticas ilícitas como la suplantación de la identidad, con la consecuencia de que se facturan los servicios a personas que no los han contratado y cuyos impagos dan lugar a su inclusión en los denominados ficheros comunes de solvencia, con los innegables perjuicios que ello conlleva para los ciudadanos afectados.

Los efectos negativos de estas prácticas han supuesto la inclusión en el Plan Estratégico de nuevas acciones proactivas, que se han concretado en la celebración de reuniones con las empresas de los principales sectores afectados y con los responsables de los ficheros comunes de solvencia, para informarles de las deficiencias detectadas y requerirles iniciativas para su resolución.

Asimismo, en estrecha colaboración con la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital y los organismos competentes en materia de consumo, en especial con el Consejo de Consumidores y Usuarios –con quien la Agencia tiene suscrito un Acuerdo–, se ha previsto la elaboración de diversos materiales prácticos y guías para que los ciudadanos puedan conocer con claridad a quién deben acudir en cada caso concreto para que la defensa de sus derechos sea lo más eficaz posible, en un entorno en que los límites de las respectivas competencias administrativas en ocasiones pueden resultar difusos.

Otro de los ejes que prevé el Plan Estratégico engloba un conjunto de medidas orientadas a mejorar la protección de datos personales en relación con las últimas novedades tecnológicas, así como a apoyar aquellas iniciativas que contribuyan a generar un clima de confianza en el ámbito de la economía digital y en los usos de la tecnología por parte de los sectores público y privado, favoreciendo la competitividad de las empresas, el desarrollo y la innovación en las industrias TIC y, en

definitiva, un ambiente propicio de cumplimiento normativo en materia de privacidad.

Sin duda, la iniciativa más relevante en este ámbito durante 2016 ha sido la creación de la Unidad de Evaluación y Estudios Tecnológicos (UUET) como área específica de la Agencia para identificar y analizar tendencias, productos o servicios que puedan tener un impacto en la privacidad de los ciudadanos. Una medida que está en plena sintonía con el nuevo Reglamento General de Protección de Datos (RGPD), que atribuye a las autoridades de control la competencia para «hacer un seguimiento de cambios que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, en particular el desarrollo de las tecnologías de la información y la comunicación y las prácticas comerciales».

Entre los cometidos principales de esta nueva Unidad está la realización de estudios prospectivos y análisis de los productos y servicios para conocer de primera mano sus funcionalidades y la forma en que almacenan, tratan y comunican los datos personales que recogen, así como la transparencia con la que se llevan a cabo estos tratamientos.

En este punto es necesario dedicar un emotivo recuerdo al principal impulsor de la Unidad y persona clave para el funcionamiento de la Agencia, Emilio Aced Félez, fallecido el 28 de septiembre de 2016, cuya humanidad y profesionalidad permanecerá siempre como un referente para todos cuantos formamos parte de esta Institución.

Continuando con las iniciativas recogidas en el Plan, este incluye distintas iniciativas para acercar la Agencia a las empresas y profesionales del sector, fomentando su colaboración y proporcionando una respuesta rápida y adecuada a sus necesidades mediante la aportación de herramientas y materiales prácticos que faciliten el cumplimiento de la normativa de protección de datos, con especial atención a las pymes y micropymes.

Con este fin, de cara a la próxima aplicación del nuevo Reglamento en mayo de 2018 se están diseñando un conjunto de guías y herramientas prácticas a las que se aludirá con detalle más adelante. Asimismo, los profesionales de la privacidad tienen un relevante papel en su labor de asesoramiento a los responsables y encargados del tratamiento, ya que su experiencia en la materia resulta fundamental para conocer las inquietudes y dificultades que suscita la aplicación de la legislación. De ahí la necesidad de mantener una colaboración fluida y ágil con ellos, a través de sus asociaciones, para conocer sus problemas y sus propuestas y, al mismo tiempo, poder transmitir los criterios y líneas de actuación de la Agencia, especialmente en relación con la aplicación del Reglamento europeo. Ello redundará, sin duda, en la calidad de su asistencia profesional y, por tanto, en un mejor cumplimiento de la normativa y de las garantías de los ciudadanos.

Otro bloque destacado de iniciativas pretende mejorar los sistemas de gestión de la Agencia, tanto para prestar un servicio más eficaz a los ciudadanos como para disponer de los recursos adecuados con los que poder afrontar en las mejores condiciones sus funciones de autoridad de control y, en especial, los retos derivados del nuevo Reglamento europeo.

La Agencia recibe más de 12.000 denuncias y reclamaciones al año, lo que exige tratar de optimizar al máximo los recursos disponibles. En este sentido, se han previsto un conjunto de medidas encaminadas a la simplificación de los procedimientos, la reducción de los tiempos de tramitación y el uso intensivo de las herramientas de la Administración electrónica.

El último de los retos estratégicos es el relativo a la aplicación del nuevo Reglamento General de Protección de Datos, que va a marcar la agenda de la Agencia los próximos años y va a requerir un importante esfuerzo de adaptación tanto del marco regulatorio vigente como de los principales actores implicados (ciudadanos, responsables y profesionales de la privacidad), y también de las propias autoridades de control, que van a tener que llevar a cabo cambios profundos tanto en su organización y funcionamiento como en sus poderes de actuación.

En particular, corresponde a las autoridades de protección de datos, como organismos de supervisión y promoción de la correcta aplicación del Reglamento, realizar un riguroso y permanente esfuerzo de interpretación y aclaración de sus disposiciones y, asimismo, desarrollar instrumentos que faciliten el conocimiento y la adaptación al mismo por parte de los responsables y encargados, y por los ciudadanos.

Esta labor de adaptación y puesta en marcha de instrumentos que faciliten el cumplimiento del Reglamento se está llevando a cabo a través de distintas iniciativas.

En el plano normativo, se está participando de forma activa en el Grupo de Trabajo creado en el seno de la Sección de Derecho Público de la Comisión General de Codificación, para la reforma de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).

En el ámbito interno, se están definiendo medidas de adaptación que permitan optimizar los recursos de la Agencia para poder afrontar con garantías los retos que supone la aplicación efectiva del Reglamento.

Uno de los mayores desafíos a los que se enfrenta la Agencia está relacionado con el hecho de conseguir que la aplicación del Reglamento no suponga una carga excesiva para las empresas y organizaciones, constituyéndose como un valor añadido que contribuya a su crecimiento y a una mejora de su competitividad. A tal fin, desde la Agencia se está realizando un importante esfuerzo por dotar a las empresas, y especialmente a las pymes y micropymes, de un conjunto de herramientas y materiales que faciliten su proceso de adecuación al Reglamento.

Todos estos materiales, tanto los ya elaborados como los que se vayan generando, están reunidos en una sección específica creada en la web de la Agencia para ofrecerlos de una forma integrada y más accesible. Para verificar su utilidad práctica, están siendo contrastados con los sectores implicados (CEPYME, Cámara de España, Unión Profesional), con el objeto de articular una difusión conjunta.

En este ámbito hay que poner en valor la estrecha relación que en este proceso de adaptación viene manteniéndose con la Autoridad Catalana de Protección de Datos y la Agencia Vasca de Protección de Datos como ejemplo de cooperación institucional.

Finalmente, en el marco europeo, hay que destacar el trabajo de armonización que están llevando a cabo las Autoridades europeas de protección de datos en el seno del Grupo de Trabajo del Artículo 29 (GT29) para la fijación de criterios comunes de interpretación y aplicación en los numerosos aspectos del Reglamento.

En cuanto a las Administraciones Públicas, también se están poniendo en marcha distintas iniciativas, en particular, respecto de la figura del Delegado de Protección de Datos que será obligatorio para ellas.

Estas y otras iniciativas se describen de manera más detallada en los epígrafes correspondientes de esta Memoria.

2 PREVENCIÓN PARA UNA PROTECCIÓN MÁS EFICAZ

2.1. PROTECCIÓN Y EDUCACIÓN DE LOS MENORES

Como se ha mencionado con anterioridad, la Agencia Española de Protección de Datos en su Plan Estratégico 2015 – 2019 ha establecido la prevención y la concienciación como una de sus líneas de actuación prioritaria para reforzar el derecho a la privacidad y protección de datos de los menores de edad, colectivo que por su vulnerabilidad exige una especial sensibilidad y atención por parte de los poderes públicos.

Conforme al Plan Estratégico, la Agencia despliega esta especial atención a los menores a través de medidas y acciones dirigidas fundamentalmente a fomentar su educación y concienciación sobre el valor de la privacidad y la importancia del uso responsable de la información personal en internet, impulsando la colaboración con los distintos actores, públicos y privados, implicados en la protección de los menores con la finalidad de dotar de mayor efectividad a las actuaciones desplegadas.

Entre las instituciones, organismos, entidades e iniciativas con las que de una u otra forma se ha colaborado, cabe señalar a los organismos competentes de los Ministerios de Educación, Cultura y Deporte, Interior, Justicia, Energía, Turismo y Agenda Digital, Sanidad, Servicios Sociales e Igualdad, así como de la Fiscalía y la Comisión Nacional de los Mercados y la Competencia, la Fundación ANAR, el Observatorio de Contenidos Televisivos Audiovisuales, Pantallas Amigas, asociaciones del ámbito de la comunidad educativa (padres, docentes, centros), y empresas como Telefónica, Orange, Google, RTVE, Mediaset o Atresmedia.

Para el cumplimiento de este objetivo, las actuaciones que en ejecución del Plan Estratégico se han llevado a cabo durante 2016 han sido las siguientes:

2.1.1. Canal de comunicación con centros educativos, docentes, padres y menores

El canal de comunicación específico de la Agencia (canaljoven@agpd.es, 901233144, WhatsApp: 616172204), que se puso en marcha en octubre de 2015 para potenciar la comunicación con los propios menores, padres y profesores sobre las cuestiones que afectan al tratamiento de datos de y por menores ha atendido cerca de 700 consultas, en su mayor parte planteadas por padres, miembros de la comunidad educativa, servicios sociales, sanitarios e incluso policía local. A las tres vías de contacto lanzadas inicialmente (línea telefónica, canal de WhatsApp y buzón de correo electrónico) se han añadido las consultas que a este respecto se reciben a través de la Sede electrónica de la Agencia.

2.1.2. Herramientas y materiales para profesores, padres y alumnos

Con la intención de impulsar la formación y concienciación de los más de ocho millones de alumnos escolarizados, la Agencia, durante 2016 y continuando con la línea de colaboración iniciada con la firma el 13 de octubre de 2015 del convenio con el Ministerio de Educación, Cultura y Deporte, ha desarrollado y puesto a disposición de la comunidad educativa y otros agentes interesados nuevos materiales y recursos.

Conscientes de que determinadas conductas de los menores en internet, además de causar daños y perjuicios, pueden llegar a ser constitutivas de delito, se publicó la guía Sé legal en internet, dirigida a menores de entre 10 y 14 años, con un lenguaje accesible a su nivel de madurez, y Enséñales a ser legales en internet, versión destinada

a padres y profesores como ayuda para el desempeño de la labor educativa y orientadora de hijos y alumnos, respectivamente. En ellas se alerta de los comportamientos inadecuados en internet, de los que constituirían delito y de sus consecuencias tanto para los menores como para sus padres.

Con el objetivo de llegar al mayor número posible de menores, se ha colaborado con Clan, el canal infantil y juvenil de RTVE, que ha realizado una campaña de educación digital en el uso responsable de internet y las redes sociales entre los más jóvenes, a través de vídeos protagonizados por los personajes de la serie de ficción Big Band Clan. Los vídeos, que promueven la privacidad como un valor imprescindible a la hora de usar las tecnologías de la información y la comunicación, permanecen accesibles en Tudecideseninternet.es y en la web de Clan. También se mantuvieron contactos con las principales cadenas generalistas de televisión.

Estos y otros materiales se encuentran disponibles en la página específica de menores de la Agencia www.tudecideseninternet.es, que durante 2016 registró 48.938 visitas. También se han difundido a la comunidad educativa, administraciones educativas (a través de la Comisión General de Educación), centros escolares, organizaciones de profesores, AMPAS, instituciones y asociaciones que trabajan con menores y otras organizaciones como el Consejo de Consumidores y Usuarios.

Es común la expresión «nativos digitales» para referirse a los menores de edad en relación con el mundo virtual y, sin embargo, es un término que puede no corresponderse con lo que da a entender. Los menores son muy hábiles en el manejo de los dispositivos, pero necesitan formación para conocer las posibilidades que ofrece internet y, sobre todo, de los riesgos que puede comportar. Necesitan aprender y en esa tarea cobran una especial relevancia dos colectivos fundamentales para ello, el de las familias y el de los profesores, que son clave y a los que también hay que prestar atención para reducir la brecha generacional y evitar que los menores se conviertan en «huérfanos digitales».

La Agencia, con el objetivo de concienciar y formar a las familias y de que dispongan de recursos para educar a sus hijos en el mundo digital, ha organizado un taller para familias, que ha sido objeto de grabación y que se está editando para, a través de la web www.tudecideseninternet.es, ponerlo a disposición de las familias y de la comunidad educativa.

2.1.3. Plan de Inspección sectorial de oficio sobre servicios cloud en el ámbito educativo

Tras la presentación en 2015 de los resultados de la primera inspección sectorial en Europa sobre servicios cloud en el ámbito educativo, en 2016 la AEPD ha continuado supervisando las principales recomendaciones recogidas en este informe. En particular se han desarrollado dos iniciativas:

- La primera de ellas en relación con las editoriales que proporcionan licencias de uso de los libros digitales que conforman la *mochila digital* de los alumnos, las cuales han desarrollado plataformas de aprendizaje EVA (Entornos Virtuales de Aprendizaje). En la mayor parte de los casos, además de gestionar los contenidos del libro digital, se permite identificar a cada uno de los profesores, de los alumnos y conservar información sobre la evolución de los mismos.

  La AEPD convocó una reunión a la que acudieron la mayor parte de las editoriales que proporcionan libros digitales a la enseñanza no universitaria, junto con representantes del Ministerio de Educación y Ciencia y del Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF) en la que se planteó la problemática detectada, poniendo de manifiesto que las editoriales carecen de legitimación para el tratamiento de datos personales distintos de los previstos en la licencia del servicio.

  Asimismo, se planteó la necesidad de anonimizar los datos de los usuarios de tal forma que no se conozca la identidad de los alumnos y de los profesores que utilicen el entorno EVA del que disponen las editoriales. Además, se propuso impulsar proyectos que permitan utilizar todas las ventajas que proporcionan los contenidos digitales con una garantía que permita el tratamiento de datos personales únicamente a las entidades que tengan legitimidad y consentimiento para ello.

- La segunda iniciativa se refiere a la utilización, por parte de los docentes, de servicios de almacenamiento en cloud computing u otras aplicaciones distintas de las contratadas por los centros. Durante las actuaciones preventivas realizadas por la Agencia en el año 2015 se detectó la utilización de diversas aplicaciones informáticas instaladas generalmente en los dispositivos móviles de profesores y alumnos, distintas de las plataformas educativas, que podían registrar datos de carácter personal, incluidas imágenes y calificaciones.

  Este tipo de aplicaciones, si bien pueden ser de gran utilidad para el aprendizaje y para la organización de las aulas, no suelen estar incluidas en la política de seguridad, siendo utilizadas sin un proceso previo de autorización por parte del centro educativo.

  También se detectó la utilización de herramientas de almacenamiento en nube, al margen de las plataformas educativas utilizadas por los centros, para la compartición de documentos entre alumnos o entre el profesor y los alumnos.

  Durante el año 2016 la Agencia ha celebrado reuniones con las asociaciones de centros educativos más representativas del sector con el fin de promover la aplicación de las citadas recomendaciones. En el marco de estas reuniones se ha solicitado la colaboración de las asociaciones para la puesta en marcha de un cuestionario on-line redactado por la Agencia y consensuado con las asociaciones para recabar información de los centros sobre la utilización de este tipo de aplicaciones y herramientas.

  Los resultados del cuestionario permitirán la realización de un estudio que tendrá como objetivo la emisión de recomendaciones por parte de esta Agencia, previsiblemente durante el año 2017.

2.1.4. Colaboración con las administraciones educativas

La colaboración con las administraciones educativas resulta esencial para llegar a los menores, tal y

como se recoge en el convenio suscrito con el Ministerio de Educación, Cultura y Deporte. A lo largo de 2016 esta colaboración se ha materializado en la elaboración de los contenidos de los recursos editados, en su difusión, así como en la divulgación del Premio a las Buenas prácticas educativas en privacidad y protección de datos para un uso seguro de internet, que se abordará en detalle en otro apartado de esta Memoria.

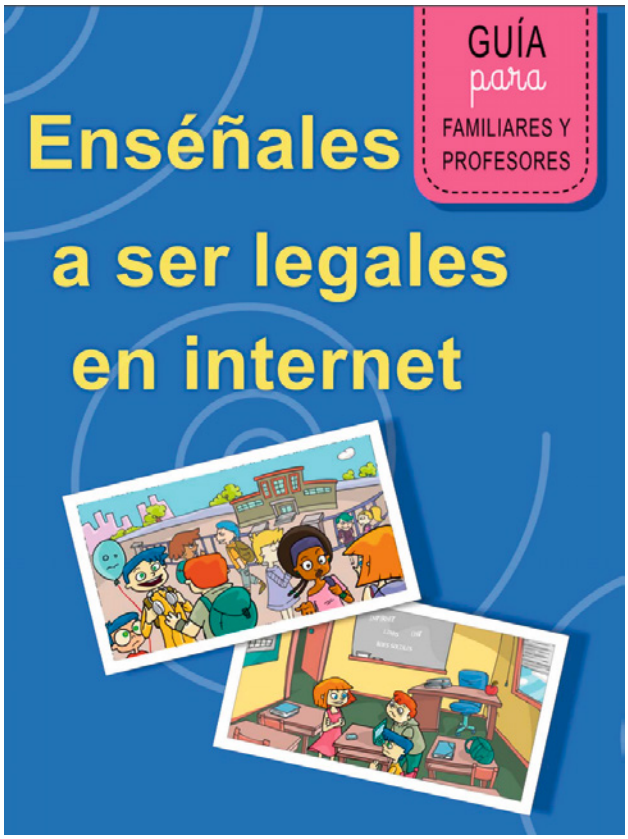
Asimismo, se mantienen contactos periódicos con las administraciones educativas a través de la Comisión General de Educación, en cuyo seno se han presentado los materiales y recursos elaborados y un Marco de competencias digitales en protección de datos y privacidad como orientación para su inclusión en el currículum educativo y se ha participado en jornadas organizadas por la Inspección de las administraciones educativas.

2.1.5. Colaboración con la Fiscalía y las Fuerzas y Cuerpos de Seguridad

La Fiscalía, tanto la de Menores como la de Criminalidad Informática son actores clave en la seguridad de los menores en internet y han colaborado en la elaboración de los contenidos de los materiales presentados, especialmente de la guías Sé legal en internet y Enséñales a ser legales en internet, en las que también han colaborado el Ministerio de Justicia y el Instituto Nacional de Ciberseguridad (INCIBE).

Además, con la Fiscalía de Criminalidad Informática se han mantenido contactos para colaborar en otros ámbitos como el de la tramitación judicial de hechos objeto de denuncia ante la Agencia que pudieran ser constitutivos de delitos y para elaborar nuevos materiales sobre privacidad y conductas delictivas.

La colaboración con las Fuerzas y Cuerpos de Seguridad, a través de la Secretaría de Estado de Seguridad, se ha concretado en la elaboración de los materiales dirigidos a educar a los menores, la asistencia a diferentes encuentros y la participación de la Agencia en las acciones de formación de formadores para el Plan Director del Ministerio del Interior para la convivencia y mejora de la seguridad en los centros educativos y sus entornos.



2.1.6. Otras actuaciones

Con ocasión de la celebración del Día Europeo de la Protección de Datos, el 28 de enero, se celebró en la sede de la Agencia una jornada sobre «Menores, privacidad y conductas delictivas» que contó con la presencia de miembros de la comunidad educativa, del Ministerio de Educación Cultura y Deporte, del de Justicia, la Fiscalía, la Secretaría de Estado de Seguridad y de la Fundación ANAR, que se detalla en un apartado posterior de esta Memoria.

La 20.ª edición de los Premios de Protección de Datos Personales convocados por la Agencia Española de Protección de Datos en 2016 incluyó por primera vez un Premio a las Buenas prácticas educativas en privacidad y protección de datos para un uso seguro de internet, con dos modalidades: una orientada a los centros educativos y otra a

personas o entidades destacadas por difundir el uso seguro de internet entre los menores.

Este nuevo galardón, encuadrado en las actuaciones previstas en el Plan Estratégico, tiene por objeto premiar a los centros educativos en la adopción de buenas prácticas que promuevan el conocimiento del derecho fundamental a la protección de datos de los alumnos de Educación Primaria, Secundaria, Bachillerato y Formación Profesional, contribuyendo también a concienciar a los alumnos sobre el valor de la privacidad y el uso responsable de la información personal que comparten en internet, tanto propia como de terceros.

La primera modalidad premia las buenas prácticas llevadas a cabo por centros educativos públicos, concertados y privados y está dotado con material escolar por valor de 3.000 euros.

La segunda modalidad reconoce el compromiso de personas, instituciones, organizaciones y asociaciones, públicas y privadas, que se hayan distinguido de manera destacada en el impulso y la difusión entre los menores de edad del uso seguro de internet, relacionado fundamentalmente con la información personal y con el valor de la privacidad. Este galardón es honorífico y consiste en un trofeo así como, en su caso, la difusión de las iniciativas y proyectos premiados.

Asimismo en la convocatoria de los premios de la Agencia en la modalidad de medios de comunicación se priorizó por su importancia y especial vulnerabilidad al colectivo de menores.

Por otro lado, la Agencia también ha colaborado, junto con el Instituto Nacional de Ciberseguridad (INCIBE), la Agencia Española de Consumo, Seguridad Alimentaria y Nutrición (AECOSAN) y la Confederación Española de Asociaciones de Padres y Madres de Alumnos, (CEAPA), en el concurso que organizan la Organización de Consumidores y Usuarios (OCU) y Google en el marco de la campaña Vive un Internet Seguro, lanzada en enero de 2017.

2.2. UNA RESPUESTA INTEGRAL PARA GARANTIZAR LOS DERECHOS DE LOS CIUDADANOS

2.2.1. Inspecciones sectoriales de oficio

Una de las actuaciones más importantes de la Agencia es el impulso de inspecciones sectoriales dirigidas a evaluar el cumplimiento de la normativa de protección de datos en relación con actividades de mayor relevancia que puedan ser de interés general.

2.2.1.1. *Plan de inspección sectorial de sanidad*

La Agencia Española de Protección de Datos ha prestado siempre una especial atención al tratamiento de los datos de salud. Es por ello que en el año 1995 desarrolló un Plan Sectorial de Oficio en el sector sanitario al objeto de comprobar el nivel de conocimiento y cumplimiento de la normativa de protección de datos personales en los hospitales públicos.

El plan se circunscribió a hospitales públicos y la selección de los mismos se realizó a partir del Catálogo Nacional de Hospitales, publicado por el entonces Ministerio de Sanidad y Consumo. En una primera aproximación se comprobó que había variaciones entre los hospitales según el número de camas, la finalidad asistencial (General, Quirúrgico, Maternal, Infantil, Materno-Infantil, Psiquiátrico, Enfermedades del Tórax, Oncológico, Traumatología y/o rehabilitación, Geriatría y larga estancia y Otras) y su dependencia funcional (Sistema Nacional de Salud, Municipio, Ministerio de Defensa, Ministerio de Justicia). Por tanto, la selección de hospitales a visitar se realizó atendiendo a la dependencia funcional (Sanidad, Defensa, Justicia) número de camas y ubicación geográfica y dentro de estos criterios la selección del hospital fue aleatoria.

Las inspecciones a los hospitales finalizaron el año 1996 con la elaboración de un informe de conclusiones que ponía de manifiesto con carácter general el desconocimiento por parte de la dirección de los centros sanitarios de la normativa de protección de datos y por tanto, una falta de implicación en su aplicación práctica, sobre todo en cuanto a las medidas de seguridad a implantar para evitar pérdidas o alteraciones en los datos personales tratados.

Dado que los resultados obtenidos del plan citado, entre otros, ponía de manifiesto la presencia de entidades externas que permanecían conectadas a los laboratorios durante las 24 horas del día al objeto de prestar un servicio de atención continuado y facilitar más rápidamente las soluciones a problemas planteados o detectados por los usuarios, todo ello sin un adecuado control por parte de los responsables de los sistemas de información de los citados laboratorios y que los ficheros a los que podían acceder estas entidades externas contenían datos personales relacionados con la salud de los pacientes, durante 2003 y 2004 se realizó un Plan de Inspección de oficio al objeto de comprobar la situación en ese momento y si se habían producido avances en el cumplimiento de la normativa de protección de datos vigente.

En diciembre 2004 se elaboró un documento de conclusiones y recomendaciones basadas en los incumplimientos detectados por parte de laboratorios y entidades de mantenimiento.

Por otro lado, la Agencia, debido al aumento de reclamaciones relativas al ejercicio de derechos ARCO y denuncias que se recibían en relación con historias clínicas, en marzo de 2010 tomó la iniciativa de valorar la situación respecto del cumplimiento de la LOPD en hospitales públicos y privados incluidos en el Catálogo Nacional de Hospitales publicado en la página web del entonces Ministerio de Sanidad y Política Social.

A tal efecto se elaboró un cuestionario en el que se solicitaba información de su situación respecto de la inscripción de ficheros en el RGPD, el deber de información al interesado y derechos ARCO, la contratación de servicios de tratamiento de datos personales (art. 12) y las medidas de seguridad y auditoria.

Los resultados obtenidos tras el análisis de todos los cuestionarios se plasmaron en un informe de cumplimiento de la LOPD publicado por la AEPD en octubre de 2010 donde se ponía de manifiesto que el cumplimiento de la normativa era más alto en el conjunto de centros privados que en los públicos, alcanzándose en los privados niveles elevados en la mayoría de conceptos analizados: inclusión de cláusulas informativas en los formularios de recogida de datos, disponibilidad de procedimientos para atender el ejercicio de los derechos ARCO y, en general, en la implantación de medidas de seguridad y su auditoría periódica.

En los centros públicos, las mayores diferencias de cumplimiento con respecto a los privados se presentaron en las cláusulas informativas de los formularios de recogida de datos y en la realización de la auditoría bienal de seguridad. Otros aspectos con carencias en el sector público fueron los carteles informativos sobre protección datos, las revisiones del documento de seguridad, el registro de los accesos a los datos, la seguridad en el almacenamiento de las historias clínicas en papel para evitar accesos no autorizados, así como la adopción de medidas para evitar la sustracción, pérdida o acceso indebido a la documentación durante su transporte.

En 2015, tras valorar todo lo expuesto anteriormente, la AEPD decidió incorporar en su Plan Estratégico una iniciativa a desarrollar en los hospitales al objeto de conocer el impacto de las recomendaciones dictadas por la AEPD en cada una de las actuaciones abordadas en el pasado.

Así, durante el año 2016 la Agencia ha realizado nuevas actuaciones de inspección dirigidas a los centros hospitalarios de titularidad pública teniendo en cuenta los gestionados tanto de forma directa como indirecta, centrándose en la auditoria de las medidas de seguridad implementadas, con visitas presenciales a los hospitales que fueron inicialmente auditados y hospitales de nueva creación.

Se han auditado hospitales públicos de gestión directa e indirecta, incluyendo hospitales que, partiendo de una situación de historia clínica en papel, la han automatizado a formato electrónico; hospitales que conservan aún la historia clínica de sus pacientes en papel y que están inmersos en distinta medida en procesos de automatización de la documentación médica, y hospitales de nueva creación que han incorporado la historia clínica electrónica desde su nacimiento.

Con respecto a los servicios hospitalarios inspeccionados, la selección se ha realizado atendiendo a los tratamientos de datos personales que realizan, con especial atención a los relativos a datos especialmente protegidos. Entre los servicios auditados se encuentran admisión, urgencias, consultas externas, anatomía patológica, unidad de cuidados intensivos, laboratorio de análisis clínicos, farmacia hospitalaria, departamento de informática, atención al paciente y servicios sociales. También se ha auditado un biobanco.

Las conclusiones y recomendaciones de la inspección se harán públicas en 2017.

2.2.1.2. *Inspección sectorial del Sistema de Información de Visados VIS – II y de Schengen SIS – II*

Las inspecciones sectoriales de oficio del Sistema de Información de Visados Vis-II y de Schengen SIS-II se enmarcan dentro de la «Supervisión de la AEPD del acervo Schengen».

El Sistema de Información de Schengen o SIS, creado en virtud del Convenio de Aplicación del Acuerdo de Schengen, es un sistema de información común que permite a las autoridades competentes de los Estados Miembros disponer de información relativa a algunas categorías de personas y objetos, y cuyo propósito es el mantenimiento de la seguridad pública, apoyo a la policía, la cooperación judicial y gestión del control de las fronteras exteriores.

Esta información es compartida entre los Estados participantes mediante un sistema de información que permite a las autoridades asignadas incluir información (llamadas señalamientos) y disponer de acceso a las descripciones de personas y de objetos introducidos por otros países, con ocasión de controles en las fronteras, aduanas y controles de policía.

El SIS está compuesto por el Sistema de Información Central C-SIS situado en Estrasburgo y los Sistemas de Información Nacionales N-SIS de los distintos estados, concertados con el C-SIS, y que permite a los servicios de policía nacionales competentes consultar la información introducida en el C-SIS.

El SIS recibe el apoyo de la red de oficinas SIRENE establecidas en cada uno de los Estados. La oficina SIRENE (Supplementary Information Request at the National Entry) es el órgano de intercambio de información y comunicación bilateral entre las autoridades responsables de SIS en los países adheridos al Acuerdo Schengen.

Las oficinas SIRENE facilitan información complementaria sobre descripciones y coordinan las actuaciones en relación con estas últimas, garantizando además que se tomen las medidas adecuadas cuando se detenga a una persona buscada, cuando intente volver a entrar una persona a la que ya se ha denegado la entrada en el espacio de Schengen, cuando se encuentre a una persona desaparecida o cuando se confisque un coche o documentos de identidad robados. También intercambian datos relevantes para la cooperación policial y judicial, consultan bases de datos, coordinan operaciones transfronterizas, etc.

En este marco, la AEPD realiza actuaciones de control periódicas sobre la información que se incluye en la parte nacional del SIS.

Por otro lado, dentro del Consejo de la Unión Europea se define el Grupo de Trabajo en Temas de Schengen, dividido en cuatro subgrupos, uno de ellos específico para la evaluación de la adecuación al Acuerdo de Schengen. Los procedimientos de evaluación Schengen tienen como objetivo verificar el cumplimiento de la normativa aplicable por las administraciones de cada

uno de los Estados Miembros en el ámbito de sus competencias en los principales ámbitos cubiertos por el Acuerdo, incluyendo las disposiciones relativas a la protección de datos de carácter personal. El sistema de evaluación combina los requerimientos de información con visitas presenciales realizadas por equipos internacionales. Los resultados de esta evaluación, incluyen tanto la evaluación en sí como recomendaciones de mejora que son a su vez objeto de seguimiento en función de los compromisos asumidos por el estado miembro.

Las últimas evaluaciones realizadas a España tuvieron lugar en 2003 y 2010. La próxima evaluación tendrá lugar a comienzos del último cuatrimestre de 2017 en relación al grado de cumplimiento del acervo Schengen en el ámbito de la protección de datos de carácter personal.

Un aspecto importante que se toma en consideración es el nivel de cumplimiento y de progreso respecto a las recomendaciones realizadas como resultado de la evaluación previa.

El nuevo marco normativo vigente, actualizado desde la última evaluación, del Sistema de Información Schengen y del Sistema de Información de Visados ha venido a delimitar un marco de supervisión más estricto en el sentido de establecer una actuación más proactiva por parte de las autoridades de protección de datos.

Para cumplir con las obligaciones establecidas, se están llevando a cabo una serie de actuaciones de inspección por la AEPD tanto en el Sistema Nacional de Información de Schengen (N-SIS) como en el Punto Nacional del Sistema de Información de Visados (N-VIS).

En relación al N-VIS, en 2016 se han realizado inspecciones presenciales en:

- Servicios Centrales del Ministerio de Asuntos Exteriores y de Cooperación. (Dirección General de Españoles en el Exterior y de Asuntos Consulares y Migratorios y Subdirección General de Informática Comunicaciones y Redes de la Dirección General del Servicio Exterior).
- Oficinas consulares: Consulado de España en Casablanca (Marruecos).
- Empresa adjudicataria de la prestación de servicios de apoyo a las oficinas consulares.
- Comisaría de Extranjería y Fronteras del Ministerio del Interior.
- Puestos Fronterizos en Barcelona (Puerto y Aeropuerto)
- Subdirección General de Asilo de la Dirección General de Política Interior del Ministerio del Interior.

En relación con el NSIS, las actuaciones de inspección se realizarán en los primeros meses de 2017.

2.2.1.3. *Actuaciones de oficio en relación a quiebras de seguridad*

- Agencia Estatal de Administración Tributaria

En abril de 2016 la Agencia Estatal de Administración Tributaria (AEAT) notificó a la AEPD que se había producido una quiebra de seguridad en la campaña del IRPF. Dicha quiebra consistió en mostrar el borrador de la declaración de renta de 2.793 declarantes a terceros.

A raíz de dicha notificación, la AEPD realizó una inspección en la AEAT, instándola a que notificase a los afectados el filtrado de su información y constatando que la gestión de la incidencia fue diligente en cuanto al bloqueo de los sistemas y la corrección de los errores. Las actuaciones de inspección evidenciaron que los hechos se produjeron por un error de programación que no fue detectado en las fases de pruebas y en la puesta en producción. Por ello, se determinó iniciar un procedimiento de infracción de Administraciones Públicas.

- VTECH

La AEPD tuvo conocimiento de que a finales de noviembre de 2015 VTECH sufrió un ataque que dejó al descubierto datos de millones de usuarios (menores y adultos) de sus juguetes.

La AEPD inició actuaciones de oficio, realizando inspecciones en la filial española del grupo, y se están llevando a cabo acciones coordinadas con las autoridades de protección de datos de Holanda y de Hong-Kong, donde se encuentra localizada la responsabilidad de ciertos tratamientos de datos.

- Yahoo

Yahoo hizo público que había sufrido un ataque informático que podría haber afectado a más de mil millones de cuentas de sus usuarios. A partir de esta noticia la Agencia inició actuaciones de investigación para determinar las circunstancias en las que se produjo dicha quiebra de seguridad y analizar las medidas adoptadas por la empresa Yahoo para proteger de los datos de carácter personal de sus usuarios.

Aunque los hechos se produjeron en 2013 y 2014, el impacto para los usuarios ha sido de tal magnitud que es obligado realizar acciones para determinar si las circunstancias que permitieron tal quiebra se han identificado y eliminado, así como para obtener información de las campañas de prevención que ha realizado Yahoo entre sus usuarios en España para proteger la confidencialidad de sus datos.

Las acciones, debido a que ha afectado a usuarios de todo el mundo y en particular europeos, se están realizando en coordinación con el resto de autoridades europeas dentro del Subgrupo de Enforcement del GT29.

2.2.2. Ciudadanos mejor protegidos

Además de las inspecciones sectoriales que se han descrito en otros apartados de esta Memoria, la Agencia ha continuado tramitando las denuncias y las reclamaciones de tutela de derechos presentadas por los ciudadanos.

2.2.2.1. *Denuncias y tutela de derechos*

Cuando una persona formula una denuncia o una reclamación ante la Agencia lo hace porque considera que el derecho fundamental a la protección de sus datos personales ha sido vulnerado o corre un serio peligro de serlo y la respuesta ofrecida debe ser firme y ágil. Esta ha sido una de las motivaciones para introducir mejoras en la gestión que se enmarcan dentro de la profunda reorganización de la Agencia en estos últimos años, tal y como se viene explicando a lo largo de esta Memoria.

Las cifras de 2016 confirman la correcta orientación de todas estas medidas a la vista de sus resultados, lo que no significa que aún haya nuevas medidas que adoptar o pautas que corregir y, por tanto, recorrido por el que seguir mejorando. En cualquier caso si el 31 de diciembre de 2014 las denuncias y reclamaciones en tramitación ascendían a 5.401, el 31 de diciembre de 2016 el número de denuncias y reclamaciones en esta misma situación se redujo en un 43,73%, dejándolas en un total de 3.039. Ciertamente que el principal descenso se produjo en 2015, con la puesta en marcha en el último trimestre del año de la Unidad de Admisión, pero también es cierto que 2016 confirmó esa tendencia reductora, en particular por lo que a las denuncias se refiere.

Por otro lado, en 2016 también se ha seguido la estela ligeramente descendente en cuanto al número de solicitudes ciudadanas presentadas con una clara diferencia entre las denuncias que tuvieron entrada durante ese período cuyo volumen supone una disminución del 6,53% respecto al 2015 y las reclamaciones de tutela que tuvieron entrada, con un aumento del 24% en 2016 lo que, en ocasiones pueda encontrar explicación en la circunstancia de que cuando el ciudadano acude a la Agencia no lo hace tanto pensando o buscando la sanción punitiva del sujeto al que considera infractor de su derecho como la corrección del comportamiento que considera que le perjudica con independencia de cuál sea el procedimiento administrativo que se siga.

La combinación de varias circunstancias, entre ellas las descritas anteriormente (una importante reducción de las denuncias y reclamaciones «en tramitación» y una ligera disminución de las solicitudes que entraron durante 2016) junto con las medidas estratégicas y organizativas que se han ido incorporando, han permitido a la Agencia una

utilización más eficaz de los recursos con los que cuenta.

Descontando las inadmisiones a trámite, (4.681 en el 2016), las resoluciones de la Agencia aumentaron un 2'3% respecto al 2015 y un 7'34% respecto al 2014. En este sentido, destaca el incremento en un 16'7% de los procedimientos de apercibimiento y una reducción del 16% de las resoluciones con declaración de infracción económica.

Si se contabilizan también las resoluciones de inadmisiones a trámite, si bien el número de denuncias y reclamaciones resueltas ha descendido en el caso de las denuncias (–25,37%) y ha crecido en el caso de las reclamaciones (14,49%), esto debe matizarse si se tiene en consideración la muy importante reducción en el número de resoluciones de inadmisión de denuncias, es decir, la reducción de aquellas resoluciones que, por su propia naturaleza, no dan lugar a ninguna clase de actuación y que en 2016 han descendido en un –22,60% pasando de un total de 6.049 en 2015 a 4.681 en 2016. Este descenso en las denuncias inadmitidas significa, ni más ni menos, una mayor carga de trabajo para la Agencia que asume así un mayor número de actuaciones previas, investigadoras, instructoras… que responden a una política de acercamiento al ciudadano, que cada vez tiene más información sobre qué puede denunciar y cómo hacerlo, y que, finalmente, se traduce en el importante incremento en el número de expedientes iniciados en 2016 que han ascendido a un total de 2.826 frente a los 2.293 iniciados en 2015 o a los 2.199 iniciados en 2014, con un incremento del 28%, que corresponde a expedientes que serán resueltos en el 2017 una vez concluyan las actuaciones de investigación por los servicios de la inspección.

En lo referente a las resoluciones de tutela de derechos ARCO, si bien el número de reclamaciones mantiene un crecimiento anual por encima del 20% (24,30% en2016 y 23,30% en 2015), el número de inadmisiones y desistimientos también ha crecido en un 40,20%, con lo que el número total de resoluciones de tutelas se mantiene prácticamente estable (crece un 0,66%). Para poder admitir una tutela de derechos, es requisito legal que el ciudadano acuda previamente al responsable del tratamiento de sus datos y en bastantes ocasiones, por desconocimiento de éstos, acuden directamente a la Agencia.

Este conjunto de datos demuestra que durante el año 2016 la actividad de la Agencia se ha diversificado e intensificado buscando el mejor servicio al ciudadano y sin merma de lo que podemos llamar la *eficacia administrativa* a la vista de que los tiempos medios de gestión, con carácter general, se están reduciendo. Destaca un descenso del 40% en los tiempos de archivo de la denuncia que no requiere actuaciones de investigación, de un 53% de las actuaciones que se archivan tras no subsanar el ciudadano la denuncia y del 30'92% de los procedimientos de apercibimiento.

El análisis conjunto de todos los indicadores presentados en 2016, junto con las tendencias de los últimos dos años confirman que las mejoras en la gestión emprendidas en toda la Agencia están dando sus frutos de forma progresiva, e invitan a pensar que esta dinámica continuará en 2017.

En relación con el incremento de los apercibimientos frente a la imposición de sanciones debe señalarse que son muchas las ocasiones en las que los hechos denunciados e investigados ponen de relieve la concurrencia de circunstancias que permiten a la Agencia apercibir al denunciado sobre la irregularidad de su conducta en lugar de imponer una sanción, exigiéndole la corrección de la misma, cuando no lo ha hecho previamente, y el suministro de la información necesaria que acredite la adopción de tales medidas. Se trata de un mecanismo, el del apercibimiento, más rápido y más eficaz a la hora de conseguir la adecuación de los comportamientos infractores o en riesgo de serlo y, con ello, más eficiente a la hora de garantizar los derechos ciudadanos en esta materia.

En cuanto a la naturaleza de las denuncias tramitadas, cabe destacar el notable aumento de los casos de morosidad y de contratación irregular. Ambas modalidades suponen el grueso de las quejas que recibe cotidianamente la Agencia, y de ahí que se haya optado por darles un tratamiento singularizado en el apartado de La

Agencia en cifras. Otras tendencias menos acusadas se refieren al suave descenso de los casos de videovigilancia y spam, supuestos ambos que, cuando las circunstancias legales y reglamentarias lo permiten, están siendo objeto no de la imposición de sanciones sino del correspondiente apercibimiento al sujeto infractor con las connotaciones anteriormente mencionadas. Por otra parte, hay una mayor presencia de expedientes relativos al sector público, al sanitario y al laboral. En paralelo a lo descrito hasta aquí, el mayor número y porcentaje de sanciones impuestas han recaído en infracciones cometidas por la inclusión indebida en los llamados «ficheros de morosos» y, en segundo lugar, en supuestos de contratación irregular.

Con respecto a la tutela de derechos de acceso, rectificación, cancelación y oposición (ARCO) el 14% de las reclamaciones han sido estimatorias y un 10% adicional parcialmente estimatorias. Un año más, el derecho más tutelado es el de cancelación que representa un 63% de las reclamaciones presentadas.

Destaca el incremento en un 40% de reclamaciones inadmitidas o archivadas, pues en muchas ocasiones el ciudadano no ha presentado previamente su reclamación ante la entidad responsable del tratamiento de datos o ha desistido de su solicitud.

Por esta razón en 2017 la Agencia actualizará los contenidos prácticos para orientar a los ciudadanos sobre cómo ejercer el derecho al olvido en los principales buscadores de internet.

2.2.2.2. *Ficheros de solvencia patrimonial*

En este sector de actividad destacan dos líneas de actuación de la Agencia. La primera es el control del cumplimiento de los requisitos requeridos para la inclusión de datos de carácter personal en este tipo de ficheros por parte de las entidades acreedoras y la segunda el control del cumplimiento de las obligaciones exigibles para el mantenimiento de datos de carácter personal en estos ficheros por parte de las entidades responsables de los mismos.

En el primer caso, destacan las denuncias sobre la ausencia del requerimiento previo de pago o el incumplimiento de los requisitos necesarios para su validez. En especial llama la atención el del carácter previo del requerimiento y la acreditación de haberse realizado el envío o la recepción efectiva por el destinatario.

En menor cuantía aparecen las denuncias por otro tipo de deficiencias de tipo formal que también invalidan el propio requerimiento realizado, como es la falta de información al afectado sobre la posibilidad de incluir sus datos en ficheros de solvencia patrimonial.

Dentro de esta línea es preciso señalar que, aunque la concesión de un determinado plazo para proceder al pago de la deuda no constituye una obligación del acreedor, cuando se otorga al afectado un plazo para el abono de la deuda y éste no se cumple o bien no se otorga dicho plazo pero se procede a realizar la inclusión simultáneamente a la notificación, se declara una infracción.

En la línea de control del cumplimiento de las obligaciones exigibles para el mantenimiento de datos de carácter personal en los ficheros de solvencia, los hechos denunciados más frecuentes hacen referencia a la falta de acreditación del envío o recepción de la notificación de inclusión al afectado.

Aunque en menor medida, también se han tramitado denuncias que concluyen con una declaración de infracción cuando los procedimientos de notificación del requerimiento de pago o de inclusión en el fichero de solvencia patrimonial no se efectúan a través de un medio fiable, auditable e independiente de la entidad notificante.

Por último, hay que destacar aquellos casos en los que se denuncia que la deuda se encuentra en litigio, bien en sede judicial o administrativa, cuestionándose su certeza y, sin embargo, se incluye o mantiene en este tipo de ficheros.

2.2.2.3. *Contratación irregular*

En la contratación irregular destaca el relevante aumento de denuncias por contrataciones de microcréditos a distancia a través de una web. La falta de protocolos adecuados por parte de este tipo de entidades para proceder a la identificación inequívoca de los solicitantes de crédito da lugar a imputaciones erróneas a terceros ajenos, provocando los consiguientes perjuicios en materia de protección de datos a los afectados.

También deben mencionarse las denuncias respecto de las contrataciones realizadas por entidades de telecomunicaciones. La liberalización del sector de telecomunicaciones permite que los ciudadanos puedan cambiar de entidad que les suministra los servicios. Sin embargo, la falta de diligencia por parte de algunas entidades prestadoras de este tipo de servicios da lugar a tratamientos ilícitos de datos personales de terceros, al tiempo que los protocolos de identificación y para recabar el consentimiento no se cumplen o son defectuosos impidiendo su acreditación.

2.2.2.4. *Entidades financieras*

En el sector de las entidades financieras, las denuncias revelan que con frecuencia se descuidan las garantías en materia de protección de datos de los afectados.

Es el caso de las quitas judiciales que no se aplican a la cuantía de la deuda dando lugar no sólo a asientos contables inexactos sino a comunicaciones a terceros de datos inexactos, en especial a los ficheros de solvencia patrimonial antes aludidos, o a la Central de Información de Riesgos del Banco de España (CIRBE).

Dentro del sector de entidades financieras, las entidades aseguradoras y las de mediación han generado un incremento de denuncias como consecuencia de ciertas debilidades que se acusan en el tratamiento de los datos de los ciudadanos. Esto sucede especialmente en tratamientos de cambio de tomador del seguro, que originan que la prima a abonar se impute contra una cuenta bancaria sin el adecuado soporte físico que permita acreditar el consentimiento para tal tratamiento. En cuanto a los corredores de seguros, la infracción más común se refiere a la gestión de nuevas contrataciones de antiguos clientes sin su consentimiento. Por último, en cuanto a los agentes de banca-seguros se aprecia que la infracción principal es la falta de soporte documental que acredite el consentimiento para la contratación.

2.2.2.5. *Entidades de recobro de deudas*

Las entidades de recobro de deudas suelen tener la condición de encargadas del tratamiento por cuenta del responsable para averiguar los datos identificativos del deudor al objeto de facilitar el cobro de la deuda reclamada. No obstante, en esta labor de identificación suelen incurrir en tratamientos indebidos cuando la persona supuestamente identificada no se corresponde con la verdadera deudora, dando lugar además, a un enriquecimiento ilícito de datos en el fichero del responsable. Debe señalarse que con respecto a este tipo de entidades que se nutren de información de terceros (como son los detectives privados, entre otros) abundan los tratamientos ilícitos. A veces se debe a la falta de diligencia en la comprobación de la identificación facilitada, y en otras ocasiones a la ausencia de protocolos adecuados que permitan regularizar diligentemente las identificaciones erróneas y la resolución de las reclamaciones mediante un contacto adecuado con el acreedor al que prestan servicio.

2.2.2.6. *Comunicaciones comerciales*

Al igual que en años anteriores, la mayor parte de los procedimientos sancionadores tramitados por el envío de comunicaciones postales han tenido como base el hecho de que los responsables de los envíos no pudieran acreditar el origen de los datos utilizados en la campaña publicitaria.

Asimismo, siguiendo una tendencia anterior, se ha analizado la participación en las campañas publicitarias de los anunciantes y otros sujetos que intervienen en la selección del público objetivo de la acción publicitaria, a fin de determinar su responsabilidad en el tratamiento de los datos utilizados en la campaña, cuando dicho tratamiento

no se ha amparado en ninguna de las causas que lo legitiman. Todo ello en aplicación de lo que dispone el Reglamento de desarrollo de la LOPD en cuanto a la responsabilidad de las entidades que fijan los parámetros identificativos de los destinatarios de la campaña publicitaria.

Por otro lado resulta interesante destacar que, respecto del ejercicio anterior, han disminuido los expedientes de investigación seguidos como consecuencia de las denuncias presentadas por los destinatarios de llamadas telefónicas realizadas con fines de venta que se habían opuesto a recibir este tipo de comunicaciones, bien a través del ejercicio del derecho de oposición o bien con motivo del registro de su línea telefónica en el servicio de la Lista Robinson.

También en el ámbito de las comunicaciones publicitarias realizadas telefónicamente, deben resaltarse los procedimientos sancionadores abiertos contra empresas contratadas por el responsable del tratamiento para desarrollar y ejecutar una campaña, llevándola a cabo contraviniendo las instrucciones dadas por el responsable y las cláusulas contractuales pactadas en el contrato de prestación de servicios suscrito por ambas partes.

2.2.2.7. *Videovigilancia*

A lo largo del año 2016 se viene a confirmar la tendencia general de los ejercicios anteriores en materia de videovigilancia. Así, la mayoría de las resoluciones recaídas en este ámbito han sido de apercibimiento.

No obstante, para determinar si procede la aplicación del citado precepto al tratamiento de imágenes de personas físicas identificadas o identificables realizado a través de cámaras y/o videocámaras, habrá de aplicarse la regla de ponderación prevista en el mismo. Esto es, será necesario valorar si en el supuesto concreto de la instalación del sistema de videovigilancia existe un interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos que prevalezca sobre el interés o los derechos y libertades fundamentales del ciudadano.

2.2.2.8. *Otras áreas de actividad relevantes*

Aunque las cifras no resultan significativas a nivel global, en el sector de los directorios de telecomunicaciones se aprecia un incremento de las denuncias relacionadas con la publicación de datos; generalmente en directorios telefónicos de Internet. En 2016 la proporción ya llega al 1,3% del total de denuncias, cuando en los años anteriores no llegaban al 1%. Lo significativo es que la mayoría de los directorios denunciados son responsabilidad de compañías que no tienen establecimiento en España y cuyo funcionamiento no se ajusta a la normativa prevista en la normativa española para la elaboración de guías telefónicas. Varias de estas compañías están ubicadas en Alemania y en Panamá. En estos casos la Agencia, ejerciendo sus competencias, solamente puede remitir a los ciudadanos a las autoridades nacionales correspondientes. Es el caso de 411numbers.es, que acumula la mayor parte de las denuncias recibidas a este respecto, y que para atender las solicitudes de cancelación de los afectados cobra una tasa.

En el sector de sanidad se mantiene básicamente el número de denuncias recibidas por accesos injustificados a las historias clínicas de los denunciantes, que en muchos casos son médicos y denuncian los accesos de sus compañeros. También se han investigado algunos incumplimientos de medidas de seguridad relacionadas con extravíos de documentos que forman parte de historias clínicas, y por envío de datos de salud a través de fax o por correo electrónico sin encriptar.

En lo relativo a relaciones laborales, la Agencia ha sancionado nuevamente a empresas por la utilización de localizador GPS en las Personal Digital Assistant (PDAs) de los trabajadores sin informarles de ello.

Asimismo, se siguen recibiendo numerosas denuncias que han dado lugar a apercibimientos, procedimientos de declaración de Administraciones Públicas o procedimientos sancionadores, sobre el abandono de documentación con datos personales en la vía pública.

En el sector educativo destacan las denuncias como consecuencia de la publicación de fotos de menores por parte de los centros de enseñanza sin que haya consentimiento de los padres, siendo frecuente que las denuncias sean de padres separados y que haya consentido uno de ellos. En estos supuestos es frecuente el archivo de las actuaciones por concurrir una conducta diligente por parte de los centros, excepto en los casos en que los padres hayan manifestado criterios distintos. De existir esta controversia debe evitarse la publicación de las fotos hasta que exista un pronunciamiento de la jurisdicción competente.

Se ha sancionado también en este ejercicio la publicación sin restricciones de listas de admitidos y de clasificaciones de personas que concurren a procesos de concurrencia competitiva.

En cuanto a partidos políticos, la mayoría de las denuncias del 2016 han sido objeto de inadmisiones a trámite. Al tratarse de un año electoral, se han recibido varias denuncias sobre la publicidad electoral sin previo consentimiento de los afectados, que se archivan porque la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General habilita a que los partidos políticos envíen propaganda de este tipo durante el período previo a las elecciones. También se han recibido algunas denuncias motivadas por la remisión de correos electrónicos sin poder indicar el origen del mismo y el consentimiento del afectado.

Finalmente, en el ámbito de las comunidades de propietarios se consolida el criterio de tramitación de apercibimiento en las denuncias por publicación de datos de deudores a los que ya se ha notificado su deuda en los accesos a las viviendas, denuncias entre vecinos y contra la comunidad, y sentencias judiciales sobre litigios en los que se encuentran inmersas las partes.

Desde otra perspectiva, durante 2016 se han continuado las actuaciones de seguimiento de los cambios introducidos por Google en su política de privacidad como parte del seguimiento de la resolución adoptada en diciembre de 2013 por la Agencia Española en el marco de la acción coordinada desarrollada por varias autoridades europeas de protección de datos.

En este sentido, hay que recordar que Google introdujo cambios sustanciales en sus términos de uso y en su política de privacidad en 2012. Varias autoridades europeas, entre ellas la Agencia Española, iniciaron procedimientos encaminados a determinar la adecuación de esa nueva política a la normativa de protección de datos y a asegurar el respeto a los derechos de los interesados en el funcionamiento de los servicios de la compañía.

En el caso español, esas actuaciones condujeron a la imposición de tres sanciones de 300.000 euros cada una, por incumplimiento de diversas disposiciones de la LOPD, así como a requerir a la compañía para que introdujera cambios en sus términos de uso y política de privacidad.

Durante 2015 la compañía introdujo varios de los cambios solicitados y se comprometió a llevar a cabo otros a lo largo de 2016, así como a informar regularmente a la Agencia sobre las novedades que pudieran irse produciendo en las características de sus servicios y que pudieran tener un impacto en materia de protección de datos.

A lo largo de 2016 se ha realizado un seguimiento de la implantación de las modificaciones anunciadas por la compañía, constatándose que a comienzos de ese año se habían aplicado la mayor parte de ellas. Asimismo, la compañía ha respondido a su compromiso de consultar con la Agencia algunas modificaciones significativas que se han producido durante 2016 en el modo en que se relacionan con los usuarios de sus servicios.

Estas iniciativas han sido complementadas a nivel europeo con el envío de una carta a Google en junio de 2016 por parte del Grupo de Autoridades Europeas de Protección de Datos, el Grupo del Artículo 29. En esa carta, el Grupo reconocía los cambios realizados por la compañía a nivel mundial, en línea con los requerimientos y recomendaciones formuladas por varias autoridades, incluida la Agencia Española, y solicitaba la introducción de mejoras adicionales que reforzaran la adecuación de la política de privacidad a la normativa de protección de datos.

2.2.2.9. *Reclamación de tutela de derechos*

El aumento de reclamaciones en este ámbito se debe principalmente a las presentadas respecto de los ficheros de solvencia patrimonial.

El derecho de cancelación ha sido de nuevo el derecho más reclamado, refiriéndose a ficheros de solvencia patrimonial casi el 25% de las reclamaciones planteadas.

Dentro de las reclamaciones por la denegación del derecho de cancelación ante los ficheros de solvencia patrimonial, la mayoría de los casos se producen por negar el reclamante la existencia de la deuda que ha sido inscrita en los citados ficheros por parte, sobre todo, de compañías de telecomunicaciones o de empresas que compran créditos.

La inclusión en los ficheros de solvencia patrimonial de deudas, muchas veces por una escasa cuantía, es una práctica habitual por parte de las empresas de telecomunicaciones, banca y energía. Esta práctica conlleva importantes consecuencias desfavorables para las personas inscritas en ellos, como negación de créditos o imposibilidad de contratar ante determinadas entidades. Por ello, resulta fundamental determinar si la inclusión en los citados ficheros se realiza dando cumplimiento a lo establecido en la normativa de protección de datos, y verificar si se atienden los derechos presentados por los afectados frente a la inclusión en esos ficheros.

Otro grupo de reclamaciones muy relevante es el referido al derecho de cancelación frente a los buscadores generalistas por enlaces donde se hace referencia a hechos obsoletos. En el año 2016 deben destacarse las sentencias del Tribunal Supremo contra Google Spain S. L., donde el Tribunal señaló que no se puede considerar corresponsable a una entidad (Google Spain) que no tiene ninguna participación en la gestión del motor de búsqueda y la determinación de los fines y medios del tratamiento. Con esta sentencia se concluye que en ese caso el interesado debe dirigirse al domicilio legal de la entidad, que se encuentra fuera de España. La citada compañía ha habilitado un formulario online para el ejercicio del derecho por parte de los afectados. La sentencia de comenta en un apartado posterior de la Memoria.

En el entorno de los buscadores, foros, blogs y páginas web en general se observa un incremento de las reclamaciones derivadas de los constantes tratamientos de datos que se producen en una sociedad digital. En ese entorno digital, que proporciona innumerables ventajas a los ciudadanos, se producen con frecuencia importantes vulneraciones de la privacidad. El anonimato con que se participa en el mismo dificulta extraordinariamente en ocasiones la posibilidad de dar una respuesta eficaz para impedir infracciones a la normativa de protección de datos.

Otros problemas añadidos en un mundo globalizado como el actual es la dificultad para tutelar los derechos ARCO frente a entidades que radican fuera de España y carecen de establecimientos en España o bien en las que las filiales en nuestro país no desarrollan actividades en el contexto de las cuales tengan lugar tratamientos de datos. También representa una dificultad el hecho de que los servidores se encuentren en el extranjero y, en el caso de los foros, que no sea posible identificar a los administradores.

Por último, se observa una mayor preocupación de los afectados en el tratamiento de sus datos en los historiales clínicos, como se aprecia por el número de reclamaciones referidas al derecho de acceso y a los derechos de rectificación y cancelación. Destacan los casos en que la Agencia ha tutelado el derecho de acceso, por no entregar o entregar de forma incompleta la historia clínica a los pacientes.

2.2.2.10. *Sentencias sobre resoluciones de la Agencia*

El análisis del grado de seguridad jurídica en la aplicación de la LOPD obliga a contemplar en qué medida las resoluciones de la Agencia Española de Protección de Datos 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 74 sentencias, de las cuales:

- 54 fueron desestimatorias de los recursos formulados contra resoluciones de la Agencia (que quedaron plenamente confirmadas) (73%).
- 4 estimaron parcialmente los recursos (5%).
- 12 estimaron íntegramente las pretensiones anulatorias de las resoluciones de la Agencia (17%).
- 4 inadmitieron los recursos interpuestos contra resoluciones de la Agencia (5%).

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 78%, lo que supone un incremento de dos puntos respecto del año 2015. Dentro de esta cifra, se mantiene el porcentaje de sentencias desestimatorias del recurso, incrementándose el correspondiente a los supuestos de inadmisión. Se confirma así la relevancia del porcentaje de supuestos en que las sentencias confirman las resoluciones de la Agencia previa valoración jurídica de los criterios de fondo que la fundan. En todo caso, el porcentaje de sentencias que confirma las resoluciones de la Agencia es el más elevado desde el año 2005.

Por otra parte, se observa un notabilísimo descenso de la litigiosidad referida a la actuación de la Agencia, por cuanto el número total de sentencias se reduce en más de un 60%, siendo el descenso acumulado de la litigiosidad si se compara con las cifras de 2013 de más de un 73%.

En relación con los sectores de actividad a los que afectan las sentencias dictadas, se ha producido, en consonancia con lo anteriormente señalado, una disminución en la práctica totalidad de los sectores. No obstante, resulta relevante el peso adquirido respecto del total por los sectores de las telecomunicaciones, banca y seguros y agua y energía. Así, mientras en 2015 estos sectores representaban solamente un 45% del total, este porcentaje se incrementa en 2016 hasta casi el 60%.

De ellos, como en años anteriores, el sector que presenta una mayor litigiosidad sigue siendo el de las telecomunicaciones, con un 31% del total, aunque reduciéndose en términos absolutos en un 58%; es decir, un porcentaje similar al de la reducción general del número de sentencias dictadas. No ocurre lo mismo con el sector financiero, que aunque disminuye su número lo hace sólo en un 33%, incrementándose su peso en el total en siete puntos porcentuales.

Por el contrario, se produce un enorme descenso de las sentencias relacionadas con prestadores de servicios de la sociedad de la información, que descienden de 46 en 2015 a una sola en 2016. No obstante, ello se debe únicamente a la práctica desaparición de los supuestos relacionados con los derechos de cancelación u oposición en el motor de búsqueda de Google.

Es igualmente significativo el descenso de sentencias referidas a recursos formulados por particulares, que descienden un 62% y sindicatos y asociaciones empresariales, en que el descenso es de un 71% respecto de 2015, así como la inexistencia de sentencias en supuestos en que el recurrente fuera una entidad dedicada al mantenimiento de ficheros de solvencia patrimonial y crédito.

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. Además, en una de las cuatro sentencias parcialmente estimatorias se produce simplemente la aplicación retroactiva de las disposiciones de la Ley de Servicios de la Sociedad de la información referidas a la posible reducción de la cuantía de las multas, introducida por la Ley General de telecomunicaciones.

Por su parte, el Tribunal Supremo dictó un total de 68 resoluciones (66 sentencias y 2 autos) referidas a recursos de casación interpuestos frente a sentencias dictadas en procesos en los que era parte la Agencia. A diferencia de lo sucedido en años anteriores, el número de recursos ha sufrido un gran incremento, multiplicándose casi por ocho. No obstante, ello se debe exclusivamente a la presentación por parte de Google Spain de un total de 63 recursos de casación contra sentencias de la Audiencia Nacional relacionadas con el ejercicio de los derechos de oposición o cancelación frente al motor de búsqueda. De este modo, al margen de este supuesto sólo cabría hacer referencia a cinco resoluciones del Tribunal Supremo.

En relación con estos recursos, el Tribunal Supremo:

- Declaró en 63 sentencias haber lugar a los recursos interpuestos contra sentencias que habían confirmado las resoluciones de la Agencia, que fueron así anuladas.
- Acordó en dos supuestos la inadmisión del recurso.
- Declaró en tres sentencias no haber lugar a los recursos interpuestos contra sentencias que confirmaban las resoluciones de la Agencia, que quedaron a su vez confirmadas.

Como puede comprobarse, estas cifras se encuentran claramente influidas por la doctrina emanada de las sentencias dictadas en relación con los recursos de Google Spain, a la que se hará referencia con posterioridad. Fuera de estos supuestos, el criterio de la Agencia ha sido siempre confirmado por el Tribunal Supremo.

De las materias analizadas por la Audiencia Nacional destacan las siguientes cuestiones:

- En relación con el ámbito de aplicación de la Ley, las SAN de 4 de marzo de 2016 y 23 de marzo de 2016 consideran aplicable la exclusión del artículo 2.3 del RLOPD en el caso de tratamiento de datos de un empresario individual en ficheros de solvencia patrimonial y crédito referidos adeudas contraídas en su ejercicio empresarial. A su vez, en cuanto al concepto de dato personal la SAN de 5 de julio de 2016 considera que tiene tal condición el número de cuenta corriente, incluso si no va acompañado de otros datos adicionales.
- La AN ha considerado vulnerado el principio de exactitud por el tratamiento del número de teléfono de una persona que se había asociado a otro abonado (SAN de 12 de abril de 2016) y por el cargo de facturas telefónicas a una cuenta corriente distinta de la que comunicó a tales efectos el abonado, aun siendo éste titular de ambas cuentas (SAN de 2 de noviembre de 2016).
- La SAN de 10 de mayo de 2016 considera incumplido el deber de información al afectado si una cláusula informativa prevé el tratamiento de los datos con fines de envío de comunicaciones comerciales sin permitir al interesado marcar una casilla, incluso aunque los datos no se hayan empleado en la práctica para tales fines, dado que en ese caso habría un tratamiento ilegítimo.
- En relación con la legitimación para el tratamiento, la SAN de 23 de septiembre de 2016 considera que puede fundarse en el artículo 7 f) de la Directiva 95/46/CE el tratamiento de datos con fines de videovigilancia. Por su parte, se ha apreciado que no existe legitimación en el caso de publicación en redes sociales de información calumniosa de la denunciante suplantando su identidad (SAN de 2 de febrero de 2016); así como en caso de mantenimiento en la Central de información de riesgos del Banco de España de información sobre un riesgo de crédito sobre el que existía acuerdo transaccional (SAN de 3 de mayo de 2016); en el caso de uso de datos de la cuenta corriente de un cliente para cargar recibos correspondientes a su hermana fallecida (SAN de 5 de julio de 2016); o en el acceso por la matriz de un grupo eléctrico a los datos de los clientes de su comercializadora (SAN de 28 de octubre de 2016).
- Son como siempre abundantes las sentencias referidas a supuestos de contratación

irregular. En este punto, la SAN de 21 de junio de 2016 insiste en la competencia de la AEPD, al considerar que el conflicto entre el operador y el cliente es estrictamente materia de protección de datos. A su vez, se aprecia la existencia de irregularidades en caso de aportación del DNI de persona distinta (SAN de 6 de abril de 2016), existencia de denuncia por suplantación en la llamada de verificación del contrato (SAN de 15 de abril de 2016), falta de constancia de la verificación (SAN de 12 de julio de 2016), uso de datos obtenidos para otras finalidades a fin de suplantar la identidad del interesado en el contrato (SAN de 10 de noviembre de 2016) o celebración del contrato por persona distinta del abonado, constando esta circunstancia –en este caso se trataba de la madre de la denunciante– (SAN de 10 de noviembre de 2016). En un supuesto especial, en que se utilizaron en el contrato los datos de una persona que se había dado de alta en un fichero de exclusión publicitaria, la AN confirmó la resolución de la AEPD en que se imponían dos sanciones, tanto por la realización del actividad publicitaria a quien figuraba en un fichero de exclusión como por el tratamiento ilícito de sus datos (SAN de 12 de marzo de 2016).

- En relación con la tutela de los derechos de acceso, rectificación, cancelación y oposición, la SAN de 28 de junio de 2016 recuerda que es requisito *sine qua non* para solicitar la tutela de la AEPD haber ejercitado el derecho ante el responsable. A su vez la SAN de 7 de octubre de 2016 considera suficiente el acceso otorgado a la historia clínica de la afectada que incluía documentos de una antigüedad superior a los diez años. Por último, la SAN de 18 de marzo de 2016 recoge la doctrina del Tribunal Supremo en cuanto a la legitimación pasiva en los supuestos de ejercicio del derecho de oposición frente al motor de búsqueda de Google.

- En materia de seguridad, la AN reitera su criterio de que no cabe exonerar la responsabilidad mediante la mera alegación de la existencia de un error informático, considerando vulnerada la LOPD en supuestos como la existencia de una quiebra de seguridad que posibilitó el acceso en banca electrónica a los datos de clientes distintos del usuario (SAN de 5 de febrero de 2016) o el acceso libre en Internet a una aplicación de gestión de expedientes de tasación judicial en que aparecían los datos de peritos y deudores (SAN de 24 de junio de 2016).

- En relación con los ficheros de solvencia patrimonial y crédito, la SAN de 29 de abril de 2016 declaró la responsabilidad de una empresa de recobro española en caso de cesión de deuda a una empresa situada en otro Estado miembro, figurando como acreedora en el fichero la entidad de recobro. A su vez, se ha considerado ilícita la inclusión de una deuda antes del cumplimiento del plazo establecido para el pago en el requerimiento remitido al deudor (SAN de 27 de septiembre de 2016) o de deudas que habían sido sometidas a arbitraje de una Junta Arbitral de Consumo, habiéndose incluso denegado el derecho de cancelación ejercido con posterioridad al sometimiento a arbitraje (SAN de 21 de octubre de 2016)

- Son reiteradas las sentencias relacionadas con la exigencia de requerimiento de pago previa a la inclusión de la deuda, siendo destacable la SAN de 4 de noviembre de 2016, que considera este requisito conforme a las exigencias para incurrir en mora derivadas de los artículos 1100 del Código Civil y 63 del Código de Comercio. En todo caso, múltiples sentencias recuerdan que no basta acreditar la puesta en correo y falta de devolución del requerimiento si se niega su recepción por el deudor (SSAN de 29 de abril, 28 de junio o 28 de octubre de 2016). Por su parte, la AN niega la suficiencia del requerimiento efectuado por SMS (SSAN de 6 de octubre y 4 de noviembre de 2016) y por correo electrónico (SAN de 4 de noviembre de 2011). Finalmente, la SAN de 11 de mayo de 2016 considera probada la existencia de requerimiento como con-

secuencia de la propia acción del afectado que ponía de manifiesto las inexactitudes en el pago requerido.

- En el ámbito del tratamiento con fines de publicidad y prospección, la AN considera inexistente la infracción denunciada si el interesado no puede acreditar que efectivamente se opuso al tratamiento de sus datos para estos fines (SAN de 12 de abril de 2016), considerando por el contrario suficiente para entender vulnerada la LOPD la realización de una sola llamada publicitaria a quien se había incluido en un fichero de exclusión (SAN de 31 de mayo de 2016).

- En relación con la infracción del artículo 21 de la LSSI, la SAN de 16 de septiembre de 2016 considera masivo el envío de cuarenta correos electrónicos a seis direcciones distintas del afectado, añadiendo que no es necesario que el interesado manifieste su negativa a seguir recibiendo las comunicaciones desde la dirección a la cual se han remitido. Por otra parte, la SAN de 16 de septiembre de 2016 rebaja la sanción como consecuencia de la aplicación del régimen más favorable contenido en la reforma operada por la Ley General de Telecomunicaciones.

- En cuanto a la aplicación de los criterios establecidos en los apartados 4 y 5 del artículo 45 de la LOPD, la SAN de 31 de mayo de 2016 aclara que los criterios del apartado 4 que hayan sido tenidos en cuenta para apreciar una cualificada reducción de la antijuridicidad o culpabilidad no deben ser tenidos nuevamente en cuenta para determinar la cuantía de la sanción. En cuanto a los supuestos en que se aprecia la aplicación del artículo cabe hacer referencia a la regularización diligente al haberse corregido una quiebra de seguridad en un período inferior a un día desde su conocimiento (SAN de 5 de febrero de 2016) o la subsanación inmediata cuando se tuvo conocimiento de la existencia de diligencias de investigación (SAN de 21 de julio de 2016), así como la falta de intencionalidad en el caso de cargo de una factura en cuenta distinta a la declarada pero perteneciente al mismo titular (SAN de 2 de noviembre de 2016). En todo caso, las SSAN de 5 de abril y 7 de junio de 2016 recuerdan que la aplicación de este precepto es excepcional y no puede apreciarse de forma automática.

- En relación con el apercibimiento, la AN ha reiterado su naturaleza no sancionadora en las SAN de 12 de abril, 31 de mayo, 24 de junio y 21 de julio de 2017), por lo que no cabe su aplicación sustitutoria de la sanción impuesta ni su aplicación sustitutiva en caso de infracción leve (SAN de 23 de septiembre de 2016). Además, se recalca que en caso de que proceda la sanción por desatender las medidas exigidas por el requerimiento el responsable ya no puede efectuar alegaciones acerca de la inadecuación del apercibimiento (SAN de 19 de mayo de 2016).

En cuanto al Tribunal Supremo, como ya se ha indicado, la mayor parte de las sentencias de la Sala Tercera dictadas en el año 2016 en relación con el derecho fundamental a la protección de datos de carácter personal estiman los recursos de casación interpuestos por la representación procesal de Google Spain contra sentencias de la Audiencia Nacional que desestimaban o estimaban parcialmente recursos contencioso-administrativos contra resoluciones en que la AEPD ordenaba la supresión de determinados resultados en los índices de los motores de búsqueda cuando el criterio de búsqueda era el nombre y apellidos del afectado que había ejercido el comúnmente denominado «derecho al olvido». En todo caso, es preciso señalar que tales sentencias no analizan la procedencia o improcedencia de la desindexación aplicando los criterios sentados por la sentencia del tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, sino que únicamente analizan la cuestión relativa a la legitimación pasiva de Google Spain.

Así, a partir de la sentencia de 11 de marzo de 2016 se dictaron varias sentencias en que el Tribunal Supremo apreció la falta de legitimación pasiva de la citada entidad al considerar que, sin perjuicio de que la realización de tratamientos en

el entorno de su actividad ha de ser considerada como punto de conexión para la aplicación de la legislación española de protección de datos, lo cierto es que el tratamiento se lleva a cabo materialmente por Google Inc., lo que implica que la solicitud de desindexación debe dirigirse a la misma, debiendo igualmente referirse a dicha entidad la resolución que en su caso pudiera dictar la AEPD estimando la tutela que fuera planteada en caso de no haber sido atendido el derecho.

No obstante, la sentencia de la Sala Primera del Alto Tribunal de 5 de abril de 2016 sentó una doctrina que en principio se oponía a la contenida en aquellas sentencias, al considerar que la acción de cesación por intromisión ilegítima en el derecho a la intimidad derivada de la publicación de los resultados podría ejercitarse contra la filial española del motor de búsqueda.

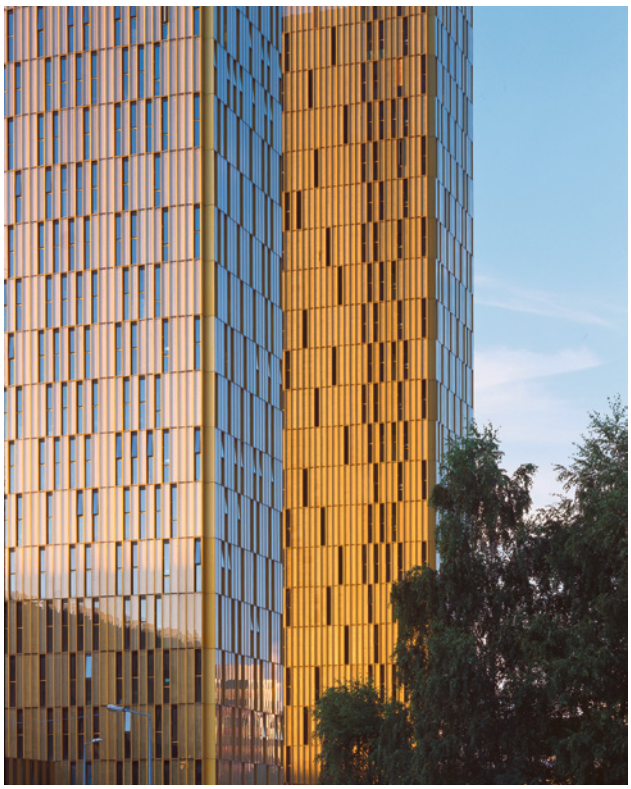
Sin embargo, la Sala Tercera del Tribunal Supremo, en sentencias posteriores a la que acaba de mencionarse, a partir de la de 13 de junio de 2016, se ratificó en su criterio de que el derecho de cancelación o de oposición habría de ejercitarse ante Google Inc., estimando así los recursos interpuestos por Google Spain. Como cuestión relevante, estas últimas sentencias toman como criterio interpretativo para la resolución de los recursos las previsiones contenidas en el Reglamento General de Protección de Datos.

2.2.2.11. *Sentencias TJUE*

Durante 2016 ha sido particularmente relevante la doctrina jurisprudencial emanada del Tribunal de Justicia de la Unión Europea (TJUE), debiendo hacer especial mención de tres casos tramitados ante el mismo.

Así, cabe en primer lugar hacer referencia a la sentencia de 28 de julio de 2016 (asunto C 191/15; Amazon EU Sàrl), relacionada con la determinación de la ley aplicable, en la que se planteaba al Tribunal si un tratamiento de datos personales efectuado por una empresa de comercio electrónico se rige por el Derecho del Estado miembro al que esa empresa dirige sus actividades aunque no tenga en ella un establecimiento.

El Tribunal analiza su jurisprudencia relacionada con la aplicación del artículo 4.1 a) de la Directiva 95/46/CE, recordando la necesaria concurrencia de dos requisitos: la existencia de un establecimiento y que el tratamiento se lleve a cabo en el marco de sus actividades. Respecto de la primera, y tras recordar su doctrina no formalista sobre el concepto de establecimiento concluye que «si bien el hecho de que la empresa responsable del tratamiento de datos no posea una filial ni una sucursal en un Estado miembro no excluye que pueda tener en su territorio un establecimiento (…) ese establecimiento no puede existir por el mero hecho de que allí se pueda acceder al sitio de Internet de la empresa en cuestión». Respecto de la segunda, recuerda que no es preciso que el tratamiento se lleve materialmente a cabo por el establecimiento, sino únicamente en el marco de sus actividades, siendo el órgano judicial nacional el que a la vista de las circunstancias que sean relevantes deba determinar si concurren ambos requisitos.



G. Fessy. © TJUE

En segundo lugar, debe hacerse referencia a la sentencia de 19 de octubre de 2016 (asunto C-582/14; Breyer), que se refiere al concepto de dato personal y a la aplicabilidad de la regla de ponderación de derechos e intereses establecida en el artículo 7 f) de la Directiva 95/46/CE.

En primer lugar, se plantea si puede considerarse dato de carácter personal para un prestador de servicios de medios en línea el dato correspondiente a la dirección IP dinámica de las personas que acceden a su sitio web aun cuando sólo el proveedor de acceso dispone realmente de la información relacionada con la persona a la que se asigna esa dirección. En este punto, el Tribunal recuerda que en su sentencia de 24 de noviembre de 2011 (C-70/10; asunto Scarlett Extended) ya señaló que la dirección IP dinámica era un dato personal para el proveedor de acceso, indicando posteriormente que la Directiva no exige que los medios que permitan la identificación del afectado se encuentren a disposición de quien trata el dato, sino que el mismo pueda identificar al interesado a través de medios que puedan ser razonablemente utilizados.

Analizando este requisito, el Tribunal considera que en este caso es posible que el prestador de servicios de medios en línea pueda acceder a los datos identificativos en poder del proveedor de acceso con la finalidad de poder ejercer acciones penales contra el interesado en caso de ataque por denegación de servicio, por lo que habrá de considerarse que para el primero la dirección IP dinámica también constituye un dato de carácter personal.

En segundo lugar, la sentencia analiza si es conforme al derecho de la Unión una norma de derecho interno que limita la posibilidad de tratamiento de los datos de direcciones IP a las finalidades vinculadas con posibilitar y facturar los servicios, pero no lo autoriza para otros fines tales como «garantizar el funcionamiento general de los mismos servicios». El Tribunal, tras recordar la doctrina contenida en su sentencia de 24 de noviembre de 2011 (Asuntos C-468/10 y 469/10; Asnef, Fecemd) considera que una restricción absoluta de esta naturaleza se opone al artículo 7 f) de la Directiva, teniendo en cuenta que los prestadores podrían «tener también un interés legítimo en garantizar, más allá de cada utilización concreta de sus sitios de Internet accesibles al público, la continuidad del funcionamiento de dichos sitios».

Finalmente, resulta especialmente relevante la sentencia de 21 de diciembre de 2016 (asuntos c-203/15 y C-698/15; Tele2) en que se analiza la conformidad con el derecho de la Unión de las leyes adoptadas por Suecia y el Reino Unido para la trasposición de la Directiva 2006/24/CE, anulada por el Tribunal en su sentencia de 8 de abril de 2014 (asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland).

La sentencia indica, en primer lugar, que tanto la obligación de los operadores de comunicaciones electrónicas de conservar los datos de tráfico y localización como la de facilitarlos a las autoridades competentes es una materia sometida al derecho de la UE, habida cuenta de que la primera impone una obligación a los operadores, que en principio se ampararía, desde la anulación de la Directiva 2006/24, en lo dispuesto en el artículo 15.1 de la Directiva 2002/58 y que la única finalidad de esta obligación es su puesta a disposición, de forma que la primera no puede entenderse sin la segunda.

A continuación, analiza los requisitos para que una norma que imponga la conservación de los datos para su puesta a disposición de las autoridades nacionales sea conforme al Derecho de la Unión, señalando que se opondría a los artículos 7, 8 y 11 de la Carta (que consagran los derechos a la intimidad, la protección de datos y la libertad de expresión), así como a su artículo 52.1, referido a las limitaciones de los derechos, una norma que, con la finalidad de luchar contra la delincuencia:

- Estableciera la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica con la finalidad de favorecer el acceso a los mismos por las autoridades competentes

- No limitase el acceso, en el marco de la lucha contra la delincuencia, a los casos de delincuencia grave.
- No supeditase el acceso a los citados datos a un control previo por un órgano jurisdiccional o una autoridad administrativa independiente.
- No exigiese que los datos se conserven en el territorio de la Unión.

De este modo, el Tribunal recuerda la doctrina sentada en la ya citada sentencia de 8 de abril de 2014 para considerar que la obligación de conservación, aun pretendiendo ampararse en lo dispuesto en el artículo 15.1 de la Directiva 2002/58 en su redacción inicial, sólo sería válida en la medida en que, conforme a la jurisprudencia del Tribunal Europeo de Derechos Humanos y del propio Tribunal de Justicia de la Unión pueda considerarse una medida proporcional en una sociedad democrática para alcanzar el fin perseguido (la lucha contra la delincuencia grave), indicando qué requisitos deberían concurrir en una Ley nacional para que quepa hablar de esa proporcionalidad.

Esta cuestión es analizada en los apartados 109 a 111, en que el Tribunal indica que sería necesario que la Ley nacional limitase la medida a «lo estrictamente necesario», de forma que la conservación responda a criterios objetivos, existiendo una relación entre los datos que deban conservarse y el objetivo que se pretenda lograr, delimitando el alcance de la medida y el público afectado por la misma. Entiende el Tribunal que esta delimitación podría hacerse, por ejemplo, especificando el colectivo al que la medida se refiriese mediante el establecimiento, por ejemplo, de un criterio geográfico.

Además el apartado 120 de la sentencia clarifica que para que la medida adoptada sea posible el acceso deberá someterse a un control previo, de forma que se limite a casos de urgencia debidamente justificados. Ese control previo deberá ejercerse por una autoridad judicial o administrativa independiente.

Finalmente, en materia de seguridad, el apartado 122 recuerda que la Directiva 2002/58 impone la adopción de medidas reforzadas de seguridad, que exigen que los datos no se transmitan fuera del territorio de la Unión.

Como consecuencia de todo ello, el Tribunal considera contrarias al Derecho de la Unión y, en particular, a la Carta de los derechos Fundamentales de la Unión una norma nacional que establece la obligación de conservación de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica con la finalidad de luchar contra la delincuencia, así como la que prevé a que el acceso a los datos por las autoridades competentes no esté sometido al control previo de una autoridad judicial o administrativa independiente.

2.2.3. Otras actuaciones de prevención: la protección de datos en relación con la reutilización de la información del sector público y la anonimización

2.2.3.1. *Las orientaciones sobre protección de datos en la reutilización de la información del sector público*

La información generada por el sector público, con la potencialidad que le otorga el desarrollo de la sociedad de la información, posee un gran interés para las empresas a la hora de operar en sus ámbitos de actuación, contribuyendo al crecimiento económico y a la creación de empleo.

El volumen de información pública generada ha aumentado exponencialmente, un hecho que, unido al progreso de las tecnologías empleadas para el análisis, explotación y tratamientos de datos, así como la creciente concienciación de la sociedad sobre el valor de la información pública, favorece su reutilización para la provisión de nuevos productos y servicios.

Las innegables ventajas de este entorno en materia de innovación, crecimiento de la economía y el empleo y de impulso a la sociedad de la información y el conocimiento hacen necesario formular

propuestas que permitan compatibilizarlas con la garantía del derecho fundamental a la protección de datos.

La AEPD asumió la iniciativa de facilitar a nivel nacional orientaciones que contribuyeran de forma equilibrada a favorecer la reutilización de la información pública, minimizando los riesgos que pueda implicar para los ciudadanos. Para ello elaboró y publicó unas «Orientaciones sobre protección de datos en la reutilización de la información del sector público».

La Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público (modificada por la Ley 18/2015, de 9 de julio), supone un salto cualitativo en orden a favorecer la reutilización de la información pública al establecer la obligación inequívoca para las administraciones y organismos del sector público de autorizar la reutilización de los documentos y ampliar su ámbito de aplicación a las bibliotecas, los museos y los archivos.

Sin embargo, la Ley de reutilización establece un punto de conexión con la normativa reguladora de la transparencia y acceso a la información pública al señalar que no será aplicable a los documentos sobre los que existan prohibiciones o limitaciones en el derecho de acceso en virtud de lo previsto en la Ley 19/2013, de 9 de diciembre, entre las que se incluyen las relacionadas con datos personales.

Por otra parte, la Ley 37/2007 contempla referencias específicas a la normativa de protección de datos personales, señalando que la reutilización de documentos que contengan datos de carácter personal se regirá por lo dispuesto en la Ley Orgánica 15/1999 de Protección de Datos de carácter personal (LOPD) (artículo 4.6).

Partiendo de este marco normativo las Orientaciones describen medidas proactivas para evaluar la incidencia de la reutilización en la protección de los datos personales y propone la anonimización de estos últimos como una fórmula segura para facilitar la reutilización.

Sus principales conclusiones son las siguientes:

- La decisión sobre la reutilización de la información del sector público está condicionada por las limitaciones incluidas en la LTAIBG, en lo que afectan al tratamiento de datos personales, tal y como exige el artículo 3.4 de la Ley 37/2007. Estas limitaciones deben ponderarse de manera diferente según que los datos sean objeto de publicidad activa o estén relacionados con el ejercicio individual del derecho de acceso a la información pública.
- Para decidir si se facilitan datos personales con fines de reutilización es necesario examinar los riesgos para los interesados y las medidas que pueden minimizarlos mediante una evaluación de impacto sobre los datos personales.
- La alternativa más apropiada para permitir la reutilización de información pública que contenga datos personales es proceder a su anonimización, de forma que estén excluidos de la aplicación de la normativa de protección de datos personales.
- La evolución tecnológica y la diversidad de fuentes disponibles con datos personales

pueden dificultar una adecuada anonimización de la información. Por ello, la anonimización exige evaluar los riesgos de que el reutilizador pueda reidentificar a las personas. Además, puede ampliar la información sobre cómo proceder a la anonimización consultando las Orientaciones elaboradas por la Agencia.

- Para garantizar que no se reidentifique a las personas, las medidas técnicas y organizativas dirigidas a anonimizar los datos personales pueden complementarse con compromisos jurídicamente vinculantes.
- La opción más apropiada para exigir compromisos jurídicos para evitar la reidentificación es la concesión de licencias específicas, prevista en la Ley 37/2007.

2.2.3.2. *Orientaciones y garantías en los procedimientos de anonimización de datos personales*

En la actualidad con independencia del sector de actividad, todo tipo de entidades públicas y privadas tratan importantes volúmenes de información para la toma de decisiones; información que en una gran mayoría de las ocasiones suele contener datos personales.

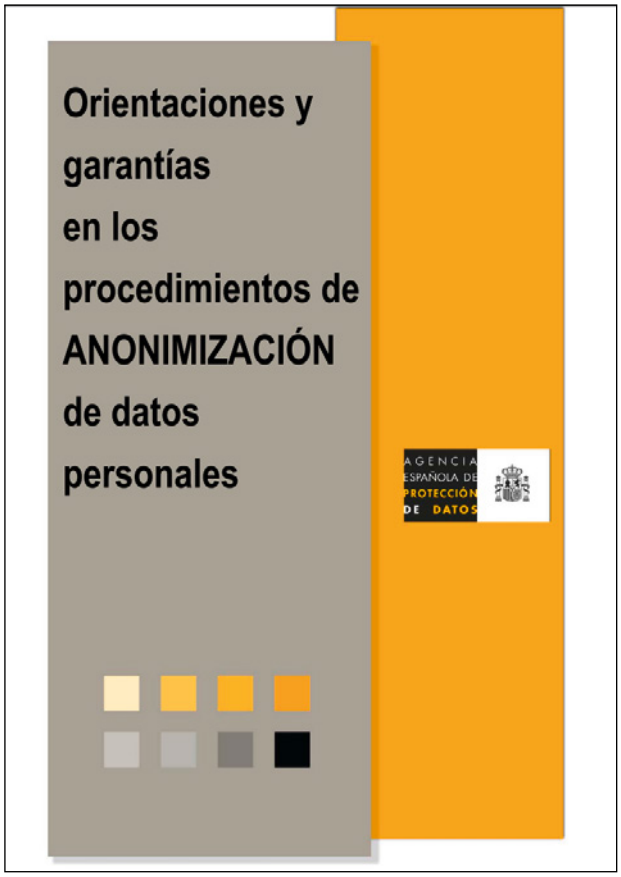
En este entorno adquiere especial relevancia la anonimización de la información personal, puesto que es una opción que va a permitir a las entidades beneficiarse del potencial que tiene el tratamiento de grandes volúmenes de información respetando a su vez la privacidad de las personas.

La anonimización de datos se configura como un procedimiento dirigido a eliminar la posibilidad de identificar a las personas y, por tanto, ofrece mayores garantías de protección de los datos personales que otras técnicas.

Sin embargo, para que la anonimización sea óptima debe tener en cuenta la necesidad de garantizar su irreversibilidad. Así, cualquier técnica empleada debe ser valorada tanto para los procesos de anonimización como para la reidentificación.

En consecuencia, el desarrollo de técnicas de anonimización de datos es un factor muy importante a tener en cuenta por todas aquellas entidades o profesionales que desarrollen estudios e investigaciones de interés social, científico o económico para poder garantizar la protección de los datos personales.

Con el fin de ofrecer criterios clarificadores en esta materia, la Agencia publicó en el año 2016 una guía denominada «Orientaciones y garantías en los procedimientos de anonimización de datos personales» donde se describen procesos y técnicas que pueden resultar útiles en los procesos de anonimización y, por tanto, para la seguridad de los datos personales.



La Guía comienza definiendo el concepto de anonimización como aquel proceso que permite eliminar o reducir al mínimo los riesgos de reidentificación de los datos anonimizados manteniendo la veracidad de los resultados del tratamiento de los mismos, es decir, además de evitar la identi-

ficación de las personas, los datos anonimizados deben garantizar que cualquier operación o tratamiento que pueda ser realizado con posterioridad a la anonimización no conlleva una distorsión de los datos reales.

Entre los principios a tener en cuenta en cualquier proceso de anonimización se recogen el proactivo (desde el inicio conceptual del diseño del sistema de información o productos a utilizar en el proceso de anonimización se tomarán las medidas necesarias para garantizar la privacidad de las personas); la privacidad por defecto (desde el inicio es conveniente que se salvaguarde la privacidad teniendo en cuenta la granularidad o grado de detalle final que deben tener los datos anonimizados); la privacidad objetiva (aceptación del umbral de riesgo o índice de riesgo residual de reidentificación que será asumido por el responsable del tratamiento como riesgo aceptable); el principio de plena funcionalidad (desde el diseño del sistema de información habrá que tenerse en cuenta la utilidad final de los datos anonimizados); el de privacidad en el ciclo de vida de la información (se deberán tener en cuenta las medidas que garantizan la privacidad de las personas durante el ciclo completo de la vida de la información partiendo de la información sin anonimizar); así como el de información y formación (clave para garantizar la privacidad de las personas es la formación e información que se facilita al personal involucrado en cualquier proceso de anonimización).

En la Guía también se indican cuáles deberían ser las fases a tener en cuenta antes de iniciar cualquier proceso de este tipo, las cuales han de estar definidas previamente en un protocolo de actuación. Estas fases son: definir el equipo de trabajo teniendo en cuenta la independencia de funciones, evaluar los riesgos de reidentificación, definición de objetivos y finalidad de la información anonimizada, viabilidad del proceso, preanonimización (definir variables de identificación), eliminación/reducción de variables, selección de las técnicas de anonimización, segregación de la información, realización de un proyecto piloto y finalmente la anonimización.

El documento hace una mención especial a la formación en protección de datos personales que debe tener todo el personal que se encuentre implicado en el proceso de anonimización, así como a las garantías jurídicas que han de considerarse para preservar los derechos de los ciudadanos ante una posible reidentificación de sus datos personales.

La Guía también recomienda realizar una auditoría de todo el proceso, que debe estar documentada y accesible al personal implicado en el tratamiento de los datos anonimizados. Su finalidad es garantizar el cumplimiento de la política establecida, proporcionando una opinión objetiva sobre el conjunto del proceso. La calidad de la auditoría es fundamental para el mantenimiento de la confianza de los interesados en el proceso de anonimización, ya que la falta de confianza de éstos en la confidencialidad de los procesos de anonimización podría provocar inquietud social y repercutir negativamente en la explotación de los datos anonimizados.

Finalmente, debe considerarse que los procesos de anonimización son una herramienta válida para garantizar la privacidad de los datos personales y sus limitaciones son inherentes al avance de la tecnología, por lo que la misma capacidad de la tecnología para anonimizar datos personales puede utilizarse para la reidentificación de las personas.

Esto lleva a concluir que los procesos de anonimización pueden no garantizar al cien por cien la no reidentificación de las personas, por lo que la fortaleza de la anonimización deberá sustentarse en otro tipo de medidas como la realización de evaluaciones de impacto, organizativas, de seguridad de la información, tecnológicas y cualquier otra que sirva para atenuar los riesgos de reidentificación de las personas y para paliar las consecuencias si se materializasen.

2.3. ACCIONES EN RELACIÓN CON LAS INSTITUCIONES PÚBLICAS

2.3.1. Colaboración con la Administración General del Estado

La Agencia Española de Protección de Datos promovió en junio de 2016 una reunión con representantes de la Dirección de Tecnologías de la Información y de las Comunicaciones de la Administración General del Estado y del Centro Criptológico Nacional al objeto de crear un grupo de trabajo sobre la implantación del RGPD en las Administraciones Públicas.

En la convocatoria a la citada reunión se pretendía constituir formalmente un grupo de trabajo dirigido por la Unidad de Evaluación y Estudios Tecnológicos, para ayudar a las Administraciones Públicas a adaptarse a las nuevas obligaciones que se establecen en el RGPD antes del 25 de mayo de 2018, prestando especial atención a las Administraciones Públicas de menor tamaño o con pocos recursos.

En materia de seguridad de los datos personales se ha considerado la opción de valorar las vías de convergencia entre el Esquema Nacional de Seguridad y los criterios de seguridad que se recogen en el RGPD, así como revisar los criterios establecidos en el RGPD al objeto de valorar si estos encajaban con el Esquema Nacional de Seguridad debiendo analizar para ello su metodología de desarrollo MAGERIT y la aplicación que lo implementa, PILAR.

En este sentido se consideró que MAGERIT/PILAR es una herramienta válida para poder aplicar el RGPD ya que se utiliza en todas las Administraciones Públicas, tiene un perfil de protección que incluye la protección de datos personales, permite realizar análisis de riesgos rápidos que pueden ayudar a las Administraciones Públicas a conocer su nivel de cumplimiento, y admite la posibilidad de incluir una dimensión de privacidad que contemple las necesidades del RGPD así como armonizar auditorías, análisis de riesgos y otros requisitos con el Esquema Nacional de Seguridad.

Partiendo de estas premisas se apreció la necesidad de realizar dos análisis de riesgos en paralelo, uno de tratamientos de datos que recogería los riesgos para los derechos y libertades de las personas y otro análisis de riesgos de seguridad, análisis que pueden realizarse con PILAR.

Posteriormente se mantuvo una nueva reunión monográfica sobre PILAR donde se presentó la herramienta y se planteó la posibilidad de desarrollar una versión de la misma con los requerimientos del análisis de riesgos del RGPD. También se planteó la posibilidad de revisar las guías de la serie 800 publicadas por CCN-STIC para adaptarlas a los contenidos del RGPD. Dicha versión ha sido ya elaborada por el CCN y está siendo evaluada por la Agencia Española de Protección de Datos al objeto de valorar si cumple con los requisitos del RGPD. A lo largo de 2017, el grupo de trabajo pretende poner a disposición de todas las Administraciones Públicas una herramienta de análisis de riesgos que contemple el cumplimiento del RGPD alineada con la ya conocida PILAR. Los trabajos de este grupo de trabajo seguirán avanzando con la elaboración de materiales que se pondrán a disposición de todas las Administraciones Públicas para facilitar el proceso de adaptación al RGPD.

2.3.2. Colaboración con las CCAA

En el ámbito de la protección de los menores, la colaboración con las CCAA se ha realizado fundamentalmente a través de las correspondientes administraciones educativas, en el marco de la Comisión General de Educación y a través de solicitudes concretas de colaboración para la difusión de los materiales elaborados por la Agencia y los Premios a las Buenas prácticas educativas en privacidad y protección de datos para un uso seguro de internet, así como en la participación en jornadas organizadas por las inspecciones educativas.

Asimismo, la Agencia ha promovido iniciativas de colaboración con las Comunidades Autónomas en materia de consumo. En este sentido la AEPD participó en la reunión de la Comisión de Coo-

peración de Consumo convocada por la Agencia Española de Consumo, Seguridad Alimentaria y Nutrición (AECOSAN), Organismo Autónomo adscrito al Ministerio de Sanidad, Servicios Sociales e Igualdad, con objeto de presentar junto a INCIBE la «Guía sobre Privacidad y Seguridad en internet» que se describe en otros apartados de esta Memoria.

2.3.3. Colaboración con las Universidades

La Agencia Española de Protección de Datos, a través de la Unidad de Evaluación y Estudios Tecnológicos (UEET), Unidad que se analiza en un apartado específico de esta Memoria, pretende acercar la protección de datos personales a las Universidades.

La Agencia pretende crear una base de datos donde se pueda conocer los distintos máster que se imparten en las universidades, públicas y privadas, relacionados con nuevas tecnologías al objeto de fomentar el conocimiento de la protección de datos, facilitar prácticas a los alumnos y potenciar la labor investigadora en temas relacionados con la privacidad y la seguridad de los datos. La Agencia considera importante que los futuros profesionales de la tecnología tengan conocimiento del Reglamento General de Protección de Datos, de tal forma que cuando se incorporen a una empresa puedan aportarlo, sobre todo cuando se trata de incorporar la privacidad desde el diseño de productos, servicios o sistemas de información, permitiendo así a la empresa tener un plus de calidad y ser más competitiva en el mercado.

2.3.4. Colaboración con el Consejo de Transparencia y Buen Gobierno

El artículo 36.1 f) de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la información pública y Buen gobierno (LTAIBG), 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 2016 se han celebrado ocho reuniones de la Comisión del Consejo y se ha adoptado un criterio de interpretación conjunto por la Agencia y el Consejo (CI/002/2016, de 6 de julio) referido a las reglas de ponderación que deberán aplicarse para el acceso a la información relacionada con las agendas de los responsables públicos.

2.3.5. Colaboración con el Consejo General del Poder Judicial

La Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial contempla, tras su modificación en el año 2015, diversos tratamientos de datos de carácter personal en el ámbito de la Administración de Justicia.

En particular, la Ley Orgánica clasifica los tratamientos de datos por los órganos judiciales y los correspondientes ficheros en dos categorías según se realicen con fines jurisdiccionales o no jurisdiccionales.

En relación con los primeros la competencia para la aplicación de la LOPD se atribuye al Consejo General del Poder Judicial y respecto de los segundos a la AEPD, que deberán prestarse la colaboración que resulte necesaria.

Esta colaboración tiene una especial transcendencia en los casos en que en las actuaciones de investigación realizadas por una de las autoridades se aprecien indicios que supongan la competencia de la otra, en orden a proceder a su traslado inmediato a la misma.

A tal efecto, en 2016 se celebró una reunión en el Consejo General del Poder Judicial con el fin de articular un procedimiento fluido para aclarar las dudas sobre la competencia de cada una de las autoridades agilizando la tramitación de los procedimientos.

Asimismo, se analizaron las posibilidades de colaboración entre las unidades de inspección de ambas autoridades.

2.3.6. Colaboración con el Defensor del Pueblo

Durante el presente año ha de destacarse el importante descenso producido en el número de asuntos que se han remitido desde la Oficina del Defensor del Pueblo con respecto a 2015. En particular, se han tramitado un total de 22 asuntos, frente a los 38 del año anterior, es decir, una disminución del 40%. Esto confirma la tendencia descendente que se viene produciendo durante los últimos años, donde se promovieron 59 asuntos en 2013, y 53 en 2014.

En cuanto a las principales materias o temas objeto de la atención del Defensor del Pueblo hay que destacar las quejas relativas a videovigilancia (7), derecho de acceso (4), morosidad (3), derecho al olvido (2), y otros como inscripción de ficheros, llamadas comerciales no solicitadas, etc. (6).

Los principales motivos de los requerimientos del Defensor del Pueblo han sido para solicitar información sobre el estado de tramitación de un procedimiento (5); plantear aclaraciones sobre el criterio seguido por la Agencia en alguna de sus resoluciones (5); solicitar información para proceder a un estudio o investigación más profunda sobre un tema o para conocer el criterio seguido por ésta en un determinado asunto de su interés (5); formular recomendaciones o solicitar actuaciones adicionales de la Agencia para el pleno cumplimiento de alguna de sus recomendaciones (2), o reclamar la actuación complementaria de la Agencia para hacer cumplir una resolución estimatoria de tutela (2).

En este sentido, hay que destacar la recomendación formulada por el Defensor del Pueblo sobre la revisión del criterio de la AEPD en las denuncias sobre avisos de zona videovigilada; la solicitud de actuaciones adicionales de la AEPD para el cumplimiento íntegro de su recomendación sobre el llamado «derecho al olvido»; la solicitud de información en relación con las investigaciones de oficio iniciadas a los ficheros de solvencia patrimonial y sobre la práctica de los llamados «falsos cupones» (mensajes enviados por Whatsapp incitando a cumplimentar una encuesta para recibir un cupón de descuento y así obtener ilícitamente datos personales activando un servicio SMS Premium), las solicitudes de informe acerca del eventual acceso a las imágenes por parte de los Directores de Centros de Internamiento o las comunicaciones de datos personales realizadas entre WhatsApp y Facebook.

2.3.7. Colaboración con las Autoridades autonómicas de protección de datos

Durante el año 2016 la colaboración entre la Agencia Española de Protección de Datos, la Autoridad Catalana de Protección de Datos y la Agencia Vasca de Protección de Datos se ha centrado fundamentalmente en las cuestiones relativas a la aplicación del nuevo Reglamento General de Protección de Datos de la Unión Europea.

El Reglamento entró en vigor en mayo de 2016 y será de aplicación dos años después, en mayo de 2018. Se trata de una norma de efecto directo que, en principio, debe ser aplicada también directamente por todos los afectados.

Desde el punto de vista de las autoridades de supervisión, ello conlleva, por una parte, un trabajo de interpretación y clarificación de sus previsiones, siempre a reservas de lo que puedan disponer las normas nacionales que se adopten para facilitar la aplicación del Reglamento o de las decisiones que en su momento puedan tomar tanto los tribunales españoles como el Tribunal de Justicia de la Unión Europea.

Por otro lado, implica también una labor de sensibilización, información y apoyo a las organizaciones que tendrán que adaptar su actividad a las

nuevas obligaciones del Reglamento y a los ciudadanos, titulares de los nuevos derechos que el Reglamento contempla.

Teniendo presente esos dos tipos de actuaciones se estableció un Grupo de Trabajo integrado por la Agencia Española y las Autoridades autonómicas con el doble objetivo de alcanzar criterios comunes en el terreno de la interpretación y aplicación de determinadas disposiciones del Reglamento y de distribuir la tarea de preparar instrumentos de apoyo basados también en un enfoque consensuado.

El Grupo de Trabajo mantuvo cinco reuniones durante el año 2016, a las que habría que añadir un mismo número de reuniones celebradas por un grupo de trabajo de seguridad creado en el seno del Grupo.

Fruto de esta cooperación, el Grupo alcanzó posiciones comunes sobre los siguientes temas:

- Consentimiento. El Reglamento Europeo exige que el consentimiento deba prestarse a través de declaraciones o de claras acciones afirmativas. La conclusión es que las formas de consentimiento basadas en la inacción del interesado dejan de ser válidas. El Grupo de Trabajo concluyó, asimismo, que de acuerdo con las previsiones del Reglamento, todos los tratamientos deben basarse en un consentimiento acorde con el Reglamento a la fecha de su aplicación, incluidos los iniciados con anterioridad a esa fecha.

- Contratos entre responsables y encargados. Al igual que en el caso del consentimiento, el Reglamento incluye expresamente nuevos contenidos en los contratos de encargo de tratamiento. Esos nuevos contenidos deberían estar incorporados a todos los contratos que regulen las relaciones responsables-encargados en mayo de 2018.

- Evaluaciones de Impacto sobre la Protección de Datos. La obligación de llevar a cabo una Evaluación de Impacto respecto a tratamientos que supongan un alto riesgo para los derechos y libertades de los interesados aparece también como novedad en el Reglamento. El Grupo entiende que en la medida en que un determinado tratamiento que pueda plantear alto riesgo incorpore, a partir de mayo de 2018, nuevos datos, debe entenderse que, pese a que el tratamiento siga siendo el mismo, se estaría aplicando a nuevos interesados cuyos derechos y libertades podrían estar en riesgo a partir de la fecha en que sus datos comienzan a ser tratados. Por ello, en esos casos sí sería necesario que se llevara a cabo una Evaluación de Impacto en los supuestos a los que se refiere el RGPD.

- Información a los interesados. El Grupo entiende que no existiría una obligación de ofrecer esa nueva información en todos los casos a todos los interesados en tratamientos ya iniciados con anterioridad a mayo de 2018. Sin embargo, también considera que el periodo transitorio debiera ser aprovechado por las organizaciones para realizar una adaptación progresiva de sus cláusulas informativas. Asimismo, recomienda que las nuevas políticas informativas que se implanten durante el periodo transitorio incluyan ya la información requerida por el Reglamento en la medida en que ello sea posible.

- Certificación de profesionales de protección de datos. El Reglamento Europeo no prevé explícitamente que los profesionales de la privacidad que opten a ser designados como delegados de protección de datos deban certificarse profesionalmente. Se limita a señalar que en la selección de los delegados se deberán tomar en consideración sus cualidades profesionales, especialmente sus conocimientos especializados en derecho y práctica de la protección de datos. La Agencia Española entendió, y así lo trasladó al Grupo de Trabajo, que la certificación de profesionales podría ser un mecanismo adecuado para ordenar el sector y para ofrecer a responsables, encargados y los propios profesionales un instrumento que permita demostrar las cualidades requeridas de una forma generalmente reconocida.

Esta certificación, que la Agencia Española está ya preparando en colaboración con la Entidad Nacio-

nal de Acreditación, no será la única vía de acceso a los puestos de delegado de protección de datos y no ha de impedir que las cualificaciones profesionales puedan acreditarse por otros métodos.

Junto con estos posicionamientos comunes en algunos aspectos clave relacionados con la aplicación del Reglamento, el Grupo de Trabajo ha preparado conjuntamente diversos materiales dirigidos a apoyar a responsables y encargados, especialmente pymes, que se harán públicos en 2017.

Al margen de la actividad de este Grupo de Trabajo, las Autoridades autonómicas han estado asociadas también al proceso de elaboración de la norma que reemplazará a la vigente Ley Orgánica de Protección de Datos. La fase inicial de este proceso, como se ha mencionado con anterioridad en esta Memoria, ha sido atribuida a la Comisión General de Codificación, en cuya Sección Tercera, de Derecho Público, se ha constituido una Ponencia, en la que participan vocales de la Sección junto con vocales procedentes de la Agencia Española de Protección de Datos nombrados al efecto, cuyo cometido es el de preparar el borrador de anteproyecto de la futura ley de protección de datos.

2.3.8. Fomento de la seguridad jurídica mediante la emisión de informes preceptivos de proyectos normativos

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 2016 fueron informadas 73 disposiciones de carácter general, lo que supone una disminución del 50% respecto las que fueron informadas en el ejercicio anterior, si bien ello se debió a la especial situación de la Administración General del estado durante el ejercicio y a la inexistencia de iniciativas legislativas, salvo en supuestos excepcionales, al encontrarse el Gobierno en funciones. Por este motivo, además, las disposiciones informadas se centraron en su mayoría en órdenes de creación de ficheros de distintos departamentos ministeriales y organismos vinculados o dependientes de los mismos, si bien cabe mencionar algunas disposiciones:

- Borrador de Anteproyecto de ley transparencia de la actividad pública de Cantabria
- Proyecto de Real decreto por el que se regulan determinados aspectos relativos a la fabricación, presentación y comercialización de los productos del tabaco y los productos relacionados
- Proyecto de Real decreto de modificación estatutos del Colegio de Ingenieros de Montes
- Proyecto de Orden por la que se aprueba la lista de información a remitir en supuestos de adquisición o incremento de participaciones significativas en entidades aseguradoras y reaseguradoras
- Proyecto de Orden por la que se modifica anexo II del RD 1088/2005, de 16 de septiembre, 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 de la Junta de Andalucía de creación de la sede judicial electrónica de Andalucía
- Proyecto de Orden de la Xunta de Galicia por la que se crea y regula la sede judicial electrónica de Galicia
- Proyecto de Orden del Gobierno de Cantabria por la que se crea la sede judicial electrónica en el ámbito territorial de la Comunidad Autónoma de Cantabria.
- Proyecto de Orden Foral de creación de la Sede Judicial electrónica del Gobierno de Navarra.
- Proyecto de Orden del Gobierno de Canarias por la que crea la Sede Electrónica de Canarias.

3 INNOVACIÓN Y PROTECCIÓN DE DATOS: FACTOR DE CONFIANZA Y GARANTÍA DE CALIDAD

3.1. CREACIÓN DE LA UNIDAD DE EVALUACIÓN Y ESTUDIOS TECNOLÓGICOS (UEET)

La Agencia Española de Protección de Datos debe estar preparada para detectar el impacto de la tecnología en la privacidad de los ciudadanos, buscando mitigar sus riesgos sin que ello suponga renunciar a las funcionalidades y beneficios de la tecnología, fomentando la investigación y la innovación.

Así, en el año 2016 la Agencia creó la Unidad de Evaluación y Estudios Tecnológicos (UEET) con la finalidad de evaluar las implicaciones que las nuevas tecnológicas tienen para la privacidad, realizando estudios prospectivos y análisis de distintos productos y servicios además de verificar la transparencia con la que se llevan a cabo los tratamientos de datos personales.

Por otro lado, la labor proactiva frente a los responsables de tratamientos pretende promover la protección de datos desde el diseño y por defecto, la realización de evaluaciones de impacto en la protección de datos personales, la revisión de las evaluaciones de impacto que evidencien un alto riesgo, así como conocer nuevos desarrollos tecnológicos de especial interés.

También con esta unidad se pretende realizar estudios e informes sobre el impacto en la privacidad de las nuevas tecnologías, coordinar acciones destinadas a implantar las nuevas medidas técnicas y organizativas del RGPD en pymes y Administraciones Públicas, colaborar con la universidad, la industria, los profesionales de la protección de datos, promover la seguridad en el tratamiento de los datos personales y estudiar los modelos de acreditación y certificación existentes en el mercado de cara a cumplir con lo dispuestos en el RGPD.

3.2. ELABORACIÓN DE ESTUDIOS SOBRE DIVERSOS ÁMBITOS DE LA SOCIEDAD CONECTADA

- **Estudio sobre reutilización de información clínica y análisis masivo de datos (Big Data) en el sector sanitario**

En el año 2016 la Agencia encargó a una empresa la realización de un trabajo de campo que posibilitara analizar la situación española respecto de la reutilización de información clínica y el uso de herramientas de análisis masivo de datos (Big Data). El estudio debía abordar todo el sector de la salud en los ámbitos asistencial, de investigación, epidemiológico y de salud pública por parte del sector público y del privado.

En este estudio se pretende identificar el uso de nuevas tecnologías y tratamientos de información en el sector, determinar los principales intervinientes en el tratamiento de la información en el ámbito sanitario, detallar el tratamiento de la información en el ciclo de vida de los datos dentro del sector, conocer el flujo de información que se produce entre diferentes entidades y países, identificar proyectos actuales en el sector asociados al tratamiento masivo de datos así como conocer las barreras técnicas o regulatorias que encuentran las entidades a la hora de abordar este tipo de proyectos.

La realización del estudio ha requerido la colaboración de un gran número de actores relacionados con el sector de la salud y la reutilización de datos sanitarios. Se ha contactado con el Ministerio de Sanidad, Servicios Sociales e Igualdad, las Consejerías de Salud de las Comunidades Autónomas, Hospitales, sociedades científicas y universidades y en el ámbito privado con grupos hospitalarios, entidades farmacéuticas, laboratorios, entidades aseguradoras y empresa tecnológicas. A raíz de estos contactos y de un proceso de investigación documental se han seleccionado aquellos casos más relevantes de reutilización de información sanitaria y uso de herramientas analíticas, como es el caso de Big Data. Para elegir los casos que han sido finalmente objeto de estudio se ha tenido en cuenta la relevancia de los mismos en el sector, la innovación y el enriquecimiento con información no sanitaria como complemento de la sanitaria así como el uso de tecnologías de análisis de información no estructurada.

La UEET evaluará y sistematizará toda la información obtenida y redactará «Documento de Trabajo sobre Reutilización de la Información Sanitaria y Big Data» para su divulgación.

- **Código de buenas prácticas en protección de datos para proyectos de Big Data, en colaboración con ISMS Forum**

La UEET de la Agencia ha participado en varios grupos de trabajo para analizar la situación actual en relación con el uso de la tecnología Big Data y elaborar un documento de buenas prácticas a tener en cuenta cuando se desarrollan proyectos utilizando esta tecnología.

A finales de 2016 ya se disponía de un borrador de este documento, que ha sido presentado en mayo de 2017.

3.3. Otras actuaciones

- **Validación de la Plataforma de intermediación**

Durante el año 2016, la Unidad de Evaluación y Estudios Tecnológicos realizó una evaluación de la plataforma de intermediación disponible en el Portal de Administración Electrónica de la AGE al objeto de verificar su adaptación a la normativa de protección de datos y con el fin de potenciar su utilización por toda la Administración Pública.

El derecho del ciudadano a no presentar aquellos documentos que ya se encuentren en poder de la Administración se reconoce desde el año 1992 en la hoy derogada Ley 30/1992. En el año 2003 se creó un grupo de trabajo para definir y especificar el mecanismo de intercambio de información entre Administraciones Públicas estableciéndose un protocolo (SCSP) consistente en un conjunto de especificaciones orientadas al intercambio de documentación y datos entre Administraciones Públicas. El objetivo del protocolo fue el de eliminar los certificados administrativos en papel, sustituyéndolos por un intercambio de datos entre administraciones que se realiza de forma electrónica, estandarizada y rápida evitando así al ciudadano presentar ante las Administraciones Públicas documentación que ya obra en poder de las mismas.

Actualmente Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas prevé que las Administraciones Públicas deben recabar los documentos electrónicamente a través de sus redes corporativas o mediante consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto.

La plataforma de intermediación ofrece un servicio de verificación que permite a cualquier organismo de la administración que lo utilice, verificar los datos de un ciudadano que ha iniciado un trámite con la entidad, de modo que no tenga que aportar documentos acreditativos, por ejemplo, de identidad ni de residencia, y hace posible que la validación de dichos documentos se realice por medios electrónicos.

Se trata de un servicio en red integrable en aplicaciones del cliente y se pretende dar cumplimiento a los derechos reconocidos en la Ley 39/2015, de 1 de octubre, facilitando el inicio de los trámites y evitando que tenga que adjuntar a la solicitud documentos que acrediten su identidad y su empadronamiento. También pretende simplificar la tramitación de los procedimientos administrativos y reducir el volumen de papel gestionado en la Administración.

Los tipos de servicios intermediados son el servicio de cambio de domicilio que puede ser integrado por las diferentes administraciones públicas en sus sistemas para que el ciudadano les notifique automáticamente su cambio de domicilio y los servicios de verificación y consulta de datos (Plataforma de intermediación) que mediante Webservices podrán integrar en sus diferentes aplicaciones de administración electrónica el uso de múltiples servicios de verificación y consulta de datos disponibles.

El Ministerio de Hacienda y Función Pública es el responsable de la plataforma de intermediación de datos y a través de ella, una Administración puede consultar de forma automatizada, desde una aplicación de gestión de un trámite adaptada para invocar los Webservice proporcionados por el servicio, cualquiera de los más de 30 certificados ofrecidos tales como datos de identidad y de residencia de un ciudadano, datos relativos al desempleo, titulaciones oficiales, datos catastrales, estar al corriente con la Agencia Española de Administración Tributaria y Tesorería General de la Seguridad Social, datos de pensiones, nacimiento, defunción y matrimonio de los Registros Civiles. Conviene matizar que la lista de certificados está en constante expansión.

La Agencia realizó un estudio de toda la información disponible en la página web del Ministerio entonces responsable de la plataforma de intermediación, entre la que se incluye el funcionamiento e intervinientes en la gestión de la misma, así como de la información aportada por los responsables de la citada plataforma. Asimismo, se realizó una visita al objeto de completar la información. Como conclusión se elaboró un informe del que se desprende que en el momento actual y según la información aportada por los responsables de la plataforma, los procedimientos y operaciones de la misma se desarrollan respetando la legislación española de protección de datos.

Otras actividades de la UEET han sido las siguientes:

- Participación en el Grupo de Trabajo creado para implantar el Reglamento (UE) 2016/679 en las Administraciones Públicas junto con representantes de la Dirección General de Tecnologías de la Información y Comunicaciones y el Centro Criptológico Nacional.
- Colaboración con la Entidad de Acreditación Nacional de Certificación para elaborar los Esquemas de Acreditación de Entidades Certificadoras de Delegados de Protección de Datos así como del Esquema de Certificación de Delegados de Protección de Datos que se detalla en otro apartado de la Memoria. Estos esquemas serán públicos a lo largo del próximo año.
- Estudio del RGPD al objeto de valorar la posibilidad de realizar los requisitos para abordar un análisis de riesgos para las Administraciones Públicas así como para las pymes.
- Se han iniciado los trabajos para desarrollar un programa informático que permita a las nanopymes y autónomos estar en disposición de acreditar que cumplen con el RGPD.
- También se han iniciado trabajos con la finalidad de poder desarrollar un programa informático que permita a las PYMES elaborar un análisis de riesgos que cumpla con los requisitos de RGPD.
- Asimismo, se ha iniciado el estudio sobre la posibilidad de desarrollar una herramienta que permita a las pymes realizar una evaluación de impacto.

Esta Unidad ha celebrado reuniones con empresas que acuden a la Agencia a presentar proyectos que pueden tener un impacto en la privacidad de las personas cuyos datos tratan. En estos casos la Unidad analiza y valora el proyecto presentado aportando sus conocimientos y experiencia para su adecuación con la normativa de protección de datos.

4 UNA AGENCIA COLABORADORA, TRANSPARENTE, MÁS ÁGIL Y EFICIENTE

4.1. CIUDADANOS MÁS Y MEJOR INFORMADOS

4.1.1. Fomento de una cultura de protección de datos

- **Consultas atendidas por el Área de Atención al ciudadano**

La AEPD ofrece a los ciudadanos, a través del Área de Atención al ciudadano, varios canales a través de los cuales puedan plantear sus dudas respecto a la normativa de protección de datos: atención telefónica, presencial y por escrito, así como la posibilidad de realizar consultas a través de la Sede electrónica y de acceder las consultas más frecuentes (FAQs) que se encuentran publicadas en la citada sede.

El número total de consultas planteadas y respondidas por este Área durante el año 2016 ascendieron a 236.955, con un incremento del 8,52% respecto al año 2015. Su desglose es el siguiente:

- Atención presencial: 4.183.
- Atención telefónica: 76.869.
- Consultas por escrito: 552.
- Consultas por la Sede electrónica: 8.054.
- Acceso a las preguntas frecuentas: 147.297.

En este sentido, hay que destacar que el mayor crecimiento respecto al año 2015 se ha experimentado en las consultas realizadas a través de la Sede electrónica (14,17%), atención presencial (11,04%) y el acceso a las consultas frecuentes (10,99%).

Los temas más consultados son los siguientes: inscripción de ficheros, tratamiento de datos personales en los ficheros de solvencia patrimonial, protección de datos en las comunidades de vecinos, videovigilancia y solicitudes de información sobre la forma de interponer denuncias y reclamaciones ante la AEPD.

Respecto a las consultas sobre el ejercicio de derechos por parte de los ciudadanos, destaca que más del 50% (53,34%) fueron sobre el derecho de cancelación, y un 26,56% específicamente sobre el denominado «derecho al olvido». Por lo que respecta al resto de derechos, un 9,5% se plantearon sobre el derecho de oposición, el 7,92% sobre el derecho de acceso, y únicamente un 2,68% sobre el derecho de rectificación.

- **Nuevo catálogo de consultas frecuentes (FAQs)**

A mediados de julio del año 2016 se renovó totalmente el conjunto de preguntas y respuestas automáticas conocido como Consultas más frecuentes (FAQs), que se encuentran publicadas en la Sede electrónica de la AEPD y que permiten consultar más de 200 preguntas-respuestas.

Para facilitar su lectura se encuentran agrupadas por diversas temáticas, entre las que destacan no sólo los temas más consultados por los ciudadanos, sino también otros como «Transparencia y protección de datos», «Cookies», «Tratamiento de datos en el ámbito laboral» y «Cloud-computing».

También se incluyó un apartado denominado «En qué te podemos ayudar y en qué no», con la finalidad de que los ciudadanos sepan cuándo pueden acudir a la AEPD.

Asimismo, en muchas de ellas, además de la pregunta con su respectiva respuesta, se facilita la consulta a otros materiales disponibles en la web de la AEPD, como pueden ser informes jurídicos o Guías.

- **Nueva Guía de Atención al Ciudadano**

Durante el año 2016 se ha elaborado esta Guía dirigida a los ciudadanos, con la finalidad de fomentar su derecho a la protección de datos, que será objeto de publicación en el primer semestre del 2017.

Esta Guía se estructura en las siguientes partes:

- Obligaciones en el tratamiento de tus datos.
- Tus derechos en el tratamiento de tus datos.
- Tratamiento de tus datos personales en ámbitos específicos (solvencia patrimonial, comunidades de propietarios, videovigilancia y publicidad).
- Recursos de la AEPD a disposición del ciudadano.
- Términos y definiciones utilizados en la Guía.

Además, en la elaboración de esta Guía se ha tenido en cuenta el Reglamento General de Protección de Datos, que será de obligado cumplimiento a partir del 25 de mayo de 2018.

- **Nueva Guía sobre Privacidad y seguridad en internet**

Uno de los ejes principales de actuación de la AEPD es apostar de forma decidida por la prevención a través de instrumentos como la formación, la información, la sensibilización y la concienciación de los ciudadanos. Actualmente es imposible mantenerse al margen de las nuevas tecnologías, pues cada vez son más los objetos de uso cotidiano que disponen de conexión a internet y cada vez encontramos en el mercado mayor número de dispositivos móviles que nos mantienen conectados permanentemente.

En este sentido, la Agencia Española de Protección de Datos, en colaboración con el Instituto Nacional de Ciberseguridad (INCIBE), presentó en 2016 la «Guía sobre Privacidad y Seguridad en internet» donde proporciona a los usuarios de internet información práctica sobre cómo reconocer la falsa identidad de un sitio web, cómo proteger los dispositivos portátiles, cómo generar y gestionar contraseñas, en qué consiste la verificación en dos pasos, cómo realizar copias de seguridad o proteger el correo electrónico, cómo gestionar la información que se almacena en la nube o los riesgos en los servicios de mensajería instantánea, sin olvidar otros temas importantes como el *phishing*, la protección de redes WIFI, el control parental o los «wearables». Y, tratándose de una guía de privacidad y seguridad en internet, no podíamos dejar de mencionar la forma en que pueden ejercerse los derechos en internet y, en particular, el denominado «derecho al olvido».

El objetivo de la guía es ofrecer contenidos claros y concisos para que el internauta no tenga que invertir demasiado tiempo, facilitando respuestas rápidas a problemas concretos.

El formato elegido ha sido modular e incluye un total de 18 fichas en las que se condensa información esencial partiendo de situaciones reales en las que se pueden encontrar los internautas.

Acompañan a las fichas seis vídeos que muestran cómo configurar las opciones de privacidad en seis de los servicios más populares de internet (Instagram, Facebook, Twitter, Whatsapp, Snapchat y YouTube) y presentan a los ciudadanos cómo pueden elegir las opciones que les ofrecen una mayor protección en términos de acceso a los datos por terceros.

Dada su buena acogida, se va a promover su difusión durante 2017 a través de distintos canales: plataformas de contenidos de los operadores de telecomunicaciones, organizaciones y entidades de usuarios y consumidores, encuentros sectoriales, etc.

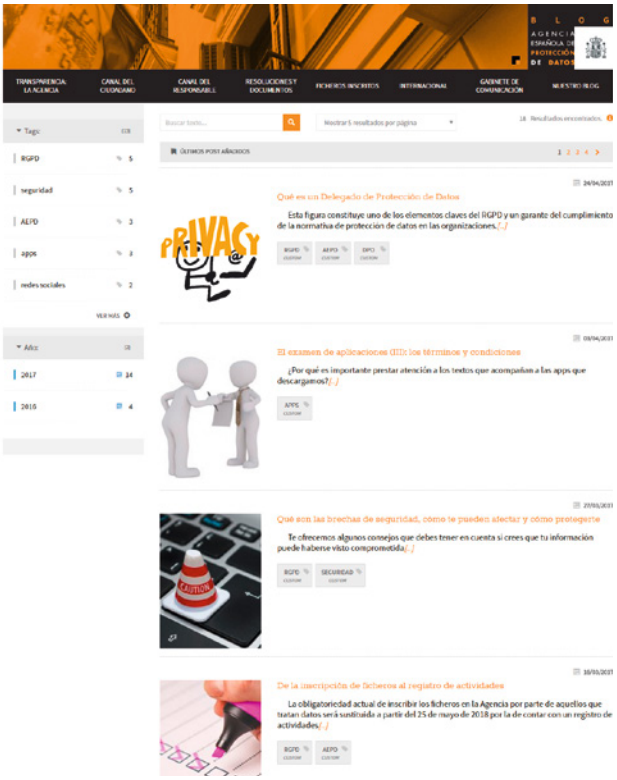
El número de descargas de los citados vídeos unido al resto de los que están disponibles para orientar sobre cómo proteger los datos en internet ascendieron a un total de 43.587.

4.1.2. Herramientas de comunicación

La Agencia Española de Protección de Datos ha puesto en marcha diversas acciones para difundir las iniciativas realizadas. Muchas de ellas se han detallado con anterioridad en otras partes de esta Memoria por lo que, a continuación, se especifican las relacionadas con prensa y comunicación, además de algunas de las acciones de divulgación realizadas a través de página web de la AEPD.

- **El blog de la Agencia**

La Agencia Española de Protección de Datos (AEPD) puso en marcha en diciembre de 2016 El blog de la Agencia, una sección web para potenciar la difusión del derecho fundamental a la protección de datos de forma práctica. Esta iniciativa es una de las actuaciones previstas en el Plan Estratégico de la AEPD, en el eje «Una Agencia colaboradora, transparente y participativa».



Con el lanzamiento de este proyecto, que recibió casi 4.500 accesos en sus primeros tres meses de andadura, la Agencia ha querido impulsar el conocimiento de las diferentes iniciativas que se han puesto o se van a poner en marcha, destacando los informes, guías, resoluciones o documentos elaborados en grupos de trabajo internacionales, entre otras materias, aportando una visión cercana tanto del trabajo que se realiza en la Agencia como de la protección de datos en un plano global.

Los contenidos que se publican en el blog están centrados en dos de las áreas de mayor importancia para la Agencia: que los ciudadanos conozcan el contenido de sus derechos y cómo ejercerlos, y facilitar a los responsables el cumplimiento de sus obligaciones.

Relaciones con los medios de comunicación

La difusión que realizan los medios de comunicación del derecho a la protección de datos es un elemento esencial tanto para fomentar la sensibilización y el conocimiento de los ciudadanos en esta materia como para que los responsables cumplan con sus obligaciones legales. La Agencia mantiene la atención personalizada a los medios, que contribuyen al fomento de la protección de datos realizando una labor de divulgación imprescindible. Durante 2016, los medios plantearon ante la AEPD más de 400 cuestiones relativas a este derecho fundamental. Los temas consultados con mayor frecuencia hacen referencia a los siguientes temas, buena parte de los cuales se encuentran recogidos con mayor detalle en otros apartados de esta Memoria:

- Política de privacidad de Google. Constatación de que la compañía ha introducido modificaciones significativas en materia de información, consentimiento y ejercicio de derechos, áreas sobre las que la AEPD le requirió que hiciese cambios tras constatar incumplimientos en una resolución de 2013.
- Reglamento General de Protección de Datos. Implicaciones prácticas para ciudadanos y responsables de tratamiento. Proceso de adaptación de los sujetos obligados durante el período de transición hasta su plena aplicabilidad (mayo 2018); retos de las Autoridades de Protección de Datos; líneas de actuación de la AEPD en relación al cumplimiento del Reglamento por parte de las organizaciones, con especial atención a las pymes.
- Presentación de nuevas guías educativas para no cometer ni ser víctima de conductas delictivas en internet, en las que se explica de forma detallada a menores, padres y profesores cómo una utilización inadecuada de la información personal puede ser no sólo una infracción de la normativa de protección de datos sino también constitutiva de un delito, en ocasiones por desconocimiento.
- Sentencia del Tribunal Supremo donde el Tribunal clarifica ante quién deben dirigirse las peticiones de 'derecho al olvido'. Los usuarios pueden seguir dirigiéndose a Google, por ejemplo, a través del formulario que la compañía mantiene habilitado en español desde el 30 de mayo de 2014 y, si Google deniega la solicitud del interesado o éste no estuviera conforme con la decisión de la compañía, puede solicitar la tutela de la Agencia.
- Cifras de reclamaciones por 'derecho al olvido' tramitadas por la Agencia desde la sentencia del Tribunal de Justicia de la Unión Europea en mayo de 2014.
- Imágenes de menores publicadas en redes sociales por sus padres. Derechos de los menores y consejos para los padres, que no siempre son conscientes de cómo pueden difundirse las imágenes que ellos mismos publican de sus hijos.
- Videovigilancia. Datos actualizados y por provincias del Registro General de Protección de Datos, así como requisitos legales para la instalación de cámaras.
- Aprobación de la Decisión de adecuación del Escudo de Privacidad UE-EEUU para la

realización de transferencias internacionales de datos.

- Drones y posibles riesgos para la privacidad. Utilización de estas aeronaves para la captura, recogida y tratamiento de datos personales. Proporcionalidad y medidas de seguridad.
- Utilización de tecnologías como el big data en el ámbito sanitario para la investigación de enfermedades. Técnicas de anonimización.
- Internet de las cosas. Análisis y riesgos a los que podrían enfrentarse los ciudadanos al aportar información a través de diferentes dispositivos sobre sus hábitos de conducta y en ocasiones sin ser plenamente conscientes de ello.
- Acceso por parte de los padres a las notas de los hijos mayores de 18 años bajo ciertas circunstancias.
- Confirmación de apertura de actuaciones previas de investigación en varios casos de relevancia pública, detalles sobre su motivación y plazos para la resolución de los mismos.
- Cambios en la política de privacidad de WhatsApp. Inicio de actuaciones previas de investigación de oficio por parte de la Agencia. Carta del Grupo de Autoridades europeas de protección de datos a WhatsApp expresando sus dudas y preocupación por los cambios realizados en las condiciones de uso y en la que se solicita a la compañía que no siga adelante con el intercambio de datos de los usuarios hasta que se confirme que ofrece las suficientes garantías legales. Reacción de WhatsApp comunicando a las Autoridades que no ha iniciado el intercambio de información.
- Privacidad en la instalación de apps. Claves y consejos prácticos en materia de privacidad y seguridad a tener en cuenta en los dispositivos conectados.
- Cifras y tendencias recogidas en la memoria 2015 de la AEPD. Análisis cualitativo en contratación irregular e inserción indebida en ficheros de morosidad, así como análisis cuantitativo de sectores con mayor volumen de sanciones.

A esta labor de respuesta a las consultas planteadas hay que sumar la comunicación proactiva realizada por la Agencia, con más de 130 notas de prensa, convocatorias y notas de agenda informativa publicadas en la web. En este sentido, se hace necesario destacar el compromiso adquirido por esta institución en su Plan estratégico 2015-2019 en cuanto a fomentar y ampliar la publicación de su agenda institucional con el objetivo de que, tanto ciudadanos como responsables puedan conocer las actividades que organiza o en las que participa la Agencia. Así, durante el año 2016 se ha publicado por primera vez la asistencia a actos por parte del equipo directivo de la Agencia más allá de su directora, con más de 80 notas de reuniones o actos públicos en los que han participado diferentes miembros de esta institución, disponibles todas ellas en este enlace.

Agenda institucional

La Agencia considera la comunicación y el intercambio de ideas con otras organizaciones como un elemento de gran importancia para avanzar en una protección ágil y eficaz del derecho a la protección de datos. Así, este organismo ha mantenido reuniones con diferentes entidades para difundir y promover este derecho fundamental desde diferentes ámbitos, agilizar los procesos administrativos y fomentar el cumplimiento de la legislación.

A continuación se recogen algunas de las reuniones institucionales y de trabajo celebradas durante 2016, así como la asistencia a actos y jornadas. En cualquier caso, como se ha comentado con anterioridad, estas pueden consultarse cronológicamente y de forma detallada en la sección Notas de agenda de la página web de la AEPD.

El Consejo Consultivo de la Agencia de Protección de Datos, establecido por 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 lo decide la dirección de la AEPD que, en todo caso, lo convoca una vez cada seis meses. Las reuniones del Consejo Consultivo para exponer y analizar la actividad de la institución tuvieron lugar el 21 de enero y el 13 de julio de 2016. En la primera de ellas se abordaron las principales actividades de la institución realizadas durante 2015, fallándose también los Premios Protección de Datos 2015, y en la segunda se expusieron las acciones realizadas en el primer semestre de 2016.

En el ámbito de las reuniones institucionales, la Agencia ha celebrado encuentros con organismos públicos y asociaciones profesionales y empresariales. Así, la AEPD ha mantenido encuentros institucionales con, entre otros, representantes de las empresas que gestionan ficheros de solvencia patrimonial Asnef, Experian, Informa y Equifax; la Asociación Profesional Española de Privacidad; las editoriales de libros digitales en el ámbito educativo –reunión a la que también asistieron representantes del Ministerio de Educación, Cultura y Deporte–; la Oficina para la Ejecución de la Reforma de la Administración (OPERA); el Consejo General del Poder Judicial; la Dirección General de Justicia y Consumidores de la Comisión Europea; y el Consejo General de Colegios de Administradores de Fincas. A estas reuniones se suman los encuentros institucionales celebrados con la Autoridad Catalana de Protección de Datos, la Agencia Vasca de Protección de Datos y el Consejo de Transparencia y Protección de Datos de Andalucía.

En el apartado de ofrecer información útil que ayude a los responsables a implementar los nuevos requerimientos que establece el Reglamento General de Protección de Datos, la Agencia ha mantenido reuniones de trabajo periódicas con representantes de la Agencia Vasca y la Autoridad Catalana de Protección de Datos en el marco del Grupo de Trabajo establecido ad hoc para abordar esta materia. Asimismo, también se han celebrado reuniones para tratar este tema con la Asociación Profesional Española de Privacidad, la Asociación Nacional de Expertos de la Abogacía TIC e ISMS Forum Spain; la Dirección de Tecnologías de la Información y las Comunicaciones (DTIC) y el Centro Criptológico Nacional; la Entidad Nacional de Acreditación; diferentes departamentos ministeriales; y la Dirección General de Industria y de la PYME del Ministerio de Economía, Industria y Competitividad, para abordar aspectos relacionados con la implementación del Reglamento y el estudio de posibles actuaciones conjuntas de sensibilización y concienciación.

Para fomentar la concienciación y promover la cooperación específica en proyectos realizados en colaboración con diferentes entidades, la Agencia también ha mantenido reuniones de trabajo con representantes del Ministerio de Educación, Cultura y Deporte; el Consejo de Consumidores y Usuarios; el Instituto Nacional de Ciberseguridad, la Escuela Técnica Superior de Ingenieros Informáticos de la Universidad Politécnica de Madrid; o la Fiscalía de Criminalidad Informática, entre otras.

Por último, en lo relativo a la colaboración de la Agencia en jornadas y conferencias para difundir diferentes aspectos del derecho fundamental a la protección de datos, la AEPD ha participado en más de una treintena de actos, entre los que pueden destacarse el XIII Foro de Seguridad y Protección de Datos de Salud, organizado por la Sociedad Española de Informática de la Salud y dedicado a los retos de la seguridad y la privacidad en la atención integral sanitaria y social; diferentes actos de difusión del Reglamento organizados por, entre otras entidades, la Autoridad Catalana y la Agencia Vasca de Protección de Datos; el encuentro EuroCloud España Expo 2016 organizado por la representación en España de la Asociación Europea EuroCloud; la jornada sobre el EU-US Privacy Shield y el impacto de la privacidad y la ciberseguridad en las relaciones transatlánticas, organizada por la Cámara de Comercio de Estados Unidos en España y la Representación de la Comisión Europea en España; el seminario Seguridad y protección de datos en los poderes judiciales del Consejo General del Poder Judicial; las reuniones de la Comisión de Cooperación de Consumo convocada por la Agencia Española de Consumo, Seguridad Alimentaria y Nutrición y la de la Comisión General de la Conferencia de Educación organizada por el Ministerio de Educación; o el VI Congreso de Regulación Publicitaria Digital

de IAB Spain. La incidencia de las nuevas tecnologías en la protección de datos también ha sido analizada por la Agencia en actos como el Taller sobre retos de seguridad y privacidad en Big Data organizado por ENISA y Telefónica, y la VIII Jornada conjunta Cátedras Telefónica UPM Beyond the big data; el VI Foro de la Gobernanza de internet en España 2016 de IGF Spain; el Foro pymes y drones: retos y oportunidades organizado por la Cámara Oficial de Comercio, Industria y Servicios de Madrid; o las X Jornadas de seguridad TIC del CCN-CERT, entre otras.

4.1.3. Página web

La página web de la Agencia ha registrado en 2016 más de 5,5 millones de accesos (5.534.282). La Agencia ha continuado publicando este año informaciones prácticas tanto para ciudadanos como para las entidades que tratan datos. A este respecto hay que destacar que todas aquellas informaciones relativas a nuevas guías, documentos de interés o secciones se recogen de manera destacada en la página de inicio de la Agencia, de forma que todos aquellos que la consultan pueden conocer de forma sencilla las novedades más importantes publicadas por este organismo.

En cuanto a acciones online específicas, con motivo del Día mundial del consumidor el 15 de marzo, la AEPD y el Consejo de Consumidores y Usuarios publicaron un documento en el que recogen los pasos básicos que debe seguir un ciudadano que haya sido víctima de una suplantación de identidad en servicios de comunicaciones para exigir sus derechos. Esta temática se eligió debido a que la Agencia ha constatado en las denuncias y reclamaciones que le plantean los ciudadanos que la contratación irregular en servicios de telecomunicaciones mediante suplantación de identidad, que suele desembocar además en una inserción indebida en ficheros de morosidad, es una de las preocupaciones más frecuentes.

A las informaciones publicadas en la web se han sumado diferentes acciones online. El 17 de mayo se conmemoró el duodécimo aniversario del Día de internet con distintas actividades que giraron en torno a la privacidad y la protección de datos. La Agencia Española de Protección de Datos forma parte del Comité de Impulso de esta iniciativa, compuesto por organizaciones de ámbito nacional que se comprometen a impulsar el desarrollo de eventos y actividades relacionadas con este día entre sus respectivas organizaciones y en sus áreas de influencia. Los diferentes actos previstos para conmemorar esta efeméride tuvieron como eje central la privacidad, tratando de fomentar tanto la concienciación ciudadana como la necesidad de que los responsables de nuevos negocios y servicios recojan y traten la información personal de manera adecuada.

En esta edición, la Agencia elaboró diferentes informaciones para difundir la celebración de este día, además de publicar un microsite en el que se recogían los principales derechos de los ciudadanos en relación con la protección de datos, y un conjunto de recomendaciones para realizar una navegación más privada.

La AEPD participó en el acto oficial de la celebración del Día de internet en el Senado, en el que puso de manifiesto algunos de los cambios más significativos que el Reglamento General de Protección de Datos incorpora para los derechos de los ciudadanos.

Tras la entrada en vigor del Reglamento General de Protección de Datos el 25 de mayo de 2016, la AEPD publicó sendas páginas para facilitar la comprensión del nuevo marco normativo, así como para facilitar a los responsables la adaptación a los cambios que incorpora y cumplir así con sus obligaciones. El primero de ellos, llamado 'El Reglamento de Protección de Datos en 12 preguntas' se trata de un documento simplificado en formato pregunta-respuesta que contesta algunas dudas comunes de carácter general. El segundo de ellos, 'Implicaciones prácticas del Reglamento General de Protección de Datos para entidades en el periodo de transición' aborda temas como el consentimiento, la información, las evaluaciones de impacto, las certificaciones o las relaciones entre responsables y encargados, de forma que las entidades puedan conocer las posibles dificultades en la aplicación del Reglamento para tomar medidas que permitan solventarlas.

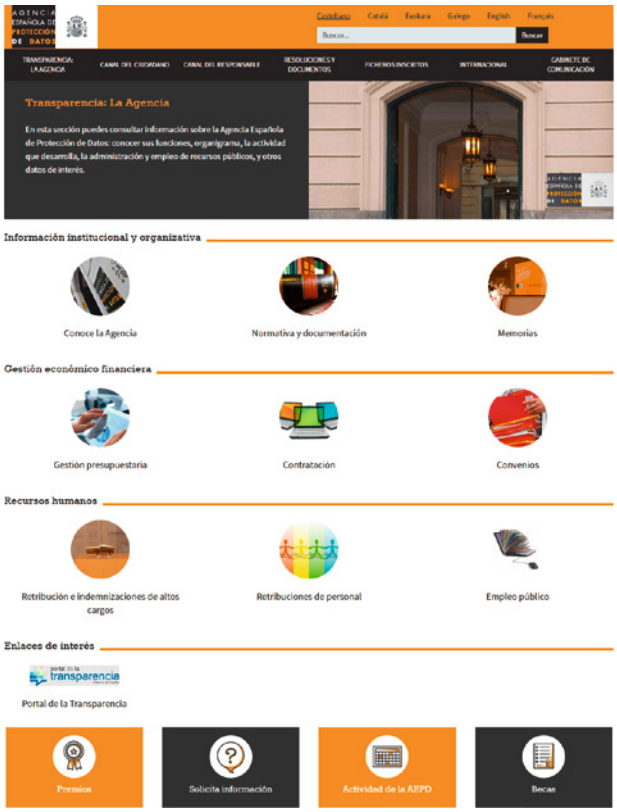
Por otro lado, uno de los ejes principales de actuación de la AEPD es apostar de forma decidida por la prevención para que los ciudadanos sean más conscientes de los derechos que les asisten y de cómo ejercerlos. La Agencia presentó el 15 de diciembre un listado de 10 claves imprescindibles en materia de privacidad y seguridad en dispositivos conectados. Entre esas claves destaca la utilización de wearables, los juguetes conectados o la instalación de aplicaciones móviles.

Por otro lado, la Agencia ya presentó en 2015, y así se recogió en la memoria de ese año, un espacio web con la información relativa al Plan Estratégico 2015-2019. En diciembre de 2016 este organismo presentó el balance del primer año del Plan, ampliando también la información ofrecida en el espacio web. Así, a los documentos incorporados con anterioridad se sumaron otros tantos que componen el informe anual de seguimiento, entre los que se encuentran el Informe de cumplimiento 2015-2016, el cuadro de actividades y los gráficos de cumplimiento, así como el detalle sistemático de las actuaciones previstas para 2017. Como ya se anunció, el Plan Estratégico de la Agencia ha sido proyectado como un documento que permite la incorporación y el desarrollo de nuevas iniciativas, el enriquecimiento de las ya existentes y su adaptación en función del diagnóstico realizado. Por ello, en el espacio web dedicado al Plan la Agencia mantiene abierto un Buzón de sugerencias, de forma que ciudadanos, responsables de tratamiento, expertos en protección de datos y organizaciones públicas y privadas puedan realizar sus sugerencias y aportaciones.

4.1.4. Canal de transparencia

La Agencia quiere reforzar su compromiso con la transparencia. Un primer paso importante fue la consulta pública sobre el Plan Estratégico en 2015, que recibió casi 400 aportaciones, y que ha continuado en 2016 con la retransmisión en *streaming* de la Sesión Anual Abierta de la Agencia y la presentación pública del balance de ejecución del primer año del Plan y de sus líneas prioritarias para el 2017.

Durante el año 2016, se ha actualizado la información que se publica en el canal web llamado «Transparencia: la Agencia», que fue creado en cumplimiento de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno, y cuya finalidad es facilitar a los ciudadanos de una forma clara y ordenada todos los contenidos de publicidad activa que regula la citada Ley.



El canal de transparencia se muestra dividido en cinco grandes grupos, mostrando en cada uno de ellos respectivamente datos de Información institucional y organizativa; Gestión económica financiera; Recursos humanos; Enlaces de interés (Portal de la transparencia del Gobierno de España); Datos de interés anuales en cuanto a denuncias y reclamaciones registradas y resueltas, ficheros inscritos o autorizaciones de transferencias internacionales, entre otros. A estas secciones se suman los apartados relativos a los Premios, un enlace para solicitar información, la actividad de agenda institucional o información referente a becas.

Este canal recibió un total de 305.538 visitas en el año 2016.

Por otra parte, y respecto a las peticiones de acceso a la información pública, se recibieron 60 solicitudes, de las cuales se concedieron 28, se inadmitieron 16, en 2 desistieron los solicitantes y 1 fue denegada.

Sobre las inadmitidas, el motivo fue la aplicación del artículo 18 de la Ley 19/2013 (abuso de derecho, solicitudes repetidas, reelaboración de la información) así como la Disposición Adicional 1.ª de la citada Ley (aplicación de otra normativa específica que regula el derecho de acceso).

Por último, señalar que dentro de esas 60 solicitudes, en 13 casos lo que se recibió a través del Portal de Transparencia del Gobierno de España eran consultas y no solicitudes de acceso a la información.

4.1.5. Actividades de divulgación

Las actividades detalladas con anterioridad en esta Memoria se han reflejado en las acciones de divulgación específicas realizadas por la Agencia. Así, la AEPD ha participado en numerosos foros y eventos organizados por terceros, fomentando así la difusión de los trabajos realizados por la institución. Estos actos pueden ser consultados, como ya se ha mencionado, en la sección Agenda de la página web.

La Agencia, por su parte, también ha organizado diferentes acciones específicas orientadas a difundir este derecho fundamental tanto entre los ciudadanos como entre las empresas y los profesionales de la protección de datos. Estas actividades han estado relacionadas en gran medida con la celebración de eventos y la presentación de proyectos de largo recorrido:

- **Jornada sobre «Privacidad, menores y conductas delictivas»**

El 28 de enero de 2016, con motivo de la celebración del Día europeo de Protección de Datos, la Agencia celebró en su sede la jornada «Privacidad, menores y conductas delictivas». La AEPD seleccionó este tema como eje central de la jornada teniendo en cuenta las advertencias de los expertos acerca del incremento de los delitos cometidos por menores a través de internet, y en especial, aquellos que tienen vinculación con el uso de la información personal. Según la Comisión Europea, 4 de cada 10 menores se han visto implicados en situaciones de riesgo en internet y, conforme a una encuesta del Ministerio del Interior, 2 de cada 3 menores tienen perfil en redes sociales y de ellos un tercio más de uno.

En la Jornada se presentaron dos nuevas guías: «Sé legal en internet», dirigida a jóvenes, y «Enséñales a ser legales en internet», para padres y profesores, con el objetivo de sensibilizar acerca de las graves consecuencias de determinadas conductas realizadas en internet.

- **29 de junio. 8.ª Sesión Anual Abierta de la AEPD**

El 29 de junio de 2016 se celebró la 8.ª Sesión Anual Abierta de la AEPD en el Auditorio Ramón y Cajal, ubicado en la Facultad de Medicina de la Universidad Complutense de Madrid. El Reglamento Europeo de Protección de Datos (RGPD), que había entrado en vigor el 25 de mayo de 2016, y los retos a los que se enfrenta este derecho fundamental fueron los temas centrales de la sesión, que fue inaugurada por el Ministro de Justicia, Rafael Catalá.

La tradicional Sesión Anual está dirigida a representantes de instituciones, empresarios, profesionales de la protección de datos y ciudadanos interesados en la materia, y es abierta, gratuita y de carácter esencialmente práctico. En esta ocasión, para potenciar la difusión de los contenidos abordados, el evento se retransmitió por primera vez en *streaming*, con más de 1.500 asistentes virtuales, que se sumaron así a los más de 500 que pudieron asistir de manera presencial. La Agencia considera su Sesión Anual como un punto de encuentro con los representantes de entidades, empresarios y profesionales de la protección de datos, proporcionando una exposición y un análisis detallado de las novedades acaecidas en el último año.

En la primera parte se abordaron los retos a los que se enfrenta el derecho fundamental, así como la creación de la Unidad de evaluación y estudios tecnológicos (recogida con detalle en otro apartado de esta Memoria). En la segunda parte, se analizaron las principales novedades producidas tanto en el ámbito nacional como internacional y, por último, en la tercera parte, vespertina, se trataron las novedades del RGPD y su repercusión en la legislación actual, analizando los principios y derechos de la nueva normativa, las obligaciones de responsables y encargados, así como los códigos de conducta, las certificaciones y las transferencias internacionales, para finalizar con la supervisión y el régimen sancionador establecidos por dicho Reglamento. Durante el evento también se entregaron los «Premios Protección de Datos 2015».

Como cada año, la Agencia también optó por publicar con posterioridad a la celebración de la sesión un espacio web específico 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, facilitando así materiales de consulta.

- **Entrega de los Premios Protección de Datos 2015 (XIX edición)**

Estos galardones, que se entregan cada año en el marco de la Sesión Anual Abierta, reconocen los trabajos de Comunicación e Investigación que promueven en mayor medida la difusión y la investigación del derecho fundamental a la protección de datos. Así, la AEPD entregó el 29 de junio los Premios de Protección de Datos 2015 (XIX edición), premiando la labor realizada por los medios de comunicación en la difusión de este derecho fundamental y el trabajo de los investigadores, que con sus análisis sobre la legislación y la evolución de las sociedades contribuyen a la reflexión sobre esta materia.

El jurado –compuesto por el Consejo Consultivo de la AEPD– concedió el premio principal de comunicación ex aequo a las periodistas de EFE Violeta Molina y Amaya Quincoces por sus informaciones relacionadas con la privacidad y la protección de datos, en las que abordaron temas como el Reglamento General de Protección de Datos, el Big data o el denominado «derecho al olvido», entre otros. Asimismo, el jurado otorgó un accésit a Ángel Luis Sucasas por sus reportajes publicados en el diario El País y en elpais.com dedicados, entre otros aspectos, a la protección de datos de los menores o a los retos del Internet de las Cosas.

En la categoría de Investigación, se concedió el premio en la modalidad de trabajos originales e inéditos a Amaya Noain Sánchez por su trabajo «La protección de la intimidad y vida privada en internet: la integridad contextual y los flujos de información en las redes sociales», mientras que se otorgó un accésit dentro de la misma modalidad a Elena Gil González, por su trabajo «Big Data, privacidad y protección de datos».

Finalmente, 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 a la candidatura de Luis Fernando Cote Peña, por su trabajo «Habeas data en Colombia, un trasplante normativo para la protección de la dignidad y su correlación con la NTC/ISO/IEC 27001:13».

La Agencia Española de Protección de Datos editó los trabajos galardonados en la categoría de Investigación, que pueden descargarse en la sección Publicaciones de página web de la AEPD.

- **Presentación de la «Guía sobre privacidad y seguridad en internet»**

La Agencia Española de Protección de Datos y el Instituto Nacional de Ciberseguridad (INCIBE) presentaron el 7 de octubre la «Guía sobre privacidad y seguridad en internet», una apuesta conjunta para concienciar a los usuarios de la importancia de proteger su información personal y que se ha detallado en un apartado anterior de esta Memoria.

- **Balance del primer año del Plan Estratégico de la AEPD**

El 1 de diciembre de 2016 la Agencia presentó en su sede el balance del primer año de su Plan Estratégico.

Durante el acto también se expusieron las líneas prioritarias que debe afrontar la Agencia en 2017, destacando, por un lado, la publicación de nuevas vías y materiales para informar a los ciudadanos de sus derechos y, por otro, sentar las bases para que tanto las entidades como los profesionales de la privacidad puedan adaptarse de forma paulatina al Reglamento General de Protección de Datos. En este sentido, la Agencia anunció que contemplaba prestar especial atención a las pymes, que constituyen el 99% del tejido empresarial español, para facilitarles herramientas y orientaciones que les permitan cumplir con la nueva legislación. Algunos de esos materiales, a fecha de cierre de esta Memoria, ya han sido presentados y se recogen en un apartado específico de la página web de la Agencia, si bien no se detallan en este documento de forma exhaustiva por estar fuera del ámbito temporal del mismo.

4.2. MÁS Y MEJORES SERVICIOS

4.2.1. Sede electrónica

Durante el año 2016 ha sido notable el aumento de entradas por medios electrónicos (certificado electrónico) a través de la Sede electrónica de la AEPD. El número de trámites electrónicos se ha multiplicado por tres como resultado de la incorporación de la tramitación a través de la Sede de notificaciones de solicitudes de modificación e inscripción de ficheros y copias de su contenido. En relación al resto de trámites electrónicos, se ha multiplicado por 2,5 el número de documentos presentados por registro electrónico.

4.2.2. Digitalización. AEPD Digital

Con los objetivos de digitalización marcados en el plan estratégico de la AEPD, durante 2016 se han llevado a cabo los siguientes trabajos:

- Firma electrónica: se han iniciado los trabajos para la utilización de la firma electrónica en la generalidad de la tramitación de los procedimientos de la AEPD.
- Sede electrónica: durante el mes de julio de 2016 se han puesto en marcha mecanismos que facilitan a los ciudadanos la tramitación electrónica sin necesidad de utilizar un certificado electrónico. En la actualidad es posible acceder a los trámites electrónicos de la AEPD mediante sistemas de clave temporal y permanente (CL@VE PIN y CL@VE PERMANENTE) disponibles para todas las Administraciones Públicas.
- Administración electrónica: Se ha realizado la contratación de los servicios para la ejecución de trabajos encaminados a potenciar la Administración Electrónica en la AEPD:
  - Desarrollo de la plataforma de servicios electrónicos de la Agencia que permitirá la interconexión de los procedimientos electrónicos de la AEPD con los servicios

de administración electrónica existentes y futuros.

- Plataforma de intermediación de la Administración General del Estado (AGE): se ha dotado a la Agencia de los medios técnicos necesarios para el intercambio de información con la plataforma de intermediación.
- Sistema de notificaciones electrónicas y acceso telemático al expediente: la AEPD ha trabajado durante el último año para adecuar sus recursos técnicos a fin de poder iniciar las notificaciones electrónicas y permitir el acceso telemático a los distintos tipos de expedientes progresivamente.

Con el objeto de consolidar los servicios electrónicos de los que la AEPD ha sido dotada durante 2016, se ha iniciado un proceso de adecuación de los sistemas de información internos y la sede de la AEPD. Con la ejecución de este proceso de adecuación, los ciudadanos y los responsables de tratamientos de datos personales podrán tener acceso a los servicios electrónicos de la AGE (NOTIFIC@, Carpeta Ciudadana, Dirección Electrónica Habilitada, etc.)

- Sistema de Interconexión de Registros: durante el segundo semestre de 2016 se han iniciado los trabajos encaminados a la integración del Registro Electrónico de la AEPD con el Sistema de Interconexión de Registros de la AGE (SIR).

4.3. SIMPLIFICACIÓN Y MEJORA DE LA GESTIÓN INTERNA

La preocupación continua por mejorar la gestión y conseguir una respuesta más ágil a las peticiones y denuncias a los ciudadanos se ha visto marcada este año por dos eventos distintos. El primero ha sido el informe realizado por la Inspección General de Servicios del MINHAP sobre la Subdirección General de Inspección de Datos (SGID), y el segundo la entrada en vigor de leyes 39 y 40 de 2015, el pasado 3 de octubre de 2016.

El 8 de febrero de 2016 la Directora de la AEPD solicitó a la Dirección General de Organización Administrativa y Procedimientos del Ministerio de Hacienda y Administraciones Públicas la realización de un estudio de los procedimientos seguidos por la Subdirección General de Inspección de Datos de la Agencia, con el fin de optimizarlos y conseguir mejorar la gestión ante la elevada carga de trabajo por el incremento exponencial de las denuncias y reclamaciones de tutela de derechos desde el año 2008.

El informe elaborado, junto con el Plan estratégico 2015-2019, constituye un marco de referencia muy completo para abordar los nuevos retos a los que se enfrenta la Agencia y dar respuesta al elevado número de expedientes que se tramitan.

El informe destaca la necesidad de una mayor planificación y dirección por objetivos, así como la definición de indicadores que permitan un mejor conocimiento y seguimiento de la actividad desarrollada.

El análisis realizado pone de manifiesto que la SGID está basada en una estructura y unos sistemas de trabajo que no permiten maximizar el rendimiento y que no han sido adaptados a la nueva estrategia y retos de la Agencia. Esto hace que los tiempos de tramitación sean demasiado largos, y que la disponibilidad de recursos para afrontar otras tareas sea escasa. Los sistemas de reparto de trabajo tradicionales deben dar paso a otros mecanismos más flexibles como las herramientas de flujo de trabajo electrónico. Asimismo el informe señala debe mejorarse la comunicación interna y la gestión del conocimiento (procedimientos y criterios) acumulado durante los años de actividad.

Respecto a la tramitación de los expedientes, se indica que debe aligerarse el modelo de tramitación, buscando una reducción de plazos en todas las fases. Se precisa asimismo simplificar los mecanismos de supervisión, y automatizar aquellos procesos que sea posible, dando pasos hacia

una verdadera transformación digital. Entre otros logros concretos a conseguir el informe señala la firma electrónica para todos los documentos, la extensión de la notificación por comparecencia en Sede Electrónica a todos los procedimientos de la AEPD, y la puesta en marcha del Archivo digital y el sistema integral de notificaciones de la AGE.

El informe propone incluso una estructura organizativa para la Subdirección, con áreas funcionales bien diferenciadas para la admisión, la investigación de denuncias, la instrucción de los procedimientos y una unidad para la coordinación de criterios y la comunicación.

Algunas de las recomendaciones del informe ya se han transformado en medidas puestas en marcha a lo largo del último trimestre del año, y otras se irán implantando de forma progresiva junto con acciones derivadas del Plan Estratégico 2015-2019, y las acciones preparatorias para la aplicación efectiva del Reglamento Europeo de Protección de Datos, en mayo de 2018.

Entre estas mejoras emprendidas puede señalarse la puesta en funcionamiento de la Unidad de Admisión, que actualmente procesa alrededor de 800 denuncias y reclamaciones al mes, resolviendo más de un 80% de las mismas. Con esta medida se está produciendo una reducción en los tiempos de primera respuesta a los ciudadanos que se dirigen a la Agencia, así como una mayor eficacia en la realización de las investigaciones pertinentes y la tramitación de expedientes. Con la puesta en marcha de ésta y otras medidas se está consiguiendo una mejora tangible en los tiempos de tramitación y en el volumen de expedientes tramitados. No obstante, no debe olvidarse que cabe pensar que la entrada en vigor del Reglamento (UE) 2016/679 exigirá una adecuación de las medidas de mejora en la gestión a fin de adaptarlas a las exigencias que esta norma europea incorporará en todos los ordenamientos europeos y, muy particularmente, en aquellos supuestos en los que la participación de la Agencia española no sea exclusiva y haya de contar necesariamente con la actuación de otras agencias o autoridades nacionales. Esta circunstancia hace necesario un esfuerzo y refuerzo adicional de los medios humanos y materiales para poder afrontar el desafío con las debidas garantías.

Por otra parte, el pasado 3 de octubre de 2016 entraron en vigor las leyes 39/2015 y 40/2015 del Procedimiento Administrativo Común de las Administraciones Públicas, y de Régimen Jurídico del Sector Público, respectivamente. El extenso articulado de ambos textos, el ámbito de aplicación y la novedad de muchos de sus principios han supuesto un reto importante para la organización y funcionamiento de la Agencia. La Ley 39/2015, de 1 de octubre tiene un impacto fuerte en la tramitación de los procedimientos sancionadores de la Agencia, introduciendo simplificaciones en la tramitación como el reconocimiento espontáneo de la responsabilidad de los denunciados, o el pago adelantado con descuento de la sanción, que están contribuyendo a aligerar la carga de expedientes tramitados. Asimismo la Ley pone énfasis en el uso de medios electrónicos para la comunicación con los ciudadanos y entre administraciones, así como para la propia tramitación de los expedientes. La implantación de estas medidas es compleja y costosa, por lo que se está abordando de una forma progresiva y con las máximas garantías.

Por su parte, la Ley 40/2015 tiene un impacto limitado en algunas facetas del procedimiento sancionador como la recusación, la retroactividad o la responsabilidad. Sin embargo, en su articulado se introducen importantes novedades en sus principios generales como la planificación y dirección por objetivos y el control de la gestión y evaluación de los resultados de las políticas públicas.

Será preciso analizar los indicadores de desempeño y resultados del año 2017 para conocer de forma numérica el alcance de las iniciativas puestas en marcha a partir del Informe de la Inspección de Servicios y de la entrada en vigor de las leyes citadas, si bien ya puede afirmarse que ambas han marcado un punto de inflexión tanto en la gestión interna del trabajo de tramitación de denuncias y peticiones de tutelas como en la relación con el ciudadano.

4.4. PROGRAMA PILOTO DE TELETRABAJO

En el marco del proceso de modernización y de búsqueda de una mayor calidad del servicio público, la Agencia Española de Protección de Datos está decidida a atraer y retener a los mejores profesionales. En este entorno, se ha considerado el teletrabajo como una herramienta flexible, capaz de incrementar la productividad del tiempo de trabajo de los empleados públicos basándose en las múltiples prestaciones que ofrecen las tecnologías de la información y la telecomunicación, al tiempo que facilita la conciliación de la vida personal, familiar y laboral de los empleados públicos.

Durante el año 2016 se ha trabajado en el diseño de un Programa Piloto de Teletrabajo en el que participará un 10% de la plantilla, con objeto de desarrollar un modelo que permita evaluar el impacto del teletrabajo en la organización y en la prestación de servicios, y la viabilidad de luna futura extensión del programa a todos los ámbitos de actividad posibles en la Agencia.

El programa se convocó el 24 de noviembre de 2016 con 17 plazas y una duración de 6 meses. Una vez seleccionados los participantes se firmará un acuerdo de teletrabajo con cada uno de ellos en el que se establecerán los días de la semana (1 o 2) en los que realizarán su actividad en la modalidad de teletrabajo, así como las tareas a realizar y la planificación de los objetivos, plazos y criterios con los que se realizará una evaluación periódica de las tareas asignadas por el responsable de cada unidad.

Se ha previsto que la ejecución de este programa no suponga incremento del gasto del Organismo.

Los representantes de los empleados en la Junta de Personal han participado en la elaboración del programa y lo harán igualmente en su evaluación.

4.5. NECESIDADES DE RECURSOS HUMANOS Y MATERIALES

La AEPD cuenta en la actualidad con una Relación de Puestos de Trabajo dotada de 159 puestos de personal funcionario y 6 de personal laboral. Esta dotación de puestos se ha mantenido prácticamente invariable desde el 2008, año en el que se aprobó por la Comisión Ejecutiva de la Comisión Interministerial de Retribuciones (CECIR) un incremento importante del número de puestos de trabajo para adaptar la AEPD al volumen de trabajo que le correspondía entonces.

Desde aquella adaptación la Agencia ha visto incrementadas de manera exponencial sus competencias por diversas normas sectoriales y por la propia evolución que ha experimentado el uso de las nuevas tecnologías, mientras que el volumen de efectivos que prestan servicio en ella no sólo no se ha incrementado para adecuarse a la nueva situación, sino todo lo contrario, se ha reducido por la imposibilidad de cubrir una parte importante de los puestos de trabajo.

La protección de datos vive un momento decisivo, con retos constantes puesto que la digitalización de la información ha ampliado enormemente las posibilidades de recogida, almacenamiento y procesado de la misma, a la vez que en los últimos años se han incrementado de forma extraordinaria la cantidad y variedad de datos personales que recogen y tratan tanto actores públicos como privados.

Por todo ello la AEPD ha experimentado un enorme incremento de su carga de trabajo, que incluso se ha triplicado en muchas de sus unidades, resultando que los recursos disponibles para afrontar la actividad de gestión ordinaria ya antes de la aprobación del RGPD en abril de 2016 eran insuficientes, al no haberse modificado la dotación de recursos humanos ni los créditos destinados a incentivar el rendimiento del personal hasta 2016.

A lo anterior se añaden ahora las nuevas funciones que el Reglamento Europeo ha asignado a las autoridades de control de los Estados Miembros de la Unión Europea que exige la adaptación de la normativa actualmente vigente y la colaboración con las autoridades de otros países en la gestión de asuntos de grandes corporaciones internacionales, o la introducción de la figura del Delegado de protección de datos (DPO) en organismos públicos y entidades privadas entre otras actuaciones.

Es evidente que el propio legislador ha sido consciente del cambio cualitativo y cuantitativo que supondrá la entrada en vigor del Reglamento. Esta conciencia se pone de manifiesto en el artículo 52 del Reglamento en el que se establece la obligación de los Estados Miembros de garantizar a cada autoridad los recursos humanos, técnicos y financieros necesarios para el cumplimiento efectivo de sus funciones.

Por parte del Ministerio de Hacienda y Función Pública se ha dado ya un primer paso en diciembre de 2016 en esta línea asumiendo un incremento significativo del crédito destinado a los incentivos al rendimiento para el personal funcionario de la Agencia, que esperamos permita a esta ser más competitiva a la hora de captar recursos y cubrir los puestos de trabajo vacantes, pero además es necesario que se adopten igualmente medidas que permitan incrementar el número de puestos de trabajo de la Agencia de forma significativa como ya se está haciendo en otros países de nuestro entorno igualmente afectados por la entrada en vigor del nuevo Reglamento.

Hoy en día la protección de datos y la privacidad se sitúan en todas las encuestas entre las preocupaciones más destacadas de los ciudadanos, y corresponde a la Agencia tanto la obligación de velar por el cumplimiento de sus deberes en este ámbito por todos los actores implicados, como la de difundir el derecho y proteger a los ciudadanos desarrollando instrumentos proactivos que mejoren la protección de datos y para ello es estrictamente indispensable contar con más medios especialmente preparados para estas nuevas tareas. Sirvan de ejemplo las dirigidas a la prevención y concienciación en la utilización de las nuevas tecnologías por la generalidad de los ciudadanos y especialmente por determinados colectivos como son los menores, o por los sujetos obligados como son las empresas o Administraciones Públicas.

5 UNA AGENCIA CERCANA A LOS RESPONSABLES Y PROFESIONALES DE LA PRIVACIDAD

5.1. RECURSOS PARA FACILITAR EL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS POR LOS RESPONSABLES, EN ESPECIAL POR LAS PYMES

5.1.1. Ficheros inscritos en el Registro General de Protección de Datos

En este epígrafe se presenta la evolución de la inscripción de ficheros durante el año 2016, que viene constituyendo uno de los indicadores para evaluar el grado de conocimiento de la normativa de protección de datos por los responsables del tratamiento. Con la aprobación del Reglamento General de Protección de Datos que, como ya se ha mencionado con anterioridad, entró en vigor en mayo de 2016 y comenzará a aplicarse el 25 de mayo de 2018, se elimina la obligación de inscribir los ficheros en los registros públicos de protección de datos. Esta circunstancia podría haber supuesto un decremento en el número de notificaciones de ficheros al Registro General de Protección de Datos y, sin embargo, no ha sido así.

El año 2016 finalizó con un total de 4.510.346 ficheros inscritos en el Registro, cifra que supone un incremento del 9,8% respecto al cierre de 2015. El 96,41% son ficheros de titularidad privada, es decir, 4.348.454, que aumentaron en un 10% y el 3,59% corresponde a los 161.892 ficheros de titularidad pública, cuyo incremento en este periodo anual fue algo inferior al 3%.

En lo que corresponde a la Administración General del Estado (AGE) el número de ficheros inscritos se mantiene prácticamente estable con un crecimiento del 5,7%.

Con respecto a las Administraciones de las Comunidades Autónomas el número total de ficheros inscritos muestra un fuerte incremento en la inscripción de ficheros de La Rioja e Illes Balears, con incrementos de más de un 56% y un 16%, respectivamente. El resto de las CCAA mantienen crecimientos por debajo del 8%, lo que demuestra su total adaptación.

En la Administración local destacan los incrementos de notificaciones y de ficheros inscritos en las provincias de Guadalajara, Cuenca, Cáceres, Ávila y Lugo.

Para una información adicional pueden consultarse los apartados correspondientes de la sección La Agencia en cifras de esta Memoria.

En 2016 se han tramitado un total de 16.749 solicitudes de información registral, lo que supone un incremento de casi un 11% con respecto a las solicitudes atendidas en 2015. Estas solicitudes son una herramienta útil para el responsable a la hora de realizar una puesta al día sobre los tratamientos de datos de carácter personal que su entidad está realizando, y para adaptarse a las previsiones del nuevo Reglamento en relación con el Registro de actividades de tratamiento.

Durante el pasado año más del 93,5% de las solicitudes entraron a través de la sede electrónica. De ellas, más del 60% se reciben ya firmadas electrónicamente.

5.1.2. Herramientas EVALÚA y DISPONE

Las herramientas EVALÚA y DISPONE que la AEPD ofrece a través de su página web para evaluar el

cumplimiento de la LOPD y de las medidas de seguridad, la primera, y para ayudar a la elaboración de la disposición general de creación, modificación o supresión de ficheros de titularidad pública, la segunda, siguen demostrando su utilidad para los responsables de los ficheros, aunque de manera desigual. EVALÚA ha visto incrementado su uso tanto en el número de accesos como en el número de informes elaborados en más de un 35%, mientras que DISPONE sólo ha experimentado incremento en su número de usuarios, siendo las Administraciones y Organismos Locales, quienes más la han utilizado, aunque también se ha registrado un incremento de su uso por las Administraciones y Organismos de las CCAA, los Colegios Profesionales, las Universidades Públicas y las Federaciones Deportivas.

No obstante, ante la próxima aplicación efectiva del RGPD, la Agencia inició los trabajos de desarrollo de una herramienta para pymes que realizan tratamientos de bajo riesgo para facilitar su adecuación al Reglamento, que será presentada fuera del ámbito temporal de esta Memoria.

5.1.3. Códigos tipo

Los códigos tipo o códigos de conducta son un mecanismo de autorregulación que facilitan el cumplimiento de la normativa de protección de datos en determinados sectores, adaptándola, a partir de la regulación establecida con carácter general, a las características de cada uno de ellos.

El Reglamento General de Protección de Datos (RGPD) asigna un papel relevante a los códigos de conducta como mecanismo para poder acreditar su observancia por los sujetos obligados, y ofrece ciertos incentivos para fomentar su adopción y la adhesión. Este impulso que el RGPD da a la autorregulación y que obliga, entre otras, a las autoridades de control a promoverlos entre los distintos sectores de actividad constituye un nuevo marco que, sin duda, atraerá el interés de los interesados, como se ha podido observar en el último tramo del año 2016.

En 2016 se han registrado los códigos tipo que se relacionan a continuación:

- Código tipo de protección de datos para organizaciones sanitarias privadas, promovido por la Federación Nacional de Clínicas Privadas (FNCP), Asociación Nacional de Actividades Médicas y Odontológicas de la Sanidad Privada (AMOSP), Asociación Nacional para la Promoción de la Excelencia en las Actividades Sanitarias Privadas (ANEASP), Associació Catalana d´Entitats de Salut (ACES) y Asociación de Empresas de Prestación Asistencial de Andalucía (AESPAA), cuyo ámbito abarca la gestión clínica, la gestión fiscal y contable, la gestión de incidencias, la gestión de personal y la gestión societaria.

  Asimismo se acordó la cancelación de la inscripción del Código tipo de la Agrupación catalana de establecimientos sanitarios, promovido por la Associació Catalana D'Entitats de Salut, por cuanto que se integró como promotora del código tipo citado en el párrafo anterior.

- Modificación del Código tipo del fichero histórico de seguros del automóvil y del Código tipo del fichero de pérdida total de automóviles promovida por la Unión Española de Entidades Aseguradoras y Reaseguradoras (UNESPA).

El interés despertado por la figura de los códigos de conducta previstos en el Reglamento se puede apreciar en sectores como el asegurador, el de la salud, el de la publicidad o la investigación de mercados, con los que se han mantenido contactos de cara a la presentación de solicitudes de inscripción de códigos tipo. En estos contactos, la Agencia ha fomentado su elaboración teniendo en cuenta el contenido que establece el RGPD sobre los códigos de conducta, en especial, en lo que se refiere al establecimiento de mecanismos que favorezcan una vía para la resolución extrajudicial de los conflictos que se puedan presentar entre las entidades adheridas y los interesados, propiciando, sin perjuicio de los derechos de los afectados, una resolución ágil y satisfactoria de los intereses en juego.

5.1.4. 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 387, de las cuales 211 (54.5%) fueron planteadas por las Administraciones Públicas y 176 (45.5%) por el sector privado.

Se produce así una disminución de un 20% en el volumen de consultas planteadas respecto a las formuladas el año anterior. Ello se debe fundamentalmente a la menor actividad del sector público y, particularmente, de la Administración General del Estado durante el año 2016. Así puede deducirse del hecho de que mientras las consultas procedentes del sector privado mantienen prácticamente las mismas cifras que en 2015 (en que fueron 180 las planteadas), las consultas procedentes del sector público han sufrido una disminución de un 31% (de 305 en 2015 a 211 en 2016).

De este modo, se produce una alteración en el reparto de las consultas entre los sectores público y privado, dado que las pertenecientes a éste último han incrementado su peso de un 37% a un 45.5%, siendo correlativa la disminución de las consultas del sector público.

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 2016 se produce una disminución de su número de en torno al 13%.
- La importante disminución de en torno a un 32% de las cuestiones relacionadas con los ficheros de los que son responsables las Administraciones Públicas, como consecuencia de la menor incidencia de las cuestiones planteadas por el sector público, a la que ya se ha hecho referencia.
- El incremento de la importancia relativa de las cuestiones relacionadas con los requisitos del consentimiento, que aumentan del 16% al 22% del total, incrementándose igualmente su número, en términos absolutos, en un 6%.
- El más que significativo incremento de las cuestiones planteadas en torno a los conceptos generales de la protección de datos, que se incrementan en un 41% respecto al año 2015
- El repunte de las cuestiones en que se plantea la posible legitimación de un determinado tratamiento en lo dispuesto en el artículo 7 f) de la Directiva 95/46/CE, que aumentan un 150% respecto de 2015, suponiendo en torno al 4% del total.
- La disminución de las cuestiones relacionadas con la conciliación de las normas de protección de datos con el principio de transparencia y el acceso a la información pública, una vez desaparecido el efecto derivado de la entrada en vigor de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, que disminuyen en casi un 63% pasando a representar un poco más de un 3% del total, frente al más del 7% que representaban en 2015.
- La drástica disminución de las cuestiones relacionadas con la existencia y funciones de los encargados del tratamiento, que se reducen a poco más de la tercera parte de las planteadas en 2015, probablemente al haber desaparecido el efecto producido como consecuencia de la problemática ocasionada por la anulación por la sentencia del Tribunal de Justicia de la UE de 6 de octubre de 2015, de la Decisión de adecuación del sistema de puerto seguro y la aprobación de la decisión de adecuación del denominado «escudo de privacidad».
- El incremento significativo de las consultas relacionadas con los ficheros de titularidad privada (un 100%), las transferencias internacionales de datos (un 30% o la videovigilancia (un 9%).

- La importante disminución de las consultas relacionadas los registros públicos (un 79%), las medidas de seguridad (un 77%) o los datos especialmente protegidos (un 52%).

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 2015, si bien se produce un descenso de más del 2.5% del peso de las consultas formuladas por la Administración General del Estado y sus Organismos vinculados o dependientes, que en términos absolutos supone una disminución de en torno al 35%. Por el contrario, las consultas planteadas por las Administraciones de las Comunidades Autónomas se incrementan en prácticamente un 3%. En cuanto al sector privado, atendiendo a la distribución sectorial de las consultas, las principales conclusiones son:

- El mantenimiento como las más abundantes 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. No obstante, el constante incremento de las mismas se ve frenado en este ejercicio, al reducirse en un 15% frente al incremento acumulado del 104% que se había producido en los dos ejercicios anteriores.

- El muy notable incremento de las consultas planteadas por prestadores de servicios de la sociedad de la información, que prácticamente doblan las del año 2015, representando un 13% del total.

- En este mismo sentido se duplican las consultas planteadas por sindicatos y partidos políticos, lo que devuelve las cifras a valores similares a los del año 2014.

- La reaparición entre los sectores relevantes a estos efectos del de agua y energía, con un 3% del total.

- La disminución muy sustancial de las consultas formuladas por el sector de distribución y gran consumo (un 60%), el de banca y seguros (un 75%, pasando ya a representar sólo un 1% del total), el de publicidad y prospección (un 75%, representando un testimonial 0.5%) y el de educación (un 80%), probablemente en éste último caso como consecuencia de las distintas acciones de divulgación emprendidas en relación con este sector por la Agencia.

- La inexistencia de informes procedentes de las empresas constructoras, que en 2015 representaban sin embargo casi un 3% del total.

Los informes no preceptivos relacionados con consultas externas que pueden revestir una mayor trascendencia, versan, entre otras, sobre las siguientes materias:

- La necesidad de que el establecimiento de un sistema de acceso a los comedores de los centros escolares basado en el uso de tecnología RFID incorporada a pulseras que portarían los alumnos y que sería objeto de lectura en el momento de ingresar al comedor escolar se someta a una previa evaluación de impacto en la protección de datos.

- La licitud del acceso, en su condición de encargada del tratamiento por una empresa que presta servicios a comedores escolares a los datos referidos a alergias o intolerancias alimentarias de los alumnos

- La aplicación de la excepción contemplada en el artículo 2.2 b) de la LOPD al tratamiento de información sobre las personas del entorno familiar de los trabajadores que contrata una entidad cuando para la realización de sus actividades se requiere la denominada «habilitación OTAN».

- La validez de la cesión a un Organismo Estadístico de la información relacionada con la ubicación de la totalidad de los terminales móviles durante un período limitado de días, a fin de servir de herra-

mienta para la realización de las operaciones estadísticas relacionadas con el censo de población y viviendas siempre que se adopte con los operadores un protocolo que garantice que la información facilitada será seudonimizada y se establezcan barreras que impidan la reversibilidad de la seudonimización.

- La consideración de datos de carácter personal de las informaciones que figuran en el registro del fabricante de un vehículo; esto es, las fechas de las revisiones y kilometraje del mismo cuando se asocian a la matrícula del vehículo, que permite la identificación de su titular a través del Registro de Vehículos de la Dirección general de Tráfico.

- El análisis de los tratamientos que podrían llevarse a cabo como consecuencia de la captación de imágenes a través de los aparatos comúnmente denominados «drones» así como, más específicamente, el estudio de las características, requisitos y circunstancias que puedan plantearse respecto de los tratamientos de datos que realicen los drones.

- La conformidad con la LOPD de la instalación de sistemas de vídeo que permitieran el seguimiento continuado de los enfermos con parálisis cerebral con el objeto de realizar el seguimiento de la salud y preservar su interés vital, al amparo de los artículos 7.6 y 11.2 f) de la LOPD, resultando sin embargo desproporcionada la instalación de estos sistemas con la finalidad de que los familiares puedan acceder en tiempo real a las imágenes de los pacientes.

- La consideración de que el registro de imágenes y sonidos de algunas partes del culto de una determinada religión incorporando no sólo imágenes de los ministros de culto, sino también de los asistentes al mismo podría ampararse en que dichos datos han sido manifiestamente hechos públicos, siempre y cuando se haya dado pleno cumplimiento al deber de información y al hecho de esa grabación y, en su caso divulgación.

- La determinación de los supuestos en que será posible la utilización con fines de control del personal del sistema de videovigilancia que ya está instalado para fines de seguridad pública, siguiendo lo sentado por la reciente doctrina del tribunal Constitucional.

- La posible atención de la solicitud de un interesado de que se proceda a la desindexación por motores de búsqueda y a la supresión por la propia consultante de la referencia que a aquélla se hace en un artículo de investigación publicado en una de sus revistas jurídicas instando al motor de búsqueda a que excluya de indexación tales informaciones, siendo esta solución preferible a la utilización de mecanismos que excluyesen la indexación de la propia publicación.

- La improcedencia de atender a una solicitud de desindexación de los datos referidos a la participación como candidato en un proceso electoral del afectado que ejercita el derecho.

- La licitud de la publicación en el portal de transparencia de una Comunidad Autónoma de una relación de nombres y apellidos de liberados sindicales y el importe del coste total de las horas dedicadas a la actividad sindical, al amparo de la normativa autonómica en materia de transparencia.

- La ilicitud de la divulgación, dentro de la actividad docente del consultante, de las informaciones reales que el mismo haya obtenido a través del ejercicio del derecho de acceso a la información pública, al tratarse de una finalidad que, de conformidad con el artículo 15.5 de la Ley de Transparencia habrá de resultar conforme a la LOPD, que exige para este caso el consentimiento del afectado.

- La conformidad con lo dispuesto en el artículo 7 f) de la LOPD de la publicación por

los laboratorios farmacéuticos de las informaciones individualizadas relacionadas con las transferencias de valor realizadas por esas entidades en beneficio de organizaciones y profesionales sanitarios, siempre que se establezcan garantías para la agregación de los datos por organización o profesional y se garantice la no indexación de la información, advirtiendo de prohibición del uso de los datos para otras finalidades.

- El carácter desproporcionado de la exigencia de aportación por los candidatos a cualquier puesto de trabajo en una entidad financiera de los datos relacionados con sus antecedentes penales, dado que la Ley únicamente impone el conocimiento de estas informaciones en determinados supuestos vinculados a la exigencia de requisitos de honorabilidad empresarial y profesional

- La obligación de una compañía de suministro eléctrico de comunicar la información referida a clientes con deudas impagadas a la Administración de una Comunidad Autónoma en virtud de los dispuesto en la legislación de medidas para afrontar la pobreza energética.

- La licitud de la cesión por un Ayuntamiento de determinados datos personales relativos al consumo, puntos de suministro, usuarios de agua conectados al servicio de abastecimiento de agua potable y otra información complementaria a una entidad dependiente del Gobierno autonómico al objeto de poder esta última gestionar un determinado tributo, en virtud de la normativa reguladora del mismo.

- La licitud de la cesión a una corporación municipal de información referida a los apartamentos anunciados en una página web siempre que no sea masiva, de manera que exista una solicitud concreta, específica y en la que resulte motivada su necesidad para el ejercicio de las funciones inspectoras de la Administración turística.

- La improcedencia de la publicación en Internet de los resultados de los sorteos para la configuración de las mesas electorales, conforme al criterio sustentado en este punto por la Junta Electoral Central

- La disconformidad con la LOPD de un modelo de negocio consistente en que una empresa obtuviera del interesado, mediante su consentimiento, la clave de acceso online a su cuenta corriente del propio interesado a fin de comprobar su solvencia patrimonial y posteriormente ceder sus datos a otras entidades financieras en caso de que el interesado quisiera recibir información adicional de una empresa de préstamos o contratar directamente uno, al suponer, entre otras cosas, una vulneración de las medidas de seguridad de la entidad financiera a cuyos sistemas de información se estaría accediendo.

- La licitud de la cesión de datos contenidos en la historia clínica a la inspección de servicios sociales de una Comunidad Autónoma, al encontrarse habilitada en las competencias que la Ley autonómica que regula dicha inspección le atribuye, siempre que se dé cumplimiento al principio de proporcionalidad.

- La condición de encargado del tratamiento de los peritos de parte cuando acceden a la información obrante en los expedientes judiciales que contienen datos de carácter personal

5.2. COLABORACIÓN CON LOS PROFESIONALES DE LA PRIVACIDAD

La Agencia está trabajando en la definición de los criterios o esquemas de acreditación y certificación de los Delegados de Protección de Datos (DPD), llamados a ocupar un papel central en las relaciones de las empresas y los ciudadanos con las autoridades de control. La Agencia apuesta por esta forma de demostrar la cualificación profesional de los DPD en el convencimiento de que promover esquemas de certificación en este ámbito es una opción estratégica con vistas a dotar de seguridad y fiabilidad al sector. Si bien la certificación no será la única vía de acceso a la profesión, ni tampoco será obligatorio utilizar un determinado esquema de certificación, la Agencia está trabajando en diseñar, en colaboración con la ENAC, unos criterios de acreditación de entidades certificadores que garanticen un nivel adecuado de habilidades y competencias en los profesionales que se certifiquen con ellos, y que está previsto que se presenten en el primer semestre de 2017. Esta iniciativa complementa las relaciones que se han descrito en el apartado de Agenda Institucional.

6 EL FUTURO DE LA PROTECCIÓN DE DATOS EN EUROPA

La protección de datos en Europa estará marcada en el futuro por la aplicación de los dos instrumentos normativos, el Reglamento General de Protección de Datos, del que ya se ha hablado en múltiples apartados de esta Memoria, y la Directiva relativa a los tratamientos en el ámbito policial y judicial penal, que configuran el núcleo del marco normativo que reemplazará al definido por la Directiva 95/46 y por la Decisión Marco 2008/977.

Ambos instrumentos entraron en vigor el 24 de mayo de 2016, aunque su aplicación sólo se producirá dos años después de esa fecha, cuando finalice el periodo transitorio fijado para el Reglamento y el plazo de trasposición que se establece para la Directiva.

De estos instrumentos es, sin duda, el Reglamento el que tendrá un mayor alcance e impacto, como consecuencia de su vocación de norma general, aplicable a todas las actividades de tratamiento de datos en el sector privado y a una mayoría de ellas en el ámbito público.

El Reglamento, como repetidamente se ha señalado, se apoya sobre tres ejes principales: mantenimiento y reforzamiento de los principios y derechos centrales del modelo europeo de protección de datos, con el objetivo de conceder a los ciudadanos un mayor control sobre sus datos personales; establecimiento de un enfoque de «responsabilidad activa» para responsables y encargados, según el cual éstos deberán adoptar una serie de medidas encaminadas a garantizar y a poder demostrar que están en condiciones de cumplir con esos principios y derechos; y armonización del sistema de supervisión sobre la base de unas autoridades de protección de datos dotadas de plena independencia y de un conjunto de poderes igual en toda la Unión, incluida la potestad sancionadora. El más claro exponente de este último punto es el establecimiento de un organismo de la Unión, el Comité Europeo de Protección de Datos, que reemplazará al Grupo de Trabajo del Artículo 29 con una misma composición pero con competencias muy ampliadas, entre las que se incluye la de adoptar decisiones jurídicamente vinculantes para las autoridades de supervisión que lo integran en casos en que existan discrepancias entre estas sobre determinadas cuestiones.

Dado que los reglamentos son normas directamente aplicables que, como tales, tienen un efecto directo y producen como resultado una unificación de los derechos nacionales en las materias que regulan, la adopción del Reglamento General de Protección de Datos ha de contribuir a establecer un régimen y unos niveles de protección más homogéneos en todo el territorio de Unión, superando las divergencias derivadas de la diversas opciones elegidas por los Estados Miembros a la hora de trasponer la Directiva del 95.

Sin embargo, el Reglamento contiene diversas habilitaciones, expresas o implícitas, para que los Estados Miembros adopten medidas legislativas que lo complementen o que faciliten su aplicación.

Estas habilitaciones tienen en ocasiones un ámbito establecido de forma muy amplia. Así sucede, por ejemplo, con la posibilidad que el artículo 6.2 del Reglamento concede a los Estados Miembros de mantener o adoptar disposiciones más específicas en todos los aspectos de los tratamientos que se lleven a cabo para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos.

En otros casos, la llamada a la normativa interna se circunscribe a sectores concretos, como ocurre en todos los casos en que, como excepción al criterio general de prohibición, se permite el tratamiento de datos sensibles para ciertas finalidades (atención médica, investigación científica, cumplimiento de las obligaciones del responsable en el ámbito laboral,…) en los términos que determine la legislación de los Estados Miembros.

El Reglamento también les pide expresamente que adopten regulaciones propias en una materia específica. El mejor ejemplo en ese sentido es posiblemente el que se contiene en el artículo 54, donde se exige a los Estados que establezcan en su derecho interno más de diez aspectos sobre las autoridades de supervisión.

Las posibilidades que el Reglamento ofrece a los Estados para regular en su derecho nacional una variedad de materias incluidas en el ámbito de aplicación del Reglamento podría conducir a un escenario en que, a pesar del carácter unificador de los reglamentos como actos jurídicos de la Unión, persistan o se creen algunas diferencias más o menos significativas entre los Estados Miembros.

El derecho de la Unión, con carácter general, y el propio Reglamento, contienen mecanismos para hacer frente a ese potencial riesgo de dispersión. La actuación del Tribunal de Justicia en su interpretación del Derecho de la Unión y en el análisis de la compatibilidad con el mismo de las normas nacionales a través de diversos recursos es uno de estos mecanismos. Los procedimientos de cooperación y coherencia entre autoridades de protección de datos que el Reglamento establece son otro de esos instrumentos para conseguir una aplicación coherente y uniforme del Reglamento.

En todo caso, la Comisión, en su papel de salvaguarda del cumplimiento del derecho de la Unión, tiene la posibilidad de hacer un seguimiento de la aplicación de las normas en los Estados Miembros, de proponer modificaciones en los casos en que estas excedan los márgenes que les concede el derecho de la Unión e, incluso, de plantear recursos por incumplimiento ante el Tribunal de Justicia.

En relación con el Reglamento, la Comisión ha iniciado ya esta tarea de seguimiento en la preparación para la aplicación por parte de los Estados. Para ello, ha constituido un Grupo de Expertos integrado por representantes de los Estados Miembro y dedicado a intercambiar información sobre los problemas que los Estados están encontrando para aplicar determinadas disposiciones del Reglamento en sus ordenamientos así como sobre las soluciones que a nivel nacional se están dando a las habilitaciones que el Reglamento contiene.

Desde el punto de vista interno, en España se ha considerado que la aplicación del Reglamento ha de conllevar una doble operación de adaptación normativa. Se trata, por una parte de preparar una nueva ley orgánica de protección de datos que incorpore todas las regulaciones horizontales que el Reglamento permite a los Estados Miembros, incluyendo, hasta donde ello sea posible, disposiciones ya consolidadas en nuestro derecho a la protección de datos. Esta opción de derogar la vigente Ley Orgánica y sustituirla por una nueva norma se ha entendido que ofrece más seguridad jurídica y una mejor accesibilidad que la alternativa consistente en haber modificado la actual Ley en todos los aspectos en que podía ser afectada por el Reglamento. Particularmente teniendo en cuenta que el derecho de la Unión no permite que las disposiciones de un reglamento sean incorporadas a normas nacionales, salvo casos excepcionales, como el que el Reglamento General contempla, en que ello sea necesario para asegurar la comprensión de las disposiciones en que la norma interna especifique previsiones de la norma europea.

Por otro lado, será preciso revisar toda la normativa sectorial para identificar qué disposiciones se ven afectadas por el Reglamento así como, lo que es igualmente importante, en qué aspectos el Reglamento ofrece posibilidades de mejorar las regulaciones existentes.

La primera de estas tareas fue encomendada por el Ministro de Justicia a la Comisión General de Codificación, y más concretamente a su Sección Tercera, de Derecho Público.

En esta Sección se constituyó una Ponencia con la misión de preparar el texto inicial del borrador de anteproyecto de futura ley orgánica. La Ponencia está integrada por tres vocales natos de la Sección, así como por cuatro vocales pertenecientes a la Agencia Española de Protección de Datos y nombrados al efecto. La Ponencia está presidida por el Presidente de la Sección Tercera.

Aunque el Reglamento sea la principal de las normas en que se plasma el futuro marco europeo de protección de datos, no cabe ignorar la importancia, al menos en algunos Estados Miembro, de la Directiva para el ámbito policial y judicial penal.

En el caso español, la Directiva tiene una significación menor en la medida en que en España la norma general sobre protección de datos, la Ley Orgánica 15/1999, de 13 de diciembre se aplica también a los ficheros y tratamientos desarrollados por las Fuerzas y Cuerpos de Seguridad del Estado, con una serie de excepciones previstas en la propia Ley. Esta situación no es la misma en toda la Unión. Dado que la Directiva 95/46 no resulta de aplicación al entorno policial y judicial penal, algunos Estados Miembros optaron por no extender a ellos sus normas generales de protección de datos y por establecer regímenes específicos no necesariamente basados en los mismos principios que la Directiva establece.

La adopción de la Directiva 680/2016 debe producir una armonización para toda la Unión de las normas sobre los tratamientos realizados en estos ámbitos. Esa armonización se produce sobre la base de unos principios y derechos consistentes con los establecidos en el Reglamento General de Protección de Datos, que opera como norma de referencia, aunque existen diferencias justificadas por las peculiaridades de los tratamientos en el ámbito de la prevención, detección, investigación y enjuiciamiento de los delitos.

No obstante, al tratarse de una Directiva, los Estados Miembros tienen una mayor flexibilidad en la trasposición que la que tienen en la adopción de normas para la aplicación del Reglamento General. Es por ello que, aunque el Grupo de Expertos de la Comisión Europea que antes se mencionaba funciona también en relación con la Directiva, su actividad se ha orientado en una primera fase a buscar un entendimiento común de algunas de las disposiciones en que la Directiva hace una regulación más innovadora o que se separa más de los criterios generales fijados por el Reglamento.

En paralelo con los desarrollos normativos que, en los márgenes permitidos por el Reglamento, se producirán en los Estados Miembros, el futuro inmediato de la protección de datos en la Unión pasa por la efectiva aplicación de sus disposiciones. En la medida en que se trata de una norma que se aplica en toda la Unión y que debe dar lugar a una protección homogénea en todos los Estados Miembro resulta fundamental evitar que existan diferencias significativas en el modo en que sus disposiciones son interpretadas e implementadas en los Estados.

Aunque la interpretación del Derecho de la Unión corresponde a los tribunales nacionales y, en último extremo, al Tribunal de Justicia de la Unión, las autoridades de protección de datos son las encargadas de supervisar la aplicación de las normas sobre protección de datos y, de forma colectiva, en el seno del futuro Comité Europeo de Protección de Datos, de ofrecer directrices, recomendaciones o criterios de buenas prácticas con el fin de promover la aplicación coherente del Reglamento.

Por ello, el Grupo de Trabajo del Artículo 29 decidió dedicar los dos años de periodo transitorio a la doble tarea de establecer criterios comunes para la aplicación de determinadas disposiciones del Reglamento y de preparar la transición desde su actual configuración como foro de cooperación a la propia de un organismo de la Unión con personalidad jurídica propia y competencias reforzadas como es el Comité Europeo de Protección de Datos.

En 2016 el Grupo concluyó tres documentos con directrices para la aplicación de las disposiciones del Reglamento sobre:

- Derecho a la Portabilidad (WP 242)
- Delegado de Protección de Datos (WP 243)
- Identificación de la autoridad principal (WP 244)

Estos tres documentos fueron, después de su aprobación provisional, sometidos a un proceso de consulta pública que finalizó a principios de febrero de 2017. Las contribuciones recibidas en

esa consulta servirán para introducir modificaciones que mejoren el contenido de los textos.

Junto con esos tres documentos, el Grupo adoptó también una serie de herramientas, de uso interno para las autoridades de protección de datos, sobre la aplicación práctica de las disposiciones del Reglamento sobre mecanismos de cooperación, asistencia mutua y operaciones conjuntas. Estas herramientas pretenden ofrecer a las propias autoridades una guía sobre los pasos a dar en cada uno de estos mecanismos, los plazos que en cada caso puedan existir, o los resultados que se esperan de las autoridades intervinientes.

En 2017 el Programa de Trabajo del Grupo tiene previsto que se adopten dictámenes, guías o directrices sobre las materias siguientes:

- Evaluaciones de Impacto.
- Esquemas de certificación.
- Multas administrativas.
- Perfilado.
- Consentimiento.
- Transparencia en la información a los interesados.
- Notificación de violaciones de seguridad de los datos.
- Instrumentos de transferencias internacionales en el Reglamento General.

En el terreno de la preparación para el establecimiento del Comité Europeo de Protección de Datos, el Grupo del Artículo 29 está siguiendo diferentes líneas de trabajo.

Por una parte, está preparando la infraestructura necesaria para asegurar que puede desarrollar su actividad desde el primer día de su constitución formal. El Secretariado del Comité será asumido, de acuerdo con el Reglamento, por el Supervisor Europeo de Protección de Datos. Por ello, el Grupo del Artículo 29 está trabajando conjuntamente con el Supervisor en la identificación de las necesidades de personal y presupuestarias, así como en los métodos para asegurar que estos recursos están disponibles en mayo de 2018.

Especial importancia en esta línea tiene el diseño y puesta en funcionamiento del sistema de información del Comité. El Reglamento establece, como se ha indicado, mecanismos de asistencia mutua, cooperación y coherencia que requieren de un fluido intercambio de información entre las autoridades y entre éstas y el Comité. Ese intercambio no sería eficaz sin un sistema que lo haga posible de una forma rápida, sencilla y segura. En esta materia el análisis de necesidades y el diseño preliminar han sido asumidos por un grupo de trabajo integrado por la presidencia del Grupo y el Supervisor Europeo.

En otro orden de cosas, el Grupo del Artículo 29 está redactando el Reglamento de Régimen Interior del Comité, que deberá ser aprobado por este tan pronto como comience a funcionar. Este Reglamento tiene especial importancia como consecuencia del hecho de que el Comité está llamado a desempeñar un papel clave en la configuración de las futuras políticas de protección de datos en la Unión Europea.

Como ya se ha indicado, el Comité hereda las funciones del Grupo del Artículo 29, ampliadas a una larga lista de materias en que el Reglamento le atribuye expresamente tareas de elaboración de recomendaciones o guías de actuación. Al mismo tiempo, recibe competencias para adoptar decisiones con una mayores consecuencias jurídicas, como son las de adoptar dictámenes en relación con una serie de decisiones que corresponde adoptar a las autoridades nacionales pero que tienen efectos sobre la libre circulación de datos en el conjunto de la Unión. Estos dictámenes no son jurídicamente vinculantes, pero si las autoridades afectadas se separan de ellos podrán ser reformulados como decisiones de contenido vinculante.

Estas últimas son las que más claramente justifican el establecimiento del Comité como organismo de la Unión con personalidad jurídica propia. El Comité podrá emitirlas siempre que sea necesario para resolver las diferencias entre autoridades

en materias relacionadas con los procedimientos de cooperación.

Estos procedimientos remiten a otra de las características que van a definir la protección de datos en el futuro.

El Reglamento establece unos mecanismos de cooperación articulados sobre el criterio de la «ventanilla única», según el cual cuando un responsable o encargado tiene establecimientos en varios Estados Miembros o realiza tratamientos que afectan significativamente a personas en varios Estados Miembros, todas las autoridades de esos Estados han de poder participar en las decisiones relacionadas con la supervisión de las actividades de esos responsables o encargados, con la autoridad del Estado donde se localice el «establecimiento principal» como autoridad líder con unas funciones específicas de coordinación y preparación de la decisión.

Este sistema, a pesar de la simplicidad que parece derivarse del hecho de que sea una autoridad la principal responsable de la gestión de los procedimientos de alcance transfronterizo, va a plantear importantes retos desde un punto de vista práctico.

El primero de ellos es el de identificar dónde se ubica el establecimiento principal de una organización y, consecuentemente, quién es la autoridad que ha de liderar la supervisión de esa organización. El GT29 ha elaborado, como se ha indicado anteriormente, unas directrices para ayudar a empresas y autoridades en esta tarea. Sin embargo, ello no impedirá que, en la realidad cotidiana del trabajo de las autoridades, a las funciones de supervisión deba añadirse, como primera medida, y en el momento de recibir una reclamación o de iniciar de oficio un procedimiento de investigación, la realización de las gestiones necesarias para establecer el carácter transfronterizo de los tratamientos afectados, qué otras autoridades pueden considerarse afectadas y cuál de ellas deberá asumir el rol de autoridad principal.

Adicionalmente, deberán también evaluar si el caso concreto, pese a enmarcarse en un tratamiento transfronterizo, tiene una relevancia puramente local, ya que entonces es la autoridad que ha recibido la reclamación o que decide iniciar una investigación la que será competente para tratar el caso, siempre que la autoridad principal, que siempre ha de haber sido identificada previamente, no decida canalizarlo a través del mecanismo general de ventanilla única.

Aunque en las grandes empresas, o en organizaciones que se relacionen frecuentemente con las autoridades de control, la identificación de la autoridad principal será relativamente sencilla una vez que se hayan abordado los primeros casos, no puede olvidarse que el sistema afecta a todas las organizaciones con más de un establecimiento en la Unión, o cuyos tratamientos afecten a personas en más de un Estado Miembro.

Por otro lado, la autoridad líder, una vez identificada, debe preparar la decisión sobre el caso en contacto con las demás autoridades afectadas y debe conseguir el acuerdo de todas ellas. En caso de que una o varias planteen «objeciones razonadas y pertinentes» a la propuesta de resolución de la autoridad principal, ésta debe modificar su propuesta y someterla de nuevo a la consideración de las afectadas o, si no ve posible una solución aceptable por todas ellas, remitir el caso al Comité Europeo de Protección de Datos. De nuevo es preciso tener en cuenta que cuando se alude a las «autoridades afectadas» puede estarse hablando de cifras que oscilan entre dos o tres, para las organizaciones con una muy limitada actividad transfronteriza, y veintiocho, para las grandes empresas, de internet o de otros sectores, con presencia o actividad en toda la Unión Europea.

Es en este proceso de adopción de decisiones consensuadas donde radican los principales elementos de complejidad del sistema. Los plazos previstos por el Reglamento no siempre son compatibles con los que a nivel nacional establece las normas generales sobre procedimientos administrativos y, a la vez, éstas no son necesariamente consistentes entre sí. Trámites esenciales del procedimiento, como puede ser la audiencia a los interesados, se ubican en diferentes momentos del proceso según la normativa nacional que se considere. Principios como el de la separación entre quien instruye el

procedimiento y quien adopta la decisión pueden resultar difíciles de adaptar a los intercambios de propuestas de decisión y a la necesidad de valorar y, en su caso, admitir, posibles objeciones que el Reglamento prevé.

Todos estos factores afectarán de forma significativa a la duración de los procedimientos y requerirán modificaciones tanto en las normas nacionales como en la estructura y dinámica de trabajo de las autoridades de supervisión.

En este sentido, hay una cuestión que, aunque siempre estuvo presente durante los debates de que el sistema de ventanilla única fue objeto durante la negociación del Reglamento, solo ahora está recibiendo la atención que merece. Se trata del idioma de los procedimientos.

Todas las legislaciones nacionales exigen que los procedimientos que se desarrollen por las autoridades públicas de un Estado Miembro utilicen la lengua o lenguas oficiales de ese Estado. Sin embargo, el mecanismo de ventanilla única implica que las autoridades afectadas tendrán que comunicarse entre sí facilitándose información y documentación.

Este intercambio de información puede hacerse remitiendo los documentos en la lengua en que fueron elaborados, y dejando a la responsabilidad de las autoridades receptoras la traducción a su propio idioma, o previa traducción de todos los documentos a una lengua accesible para todas las autoridades concernidas.

Por ello otro reto para las autoridades de supervisión será el de asumir que un idioma no oficial, casi sin duda el inglés, pasará a convertirse en lengua vehicular de un porcentaje significativo de los procedimientos que desarrollen y que deberán contar con personal capaz de trabajar en ese idioma.

El sistema, como se puede apreciar, es complejo, su principal consecuencia es que las tareas de supervisión de las autoridades de cada Estado Miembro han de ser consistentes con las de todos los demás, tanto en los procedimientos como en los contenidos de las decisiones. En ese sentido es importante destacar no sólo los efectos de esos mecanismos de cooperación sino, también, las consecuencias del papel que la doctrina que vaya elaborando el Comité a través de sus dictámenes, recomendaciones o directrices tendrá sobre las decisiones que adopten individualmente las autoridades nacionales. En un contexto en que todas las decisiones pueden, por una vía u otra, ser objeto de revisión a la luz de esos criterios comunes, es difícil que las autoridades puedan separarse sustancialmente de ellos en sus decisiones, aun cuando estas no se enmarquen formalmente en procedimientos de cooperación.

El escenario de los próximos años se configura, por tanto, sobre la base de unas normas comunes para todo el territorio de la Unión, con especial protagonismo del Reglamento, que determinan una continuación del modelo europeo de protección de datos con un reforzamiento tanto del control que los ciudadanos pueden ejercer sobre sus datos como de la vertiente preventiva como, por fin, de los poderes de las autoridades de supervisión.

La aplicación de esas normas puede tener variaciones en los diferentes Estados Miembros, pero el sistema acentúa la dimensión europea en todos los mecanismos de supervisión en busca de la máxima coherencia en las decisiones y de un nivel uniforme de protección.

7 NUEVOS DESAFÍOS PARA LA PRIVACIDAD

7.1. WHATSAPP

Ante los cambios en la política de privacidad y los términos de servicio de WhatsApp que se produjeron el 25 de agosto de 2016, en los que dicha entidad solicitaba el consentimiento de los usuarios para realizar comunicaciones de datos a la empresa Facebook, la Agencia Española de Protección de Datos publicó en su página web información sobre dichos cambios, ofreciendo indicaciones a los ciudadanos sobre los elementos más determinantes de los mismos.

A consecuencia de este estudio preliminar, la AEPD decidió abrir actuaciones de investigación de oficio para determinar el modelo general de tratamiento, la extensión de los datos transferidos, el ámbito de procesamiento y la base jurídica de la comunicación de datos, aspectos en los que están implicadas tanto la empresa WhatsApp como Facebook.

Con la iniciativa de la AEPD, en el marco de las actuaciones coordinadas de las Autoridades de Protección de Datos Europeas se remitió a WhatsApp una carta por parte de la presidenta del Grupo de Trabajo del Artículo 29 en nombre de dichas autoridades, que tuvo como consecuencia inmediata la paralización de la comunicación de datos anunciada en los cambios de la política de privacidad, al menos en el ámbito de la Unión Europea. Además, la AEPD ha activado el Subgrupo Cumplimiento dentro del Grupo del Artículo 29 para coordinar las actuaciones de sus miembros respecto sobre la nueva política de privacidad y términos de uso de WhatsApp.

7.2. FACEBOOK

Aparte de las actuaciones descritas en el apartado anterior, y de las investigaciones llevadas a cabo en relación a denuncias o reclamaciones presentadas por los ciudadanos, la AEPD está realizando una supervisión de los tratamientos de datos de los usuarios de Facebook en el marco de una actuación coordinada entre autoridades europeas, en un Grupo de Contacto formado por España, Francia, Bélgica, Holanda, y la autoridad alemana de Hamburgo.

A raíz de las acciones iniciadas se instó a Facebook a realizar una serie de cambios en relación al tratamiento de datos personales. En mayo de 2016, dicha compañía procedió a realizar algunas modificaciones, ampliando su sistema de información sobre cookies y añadiendo controles sobre la publicidad para usuarios de la red social. No obstante, las acciones de la AEPD han continuado evaluando la información proporcionada a los usuarios y los tratamientos de Facebook para determinar si dichos cambios son suficientes para garantizar un adecuado cumplimiento.

7.3. ESCUDO DE PRIVACIDAD (PRIVACY SHIELD)

El 12 de julio de 2016 la Comisión Europea aprobó mediante una Decisión de Ejecución sobre la adecuación de la protección conferida por el Escudo de Privacidad UE-EEUU (Privacy Shield, en su denominación en inglés), que sustituía a la Decisión 2000/520/CE, conocida como Decisión de Puerto Seguro, declarada inválida por sentencia del Tribunal de Justicia de la Unión Europea de 6 de octubre de 2015 (Sentencia Schrems). La Sentencia dio lugar a que la Agencia informase de sus consecuencias a un total de 1.656 responsables de ficheros domiciliados en España que habían notificado transferencias a entidades adheridas al sistema de Puerto Seguro y les solicitase información acerca de sus previsiones al respecto, solicitud que se reiteró a 560 responsables en marzo de 2016.

La adopción del Escudo de la Privacidad se producía tras un rápido proceso de negociación entre la Comisión Europea y los representantes de la Administración estadounidense encaminados a conseguir que esta última ofreciera unas garantías suficientes para responder a las insuficiencias que el Tribunal de Justicia había detectado en el marco del esquema de Puerto Seguro.

El nuevo Escudo de Privacidad tiene como objetivo primordial, como ya sucedía con el sistema de Puerto Seguro, permitir las transferencias de datos de un responsable o encargado del tratamiento en la Unión a organizaciones de los Estados Unidos que hayan auto-certificado su adhesión a los principios del Escudo de Privacidad ante el Departamento de Comercio y se hayan comprometido a atenerse a ellos. La protección que el Escudo de Privacidad confiere a los datos personales se aplica a cualquier interesado en la UE cuyos datos hayan sido transferidos desde la Unión a organizaciones en los Estados Unidos que hayan auto-certificado su adhesión a los citados principios.

Un primer acuerdo entre las partes europea y norteamericana se alcanzó a principios de febrero de 2016 y se recogió en una primera propuesta de decisión de la Comisión, integrada por el texto de la decisión propiamente dicho y por una serie de Anexos en los que figuraban los Principios del Escudo de Privacidad y los compromisos asumidos por las autoridades norteamericanas.

La propuesta de decisión fue objeto de un dictamen del Grupo de Trabajo del Artículo 29 (Dictamen 1/2016 – WP238), en que el Grupo analizaba tanto la parte del acuerdo relativa a sus aspectos puramente comerciales como las garantías ofrecidas por la Administración estadounidense en lo tocante al acceso de las autoridades a los datos por razones de seguridad nacional.

En su dictamen, el Grupo acogía favorablemente con carácter general las mejoras que la propuesta de decisión de la Comisión contenía en relación con el Puerto Seguro. Sin embargo, también identificaba una serie de materias en las que entendía que el Escudo de Privacidad no reflejaba de forma adecuada algunos de los principios clave del derecho europeo a la protección de datos. En este sentido, el Grupo recordaba que la propuesta de decisión de la Comisión declara como adecuado el nivel de protección ofrecido en el contexto del esquema y que, según la doctrina del Tribunal de Justicia en la Sentencia Schrems, ese nivel adecuado debe traducirse en que los datos sean objeto de una protección «esencialmente equivalente» a la que reciben en la Unión Europea.

Entre los problemas identificados por el Grupo se encontraba el que la propuesta decisión de la Comisión no incluía referencias al principio de conservación de los datos por el tiempo imprescindible para alcanzar los fines que justifican su tratamiento. Adicionalmente, tampoco se incluía ninguna referencia a las salvaguardas necesarias para las decisiones automatizadas basadas en perfiles.

En el terreno del acceso a los datos por parte de los servicios de inteligencia como consecuencia de una de las excepciones a la aplicación de los principios del Escudo de Privacidad, el GT29 consideraba positivo que estas cuestiones fueran objeto

de un tratamiento extenso y detallado, a diferencia de lo que sucedía en el caso del Puerto Seguro.

Pese a ello, también entendía que el esquema no contenía un mecanismo de reparación suficiente. El Escudo de Privacidad contempla la creación de un Ombudsperson, figura que será desempeñada por un alto funcionario del Departamento de Estado, que deberá investigar y dar respuesta a las reclamaciones presentadas por los interesados en todo lo relativo al uso que las autoridades norteamericanas puedan hacer de sus datos cuando el acceso a ellos se produce por razones de seguridad nacional. A juicio del Grupo, esa nueva figura, que sin duda constituye un avance muy significativo, plantearía dudas sobre si puede ser considerada formal y total independiente.

Además, el Grupo consideraba que la posibilidad, reconocida en los anexos que acompañaban a la propuesta de decisión, de que los servicios de inteligencia americanos accedan a los datos transferidos de forma masiva e indiscriminada («bulk access») no es compatible con los criterios de proporcionalidad que también se desprenden de la jurisprudencia europea y que se incluyen como una de las «Garantías Esenciales Europeas» que el propio Grupo había identificado en un documento adoptado a principios de 2016 (Working Document 1/2016 – WP237).

Este dictamen tuvo gran repercusión y, de hecho, junto con una primera reacción también negativa de los Estados Miembros en el Comité del artículo 31, motivó que se reabrieran las negociaciones entre EEUU y la Comisión con el fin de dar solución a los principales problemas identificados.

Aunque el texto que finalmente fue adoptado, tras la opinión favorable del Comité del artículo 31, incorpora esas soluciones, el Grupo del Artículo 29, en una Declaración hecha pública el 26 de julio de 2016, se felicitaba por las mejoras del esquema del Escudo de Privacidad frente al de Puerto Seguro, a la vez que manifestaba que subsisten algunos motivos de preocupación.

Más concretamente, el Grupo lamentaba que no haya en la Decisión reglas específicas sobre decisiones automatizadas, algo que ya había mencionado en su anterior Dictamen, así como que no exista un derecho de oposición formulado de manera general.

En el terreno del acceso por parte de las autoridades por motivos de seguridad nacional, el Grupo señalaba que habría sido deseable que se ofrecieran garantías más estrictas sobre la independencia y poderes del «Ombudsperson», y lamentaba la falta de garantías concretas que permitan asegurar que el compromiso de las autoridades norteamericanas de no llevar a cabo una recogida masiva e indiscriminada de datos personales se cumple en todos los casos.

Por todo ello, el Grupo entiende que la primera revisión anual conjunta deberá ser la ocasión para valorar la robustez y eficacia de los mecanismos del Escudo de Privacidad. En este sentido, el Grupo señala algunos requisitos sobre esta revisión, en especial en lo relativo al papel y facultades de las autoridades de protección de datos europeas que participen en ella.

Tras la adopción definitiva de la Decisión, y a partir del 1 de agosto de 2016, las empresas pudieron certificarse en el Departamento de Comercio, que procedió a incorporarlas a un nuevo directorio disponible a estos efectos y que sustituye al anterior directorio de Puerto Seguro.

Poco después de la publicación de la Decisión del Escudo de Privacidad, la Comisión Europea publicó una Guía sobre el mismo, orientada a los ciudadanos, que la Agencia Española de Protección de Datos publicó en español en su página web. En esta Guía se describen las obligaciones de las empresas sujetas al Escudo de Privacidad y los derechos de los ciudadanos con respecto al uso de sus datos personales, la forma de presentar una queja contra una empresa sujeta al Escudo de Privacidad, así como contra una autoridad pública estadounidense a través de la figura del «Ombudsperson».

Desde la publicación de la Decisión relativa al Escudo de Privacidad, el Grupo de Trabajo del Artículo 29 ha continuado trabajando en la elaboración de materiales que faciliten la presentación de

quejas, tanto en el ámbito comercial como ante el «Ombusperson», a las autoridades de protección de datos de la UE.

Para ello se han elaborado formularios que pueden ser utilizados de forma opcional y que estarán disponibles en las páginas web de todas las autoridades de control de Unión. Además, se ha establecido el «Panel informal de autoridades de protección de datos de la UE», como grupo de autoridades de protección de datos de los Estados Miembros, con el fin de gestionar las quejas relacionadas con datos personales de recursos humanos transferidos desde una entidad de la UE a una empresa estadounidense certificada en el Escudo de Privacidad o transferidos a empresas estadounidenses que se hayan comprometido voluntariamente a cooperar con las autoridades de protección de datos de la UE.

Como consecuencia de la indisponibilidad, durante buena parte de 2016, de un sistema que propiciase garantías adecuadas para la transferencia de datos a Estados Unidos, se produjo un importante incremento de las solicitudes de autorización a dicho destino basadas en las garantías que proporcionan las cláusulas contractuales tipo aprobadas por la Comisión Europea, recibiéndose 404 solicitudes durante 2016, frente a las 50 que se registraron en 2015.

Tras la entrada en vigor de la Decisión de la Comisión, esta tendencia cambió y las entidades exportadoras establecidas en España comenzaron también a notificar las transferencias internacionales a EEUU al amparo de Escudo de Privacidad. Ello ha dado lugar a que durante el último trimestre del pasado año 188 responsables de tratamientos de datos notificasen 368 inscripciones de ficheros en el Registro General de Protección de Datos con referencias a este tipo de transferencia. Además, fuera del ámbito temporal de esta memoria, cabe señalar que, sólo en los dos primeros meses de 2017, el Escudo de Privacidad ha sido utilizado por 200 responsables que han notificado 416 ficheros.

8 UNA AGENCIA QUE DÉ RESPUESTA A LOS RETOS INTERNACIONALES

8.1. COOPERACIÓN CON IBEROAMÉRICA. LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS (RIPD)

Durante 2016 las actuaciones más significativas de la Agencia Española de Protección de Datos, en su condición de Secretaría Permanente de la Red Iberoamericana de Protección de Datos (RIPD), han sido las siguientes:

- **XIV Encuentro Iberoamericano de Protección de Datos. 8, 9 y 10 junio. Santa Marta, Colombia.**

El evento se organizó conjuntamente entre la RIPD y la Superintendencia de Industria y Comercio de Colombia, en el marco del IV Congreso Internacional de Protección de Datos Personales, y contó en su Sesión Abierta con una participación superior a los cuatrocientos asistentes, entre representantes de las autoridades iberoamericanas de protección de datos, sectores privados y empresariales, universidad, expertos y profesionales de la privacidad de Iberoamérica, así como de Estados Unidos, Canadá y Europa.

A través de sus diferentes paneles y conferencias, se abordaron cuestiones como la privacidad y la seguridad; la protección de datos de niños y adolescentes; el internet de las cosas; el tratamiento de datos en las redes sociales, o la relación entre la protección de datos y el derecho de la competencia. Las ponencias del Encuentro pueden consultarse en la página web de la RIPD, en la sección de «Actividades/Encuentros/XIV Encuentro».

- **Taller «Privacidad y Acción Internacional Humanitaria». 16 y 17 de junio. Centro de la Cooperación Española en La Antigua, Guatemala.**

Con esta actividad se ha pretendido promover el intercambio de experiencias y transferencia de conocimientos entre las autoridades de protección de datos, expertos y representantes de organizaciones internacionales humanitarias, a fin de desarrollar el mandato dado por la 37.ª Conferencia Internacional de Autoridades de Protección de Datos y de Privacidad, para la creación de un grupo de trabajo en el seno de dicha Conferencia, integrado por representantes de las redes iberoamericana y francófona de protección de datos (RIPD y AFAPDP), para analizar los requisitos de protección de datos en la Acción Humanitaria Internacional (AHI) y cooperar con las partes interesadas en este ámbito.

Dicho evento contó con la participación de 10 entidades integrantes de la RIPD, de la OEA y representantes de organizaciones internacionales humanitarias (Cruz Roja Internacional, Federación Internacional de la Cruz Roja, Equipos Médicos de Emergencias, etc.)

Durante los dos días del taller se debatió sobre cuestiones como las bases para el tratamiento de datos personales por los agentes de acción internacional humanitaria; los derechos de los beneficiarios de la acción internacional humanitaria y garantías en el tratamiento de los datos; las comunicaciones de datos en el contexto de la acción internacional humanitaria y su dimensión transnacional, o el impacto de las nuevas tecnologías

en el tratamiento de los datos personales en el contexto de la acción internacional humanitaria.

Para una información más detallada del evento, se puede consultar la sección «Actividades» de la web de la RIPD.

- **Seminario: «Europa-Iberoamérica: una visión común de la protección de datos. El nuevo marco europeo y su incidencia en Iberoamérica». Centro de la Cooperación Española en Montevideo. 8 y 9 de noviembre.**

En dicha reunión se debatió sobre las eventuales repercusiones del nuevo Reglamento General de Protección de Datos y de otras iniciativas europeas («derecho al olvido», Privacy Shield, etc.) en la legislación iberoamericana de protección de datos, cuyos fundamentos están fuertemente inspirados en el llamado «modelo europeo» de protección de datos.

Se abordaron asimismo cuestiones esenciales para el futuro de la RIPD, como el documento estratégico «RIPD 2020», con propuestas de reformas programáticas y organizativas, o el proyecto de «estándares iberoamericanos de protección de datos», orientados a servir de referencia a las normas nacionales que se hayan aprobado o vayan a aprobarse en el futuro en la región. Asimismo, se acordó la elección de la Presidencia y del Comité Ejecutivo de la Red para el período 2017-2018.

La RIPD ha obtenido el respaldo de la XXV Cumbre Iberoamericana de Jefes de Estado y de Gobierno en cuya Declaración Final se acuerda «Encargar a la SEGIB solicitar a la Red Iberoamericana de Protección de Datos elaborar una propuesta de trabajo para facilitar la cooperación efectiva para atender cuestiones relacionadas con la protección de los datos personales y de privacidad».

8.2. CONSEJO DE EUROPA

Dentro de la reforma del marco de protección de datos en el ámbito internacional reviste especial importancia el trabajo desarrollado desde el año 2011 por el Consejo de Europa para la adopción de un Protocolo de Modernización del Convenio 108 que, en la práctica, venga a reemplazar el régimen contenido en el Convenio por otro más detallado y cercano a los estándares de nuestro entorno.

La importancia de este proceso resulta evidente, teniendo en cuenta que el Convenio 108 ha sido ratificado por todos los Estados Miembros del Consejo de Europa y que se encuentra abierto a la ratificación de Estados no Miembros (en la actualidad ya ha sido ratificado por Uruguay, Mauricio y Senegal) y se encuentra en proceso de firma y ratificación por otros cuatro Estados. Quiere ello decir que se trataría del único Tratado Internacional vinculante para sus signatarios en relación con el derecho fundamental a la protección de datos. De este modo, constituye una herramienta esencial para que la aplicación de los principios se extienda más allá de los límites de la Unión Europea.

Como ya se indicó en la Memoria 2015, el Comité ad hoc establecido para estudiar la propuesta técnica elaborada por el Comité del Convenio 108 (T-PD) elevó al Grupo de Relatores Jurídicos un texto en que, no obstante, se incluían reservas formuladas, fundamentalmente, por la Unión Europea, respecto de la cual los Estados Miembros había otorgado un mandato negociador a la Comisión Europea, y la Federación Rusa. Las reservas formuladas por la Unión Europea se centraban, básicamente, en la necesidad de uniformar el marco regulador del Convenio y el resultante de la reforma del acervo de la Unión en esta materia.

El Grupo de Relatores Jurídicos propuso otorgar un nuevo mandato negociador al Comité ad hoc a fin de tratar de superar las reservas planteadas, una vez aprobada la reforma del marco de protección de datos en la Unión Europea. De este modo, los días 15 y 16 de junio de 2016 tuvo lugar una nueva reunión del Comité ad hoc en que se adop-

tó un texto en que se levantaron las reservas formuladas por la Unión y alguna de las que había formulado la Federación Rusa. El Comité resolvió la elevación del texto resultante junto con una extensa memoria Explicativa, al Grupo de Relatores Jurídicos para la adopción del nuevo Protocolo adicional al Convenio 108.

Al tiempo de conclusión de esta Memoria el Convenio está siendo objeto de estudio por el citado Grupo, siendo ya pocas las cuestiones pendientes de resolución, por lo que es de esperar que el proceso concluya en el corto plazo.

MEMORIA **AEPD**

2016

LA AGENCIA EN CIFRAS

ACTIVIDAD GLOBAL

RESUMEN DE ACTIVIDAD GLOBAL

El desglose de estas y otras actividades se detalla en páginas posteriores de esta sección.

	2015	2016	Δ% 2015-2016
Denuncias y reclamaciones que han tenido entrada durante el ejercicio	10.571	10.523	–0,45
Actuaciones del Plan Estratégico ejecutadas o puestas en marcha*	2	74	3600
Consultas Gabinete Jurídico - sectores público y privado	485	387	–20,21
Consultas atendidas Atención al ciudadano	218.335	236.955	8,53
Visitas recibidas en la web	4.952.945	5.534.282	11,74
Consultas especializadas sobre tratamiento de datos de menores**	103	696	575,73
Registro de entrada y salida de documentos	835.500	803.278	–3,86
Operaciones de inscripción de ficheros	591.262	661.137	11,82
Solicitudes de autorización de transferencia internacional de datos presentadas	128	737	475,78
Autorizaciones de transferencia internacional de datos concedidas	108	499	362,04

** El Plan Estratégico se presentó en noviembre de 2015.
***El canal especializado se puso en marcha en octubre de 2015.

PLAN ESTRATÉGICO

BALANCE DE CUMPLIMIENTO

ACTUACIONES PREVISTAS EN EL CRONOGRAMA INICIAL PARA 2015	
Acciones anuales o no continuas*	2
TOTAL	**2**
ACTUACIONES QUE SE HAN EJECUTADO O SE HA INICIADO SU EJECUCIÓN EN 2015	
Acciones anuales o no continuas ejecutadas	2
TOTAL	**2**
Grado de cumplimiento del Plan 2015	**100%**
ACTUACIONES PREVISTAS EN EL CRONOGRAMA INICIAL PARA 2016	
Acciones anuales o no continuas*	30
Acciones plurianuales o continuas**	54
TOTAL	**84**
ACTUACIONES QUE SE HAN EJECUTADO O SE HA INICIADO SU EJECUCIÓN EN 2016	
Acciones anuales o no continuas ejecutadas	20
Acciones plurianuales o continuas en ejecución	54
TOTAL	**74**
Grado de cumplimiento del Plan 2016	**88%**

NSPECCIÓN DE DATOS

DATOS GLOBALES

DENUNCIAS Y RECLAMACIONES EN TRAMITACIÓN AL ACABAR EL EJERCICIO

AÑO	2014	2015	2016	% RELATIVO	Δ% 2015/2016	Δ% 2014/2016
Reclamaciones de tutela	385	439	**476**	14,28	8,42	23,64
Denuncias	5.016	2.634	**2.563**	85,71	–2,69	–48,90
TOTAL	**5.401**	**3.073**	**3.039**	**100,00**	**–1,10**	**–43,73**

DENUNCIAS Y RECLAMACIONES QUE HAN TENIDO ENTRADA DURANTE EL EJERCICIO

AÑO	2014	2015	2016	% RELATIVO	Δ% 2015/2016	Δ% 2014/2016
Reclamaciones de tutela	2.099	2.082	**2.588**	24,59	24,30	23,30
Denuncias	10.074	8.489	**7.935**	75,41	–6,53	–21,23
TOTAL	**12.173**	**10.571**	**10.523**	**100,00**	**–0,45**	**–13,55**

DENUNCIAS Y RECLAMACIONES RESUELTAS

AÑO	2014	2015	2016	% RELATIVO	Δ% 2015/2016	Δ% 2014/2016
Reclamaciones de tutela	1.818	2.113	**2.471**	23,34	14,49	35,92
Denuncias	9.404	10.871	**8.112**	76,65	–25,37	–13,74
TOTAL	**11.222**	**12.984**	**10.583**	**100,00**	**–18,49**	**–5,69**

RESOLUCIONES – EJERCICIO DE LA POTESTAD SANCIONADORA

El número de denuncias tramitadas no tiene que coincidir necesariamente con las resoluciones firmadas: varias denuncias referidas a un mismo denunciado pueden agruparse, y paralelamente en una denuncia pueden aparecer múltiples denunciados dando origen a múltiples procedimientos sancionadores.

	AÑO	2014	2015	2016	% RELATIVO	Δ% 2015/2016	Δ% 2014/2016
TIPO DE PROCEDIMIENTO	Archivo de actuaciones tras no subsanarse denuncia	467	691	949	32,10	37,30	103,21
	Archivo de actuaciones de investigación	1157	1040	883	29,90	–15,10	–23,68
	Resolución de procedimientos de apercibimiento	315	397	492	16,70	23,90	56,19
	Resolución de procedimientos sancionadores	752	693	573	19,40	–17,30	–23,80
	Resolución de procedimientos de infracción de las AAPP	60	65	56	1,90	–13,80	–6,67
	TOTAL	**2.751**	**2.886**	**2.953**	**100,00**	**2,30**	**7,34**

AÑO	2014	2015	2016	Δ% 2015/2016	Δ% 2014/2016
Inadmisión a trámite de denuncias sin actuaciones de investigación	5.692	6.049	**4.681**	–22,60	–17,76

RESOLUCIONES – TUTELA DE DERECHOS

AÑO	2014	2015	2016	% RELATIVO	Δ% 2015/2016	Δ% 2014/2016
Estimatoria	391	468	371	34,54	–20,73	–5,12
Estimatoria formal o parcial	309	252	270	25,14	7,14	–12,62
Desestimatoria	261	347	433	40,32	24,78	65,90
TOTAL	**961**	**1.067**	**1.074**	**100,00**	**0,66**	**11,76**

AÑO	2014	2015	2016	Δ% 2015/2016	Δ% 2014/2016
Inadmisión o desistimiento de reclamaciones de tutela	907	1.097	**1.538**	40,20	69,57

EFICACIA ADMINISTRATIVA

Se reflejan tiempos medios de tramitación (en días) desde que se registra la denuncia o se abren actuaciones de oficio hasta que se dicta resolución.

	AÑO	2014	2015	2016	Δ% 2015/2016	Δ% 2014/2016
TIPO DE PROCEDIMIENTO	Archivo de denuncia sin actuaciones de investigación	100	106	64	–40,02	–36,00
	Archivo de actuaciones tras no subsanarse denuncia	174	179	83	–53,73	–52,30
	Archivo de actuaciones de investigación	361	372	323	–13,18	–10,53
	Resolución de procedimientos de apercibimiento	392	386	267	–30,92	–31,89
	Resolución de procedimientos sancionadores	490	507	507	0,04	3,47
	Resolución de procedimientos de infracción de las AAPP	477	522	477	–8,56	0,00
	Resolución de procedimientos de tutela de derechos	116	136	120	–11,88	3,45

EXPEDIENTES INICIADOS DURANTE EL EJERCICIO

AÑO	2014	2015	2016	Δ% 2015/2016	Δ% 2014/2016
Expedientes iniciados	2.199	2.293	**2.826**	23,24	28,51

SECTOR PRIVADO

En este apartado se detallan cifras sobre infracciones declaradas en resoluciones de procedimientos sancionadores y de apercibimiento, pudiendo haberse declarado más de una infracción en cada uno de ellos.

NÚMERO DE INFRACCIONES SEGÚN LEY INFRINGIDA

AÑO	2014	2015	2016	% RELATIVO	Δ% 2015/2016	Δ% 2014/2016
LOPD	896	782	**1.174**	90,17	50,13	31,03
LSSI	95	100	**117**	8,99	17,00	23,16
LGT	6	13	**11**	0,84	–15,38	83,33
TOTAL	**997**	**895**	**1.302**	**100,00**	**45,59**	**30,59**

NÚMERO DE INFRACCIONES SEGÚN GRAVEDAD

AÑO	2014	2015	2016	% RELATIVO	Δ% 2015/2016	Δ% 2014/2016
MUY GRAVE	2	3	**2**	0,15	–33,33	0,00
GRAVE	846	759	**1.095**	84,10	44,27	29,43
LEVE	149	133	**205**	15,75	54,14	37,58
TOTAL	**997**	**895**	**1.302**	**100,00**	**45,47**	**30,59**

APLICACIÓN DE CRITERIOS DE GRADUACIÓN EN LA DECLARACIÓN DE INFRACCIONES

AÑO	2014	2015				2016				%	Δ%	Δ%
	TOT.	LOPD	LSSI	LGT	TOTAL	LOPD	LSSI	LGT	TOTAL	RELATIVO	2015/2016	2014/2016
Apercibimiento	221	163	24	0	187	**461**	**29**	**0**	**490**	37,63	162,03	121,72
Sanción por la escala de gravedad precedente	442	464	13	0	477	**248**	**7**	**0**	**255**	19,59	–46,54	–42,31
Sanción sin atenuación	334	155	63	13	231	**465**	**81**	**11**	**557**	42,78	141,13	66,77
TOTAL	**997**	**782**	**100**	**13**	**895**	**1.174**	**117**	**11**	**1.302**	**100,00**	**45,57**	**30,59**

EVOLUCIÓN DE LAS INFRACCIONES CON SANCIÓN ECONÓMICA

AÑO	2014	2015	2016	Δ% 2015/2016	Δ% 2014/2016
Total sanciones	776	708	**560**	–20,90	–27,84

SECTOR PÚBLICO

PROCEDIMIENTOS DE INFRACCIÓN RESUELTOS

AÑO	2014	2015	2016	% RELATIVO	Δ% 2015/2016	Δ% 2014/2016
Local	32	38	**23**	41	–39,47	–28,13
Autonómica	12	25	**20**	36	–20,00	66,67
General del Estado	14	12	**10**	18	–16,67	–28,57
Otras Entidades de Derecho Público	2	3	**3**	5	0,00	50,00
TOTAL	**60**	**78**	**56**	**100**	**–28,21**	**–6,67**

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

ÁREAS DE ACTIVIDAD

DISTRIBUCIÓN DE LAS ACTUACIONES PREVIAS INICIADAS*

AÑO	2014	2015	2016	% RELATIVO	Δ% 2015/2016	Δ% 2014/2016
Ficheros de morosidad			**1.313**	18,65		
Videovigilancia	966	1.157	**1.036**	14,72	–10,46	7,25
Entidades financieras	1.540	1.729	**707**	10,04	–59,11	–54,09
Telecomunicaciones	2.220	1.926	**553**	7,86	–71,29	–75,09
Servicios de Internet (excepto *spam*)	447	427	**435**	6,18	1,87	–2,68
Publicidad y prospección comercial (excepto *spam*)	314	398	**414**	5,88	4,02	31,85
Contratación fraudulenta			**356**	5,06		
Administración pública	311	292	**344**	4,89	17,81	10,61
Comunicaciones electrónicas comerciales – *spam* (LSSI)	353	321	**282**	4,01	–12,15	–20,11
Sanidad	225	206	**225**	3,20	9,22	0,00
Recursos humanos, asuntos laborales	147	177	**219**	3,11	23,73	48,98
Suministro y comercialización de energía/agua	232	250	**203**	2,88	–18,80	–12,50
Comercio, transporte, hostelería	145	189	**169**	2,40	–10,58	16,55
Inscripción de ficheros / Información artículo 5	101	74	**123**	1,75	66,22	21,78
Comunidades propietarios, admón. fincas, otros profesionales	237	260	**107**	1,52	–58,85	–54,85
Organizaciones asociativas (excepto partidos políticos y sindicatos)	105	103	**86**	1,22	–16,50	–18,10
Medios de comunicación	75	76	**72**	1,02	–5,26	–4,00
Cookies (LSSI)	58	57	**62**	0,88	8,77	6,90
Seguros	81	114	**58**	0,82	–49,12	–28,40
Partidos políticos	56	88	**50**	0,71	–43,18	–10,71
Enseñanza	53	47	**49**	0,70	4,26	–7,55
Asuntos relacionados con procedimientos judiciales	56	40	**42**	0,60	5,00	–25,00
Sindicatos	44	53	**40**	0,57	–24,53	–9,09
Fuerzas y cuerpos de seguridad	49	52	**38**	0,54	–26,92	–22,45
Documentación desechada sin destruir o borrar	39	20	**25**	0,36	25,00	–35,90
Otros	214	76	**31**	0,44	–59,21	–85,51
TOTAL	**8.068**	**8.132**	**7.039**	**100,00**	**–13,44**	**–12,75**

* 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).

El aumento de las denuncias relativas a la inclusión en ficheros de morosidad y contratación fraudulenta ha obligado a la Agencia a especializar un grupo de trabajo en estos dos temas y crear una categoría de actividad diferenciada de las áreas de origen, que típicamente eran las empresas proveedoras de servicios y las entidades financieras. En el texto de la memoria se incluye una explicación más detallada de estos cambios.

RESOLUCIONES SANCIONADORAS EL SECTOR PRIVADO*

AÑO	2014	2015	2016	% RELATIVO	Δ% 2015/2016	Δ% 2014/2016
Videovigilancia	158	158	170	25,99	7,59	7,59
Ficheros de morosidad			141	21,56		
Comunicaciones electrónicas comerciales – *spam* (LSSI)	74	88	77	11,77	–12,50	4,05
Contratación fraudulenta			74	11,31		
Publicidad y prospección comercial (excepto *spam*)	30	22	54	8,26	145,45	80,00
Inscripción de ficheros / Información artículo 5	5	5	1	0,15	–80,00	–80,00
Servicios de Internet (excepto *spam*)	50	35	34	5,20	–2,86	–32,00
Telecomunicaciones	270	234	21	3,21	–91,03	–92,22
Comunidades propietarios, admón. fincas, otros profesionales	8	10	6	0,92	–40,00	–25,00
Entidades financieras	98	91	20	3,06	–78,02	–79,59
Cookies	20	16	9	1,38	–43,75	–55,00
Seguridad privada	3	11	0	0,00	–100,00	–100,00
Seguros	8	13	10	1,53	–23,08	25,00
Comercio, transporte, hostelería	52	39	5	0,76	–87,18	–90,38
Sanidad	17	12	5	0,76	–58,33	–70,59
Otros	10	18	13	1,99	–27,78	30,00
Documentación desechada sin destruir o borrar	3	6	2	0,31	–66,67	–33,33
Partidos políticos	3		4	0,61		33,33
Organizaciones asociativas, excepto partidos políticos y sindicatos	7	10	4	0,61	–60,00	–42,86
Sindicatos		2	1	0,15	–50,00	
Recursos humanos, asuntos laborales	9	3	1	0,15	–66,67	–88,89
Enseñanza	2	2	2	0,31	0,00	0,00
TOTAL	**827**	**775**	654	100,00	–15,61	–20,92

* El aumento de las denuncias relativas a la inclusión en ficheros de morosidad y contratación fraudulenta ha obligado a la Agencia a especializar un grupo de trabajo en estos dos temas y crear una categoría de actividad diferenciada de las áreas de origen, que típicamente eran las empresas proveedoras de servicios y las entidades financieras. En el texto de la memoria se incluye una explicación más detallada de estos cambios.

ÁREAS CON MAYOR IMPORTE GLOBAL DE SANCIONES

ACTIVIDAD	2014 (€)	2015 (€)	2016 (€)	% RELATIVO	Δ% 2015/2016	Δ% 2014/2016
Ficheros de morosidad			**5.835.007**	45,85		
Contratación fraudulenta			**3.420.003**	26,88		
Publicidad (excepto *spam*)	751.411	502.108	**1.964.305**	15,44	291,21	161,42
Telecomunicaciones	10.750.502	7.090.004	**549.800**	4,32	–92,25	–94,89
Entidades financieras	2.018.501	2.395.902	**516.001**	4,06	–78,46	–74,44
Comunicaciones electrónicas comerciales – *spam* (LSSI)	645.506	897.403	**439.851**	3,46	–50,99	–31,86
TOTAL (6 PRIMERAS)	**14.165.920**	**10.885.417**	**12.724.967**	**100,00**	**16,90**	**–10,17**
% RELATIVO AL TOTAL DEL AÑO	**83,32%**	**79,38%**	**89,67%**		**12,97**	**7,62**

SANCIONES ECONÓMICAS IMPUESTAS

AÑO	2014	2015	2016	Δ% 2015/2016	Δ% 2014/2016
IMPORTE TOTAL SANCIONES	17.002.622	13.712.621	**14.190.173**	3,48	–16,54

El importe total se refiere a la cuantía de las sanciones impuestas en el ejercicio (incluyendo las posibles modificaciones en la cuantía como consecuencia de los correspondientes recursos de reposición).

PROCEDIMIENTOS DE TUTELA DE DERECHOS

DISTRIBUCIÓN DE DERECHOS TUTELADOS SEGÚN RESULTADO DE LA RESOLUCIÓN

	ESTIMATORIA	ESTIMATORIA FORMAL O PARCIAL	DESESTIMATORIA	TOTAL
Cancelación	201	143	268	612
Acceso	123	94	122	339
Rectificación	10	11	15	36
Oposición/exclusión	37	22	28	87
TOTAL	371	270	433	1.074

En cada procedimiento resuelto puede haberse tutelado más de un derecho ARCO.

DISTRIBUCIÓN GEOGRÁFICA

DISTRIBUCIÓN GEOGRÁFICA DE LAS ACTUACIONES PREVIAS INICIADAS EN 2016 (PROVINCIA DEL DENUNCIANTE)

COMUNIDAD AUTÓNOMA	PROVINCIA	N.º	% RELATIVO
Comunidad Autónoma de Andalucía	Almería	90	1,18
	Cádiz	166	2,17
	Córdoba	92	1,21
	Granada	145	1,90
	Huelva	54	0,71
	Jaén	77	1,01
	Málaga	256	3,35
	Sevilla	352	4,61
Comunidad Autónoma de Aragón	Huesca	33	0,43
	Teruel	18	0,24
	Zaragoza	152	1,99
Comunidad Autónoma de Canarias	Las Palmas	239	3,13
	Santa Cruz de Tenerife	167	2,19
Comunidad Autónoma de Cantabria	Cantabria	94	1,23
Comunidad Autónoma de Castilla y León	Ávila	32	0,42
	Burgos	52	0,68
	León	72	0,94
	Palencia	25	0,33
	Salamanca	62	0,81
	Segovia	25	0,33
	Soria	8	0,10
	Valladolid	135	1,77
	Zamora	23	0,30
Comunidad Autónoma de Castilla-La Mancha	Albacete	65	0,85
	Ciudad Real	80	1,05
	Cuenca	10	0,13
	Guadalajara	47	0,62
	Toledo	104	1,36

COMUNIDAD AUTÓNOMA	PROVINCIA	N.º	% RELATIVO
Comunidad Autónoma de Cataluña	Barcelona	684	8,96
	Girona	68	0,89
	Lleida	46	0,60
	Tarragona	94	1,23
Ciudad Autónoma de Ceuta	Ceuta	6	0,08
Ciudad Autónoma de Melilla	Melilla	9	0,12
Comunidad de Madrid	Madrid	1.789	23,43
Comunidad Foral de Navarra	Navarra	59	0,77
Comunitat Valenciana	Alicante/Alacant	242	3,17
	Castellón/Castelló	66	0,86
	Valencia/València	352	4,61
Comunidad Autónoma de Extremadura	Badajoz	100	1,31
	Cáceres	59	0,77
Comunidad Autónoma de Galicia	A Coruña	274	3,59
	Lugo	53	0,69
	Ourense	38	0,50
	Pontevedra	183	2,40
Comunidad Autónoma de Illes Balears	Illes Balears	175	2,29
Comunidad Autónoma de La Rioja	La Rioja	50	0,65
Comunidad Autónoma del País Vasco	Araba/Álava	34	0,45
	Bizkaia	104	1,36
	Gipuzkoa	42	0,55
Comunidad Autónoma del Principado de Asturias	Asturias	212	2,78
Comunidad Autónoma de la Región de Murcia	Murcia	220	2,88
TOTAL		**7.634**	**100**

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 Directora o las iniciadas por solicitud de colaboración de otras autoridades extranjeras de protección de datos.

ESTABLECIMIENTO DE INVESTIGADOS EN PROCEDIMIENTOS SANCIONADORES Y DE APERCIBIMIENTO RESUELTOS EN 2016

COMUNIDAD AUTÓNOMA	PROVINCIA	N.º	% RELATIVO
Comunidad Autónoma de Andalucía	Almería	12	1,13
	Cádiz	8	0,75
	Córdoba	7	0,66
	Granada	14	1,31
	Huelva	4	0,38
	Jaén	8	0,75
	Málaga	28	2,63
	Sevilla	26	2,44
Comunidad Autónoma de Aragón	Huesca	2	0,19
	Teruel	1	0,09
	Zaragoza	14	1,31
Comunidad Autónoma de Canarias	Las Palmas	20	1,88
	Santa Cruz de Tenerife	16	1,50
Comunidad Autónoma de Cantabria	Cantabria	22	2,07
Comunidad Autónoma de Castilla y León	Ávila	4	0,38
	Burgos	3	0,28
	León	5	0,47
	Palencia	5	0,47
	Salamanca	2	0,19
	Segovia	1	0,09
	Soria	0	0,00
	Valladolid	17	1,60
	Zamora	3	0,28
Comunidad Autónoma de Castilla-La Mancha	Albacete	4	0,38
	Ciudad Real	5	0,47
	Cuenca	0	0,00
	Guadalajara	3	0,28
	Toledo	6	0,56
Comunidad Autónoma de Cataluña	Barcelona	110	10,33
	Girona	9	0,85
	Lleida	7	0,66
	Tarragona	10	0,94

COMUNIDAD AUTÓNOMA	PROVINCIA	N.º	% RELATIVO
Ciudad Autónoma de Ceuta	Ceuta	0	0,00
Ciudad Autónoma de Melilla	Melilla	0	0,00
Comunidad de Madrid	Madrid	456	42,82
Comunidad Foral de Navarra	Navarra	6	0,56
Comunitat Valenciana	Alicante/Alacant	32	3,00
	Castellón/Castelló	9	0,85
	Valencia/València	38	3,57
Comunidad Autónoma de Extremadura	Badajoz	2	0,19
	Cáceres	9	0,85
Comunidad Autónoma de Galicia	A Coruña	22	2,07
	Lugo	6	0,56
	Ourense	2	0,19
	Pontevedra	18	1,69
Comunidad Autónoma de las Illes Balears	Illes Balears	19	1,78
Comunidad Autónoma de La Rioja	La Rioja	4	0,38
Comunidad Autónoma del País Vasco	Araba/Álava	3	0,28
	Bizkaia	11	1,03
	Gipuzkoa	4	0,38
Comunidad Autónoma del Principado de Asturias	Asturias	25	2,35
Comunidad Autónoma de la Región de Murcia	Murcia	23	2,16
TOTAL		**1.065**	**100**

SEDE DE LOS INVESTIGADOS EN PROCEDIMIENTOS DE INFRACCIÓN DE LAS AAPP RESUELTOS EN 2016

COMUNIDAD AUTÓNOMA	PROVINCIA	N.º	% RELATIVO
Comunidad Autónoma de Andalucía	Córdoba	1	1,79
	Granada	2	3,57
	Sevilla	4	7,14
Comunidad Autónoma de Aragón	Zaragoza	1	1,79
Comunidad Autónoma de Canarias	Las Palmas	4	7,14
Comunidad Autónoma de Castilla y León	Ávila	1	1,79
	Burgos	1	1,79
	León	1	1,79
	Salamanca	2	3,57
	Valladolid	1	1,79
Comunidad Autónoma de Castilla-La Mancha	Ciudad Real	1	1,79
	Toledo	3	5,36
Comunidad Autónoma de Cataluña	Barcelona	1	1,79
	Lleida	1	1,79
Ciudad Autónoma de Melilla	Melilla	2	3,57
Comunidad de Madrid	Madrid	14	25,00
Comunitat Valenciana	Alicante/Alacant	2	3,57
	Valencia/València	3	5,36
Comunidad Autónoma de Galicia	A Coruña	4	7,14
	Lugo	1	1,79
Illes Balears	Illes Balears	1	1,79
Comunidad Autónoma del País Vasco	Araba/Álava	1	1,79
Comunidad Autónoma del Principado de Asturias	Asturias	1	1,79
Comunidad Autónoma de la Región de Murcia	Murcia	3	5,36
TOTAL		**56**	**100**

DISTRIBUCIÓN GEOGRÁFICA DE LOS PROCEDIMIENTOS DE TUTELA DE DERECHOS INICIADOS EN 2016 (PROVINCIA DEL RECLAMANTE)

COMUNIDAD AUTÓNOMA	PROVINCIA	N.º	% RELATIVO
Comunidad Autónoma de Andalucía	Almería	26	1,03
	Cádiz	50	1,98
	Córdoba	48	1,90
	Granada	54	2,14
	Huelva	11	0,43
	Jaén	20	0,79
	Málaga	80	3,16
	Sevilla	111	4,39
Comunidad Autónoma de Aragón	Huesca	4	0,16
	Teruel	2	0,08
	Zaragoza	54	2,14
Comunidad Autónoma de Canarias	Las Palmas	65	2,57
	Santa Cruz de Tenerife	56	2,21
Comunidad Autónoma de Cantabria	Cantabria	26	1,03
Comunidad Autónoma de Castilla y León	Ávila	1	0,04
	Burgos	6	0,24
	León	22	0,87
	Palencia	13	0,51
	Salamanca	9	0,36
	Segovia	6	0,24
	Soria	2	0,08
	Valladolid	51	2,02
	Zamora	2	0,08
Comunidad Autónoma de Castilla-La Mancha	Albacete	15	0,59
	Ciudad Real	22	0,87
	Cuenca	3	0,12
	Guadalajara	9	0,36
	Toledo	33	1,30
Comunidad Autónoma de Cataluña	Barcelona	203	8,03
	Girona	24	0,95
	Lleida	8	0,32
	Tarragona	23	0,91

COMUNIDAD AUTÓNOMA	PROVINCIA	N.º	% RELATIVO
Ciudad Autónoma de Melilla	Melilla	4	0,16
Comunidad de Madrid	Madrid	610	24,12
Comunidad Foral de Navarra	Navarra	16	0,63
Comunitat Valenciana	Alicante/Alacant	70	2,77
	Castellón/Castelló	93	3,68
	Valencia/València	124	4,90
Comunidad Autónoma de Extremadura	Badajoz	28	1,11
	Cáceres	7	0,28
Comunidad Autónoma de Galicia	A Coruña	55	2,17
	Lugo	9	0,36
	Ourense	12	0,47
	Pontevedra	59	2,33
Comunidad Autónoma de las Illes Balears	Illes Balears	42	1,66
Comunidad Autónoma de La Rioja	La Rioja	29	1,15
Comunidad Autónoma del País Vasco	Araba/Álava	17	0,67
	Bizkaia	40	1,58
	Gipuzkoa	16	0,63
Comunidad Autónoma del Principado de Asturias	Asturias	58	2,29
Comunidad Autónoma de la Región de Murcia	Murcia	181	7,16
TOTAL		**2.529**	**100**

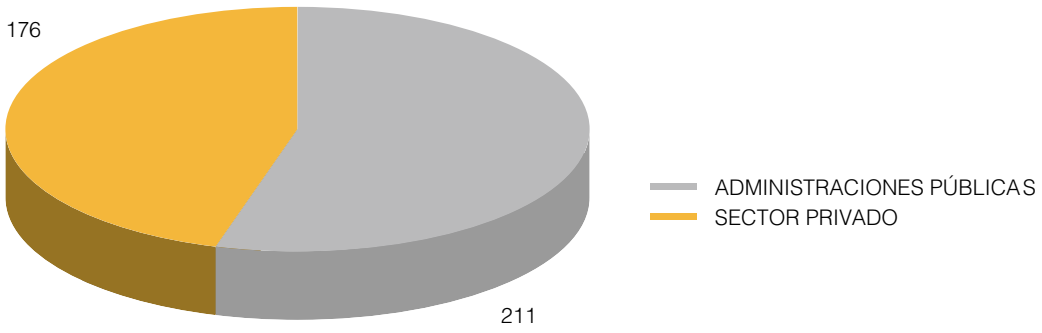
GABINETE JURÍDICO

CONSULTAS

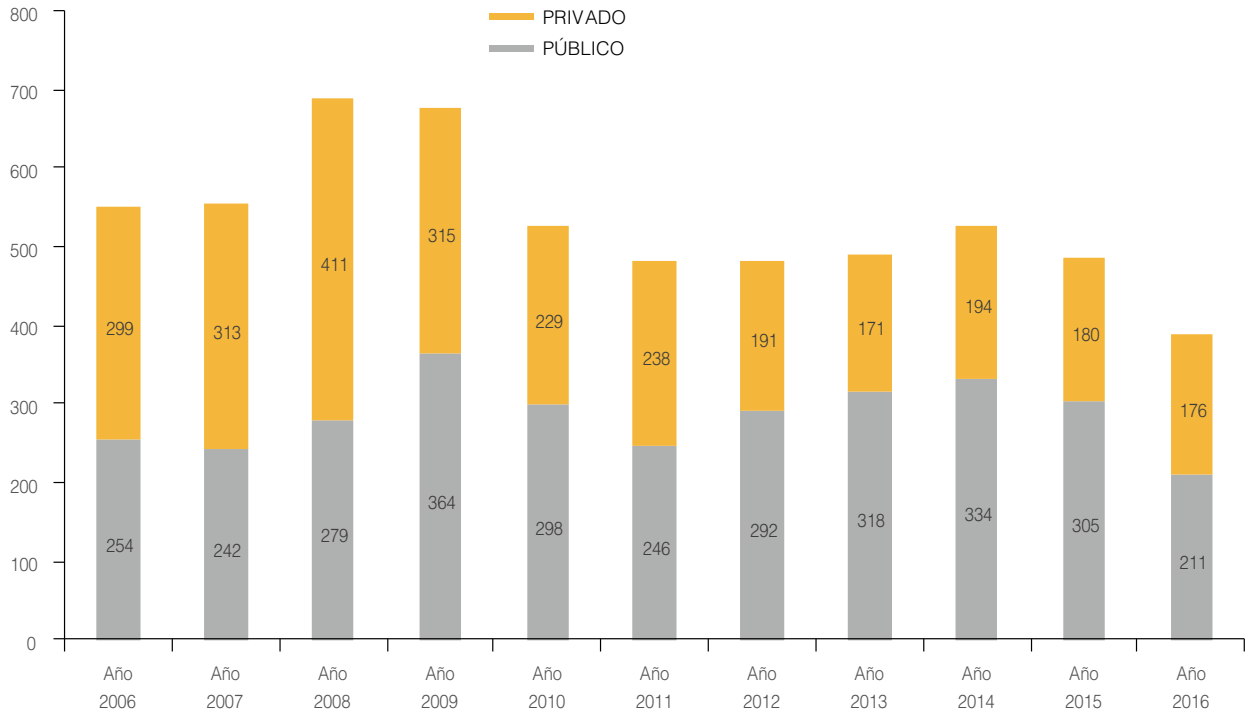
ADMINISTRACIONES PÚBLICAS	211
Administración General del Estado	92
Comunidades Autónomas	56
Entidades Locales	35
Otros Organismos Públicos	28

CONSULTAS PRIVADAS	176
Empresas	95
Particulares	47
Asociaciones y fundaciones	18
Sindicatos	16
TOTAL	**387**

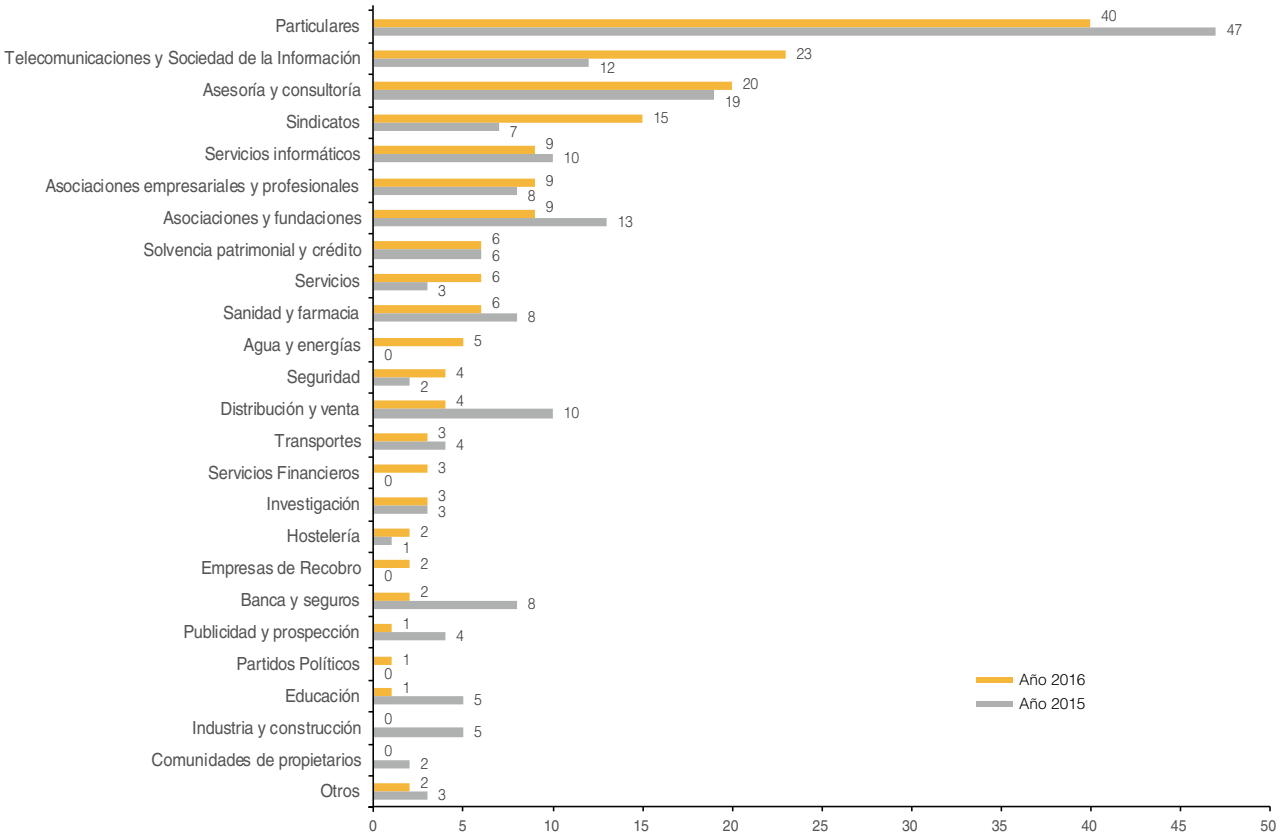
DISTRIBUCIÓN 2016 CONSULTAS PÚBLICAS/PRIVADAS



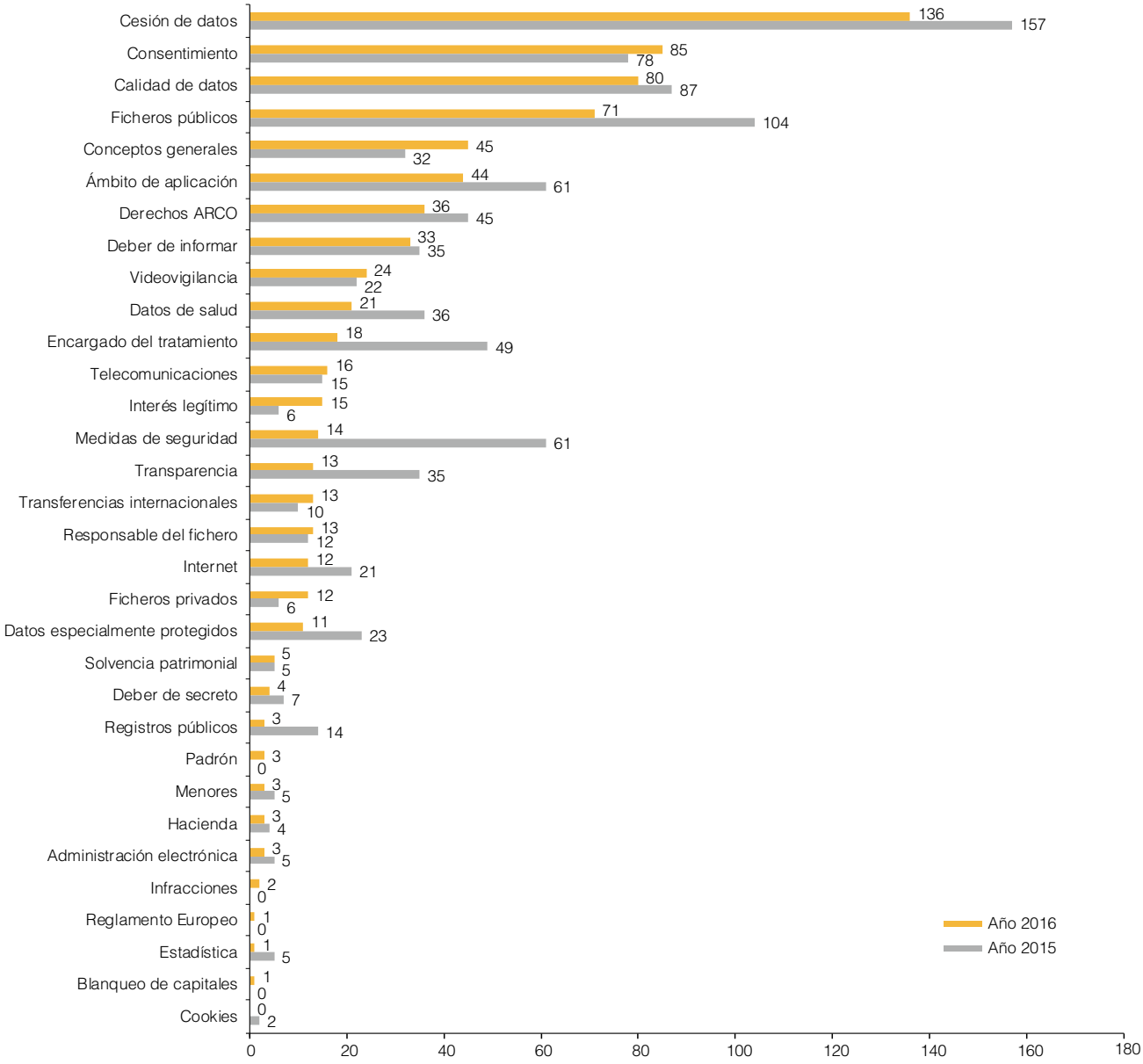
EVOLUCIÓN DE LAS CONSULTAS (2006-2016)



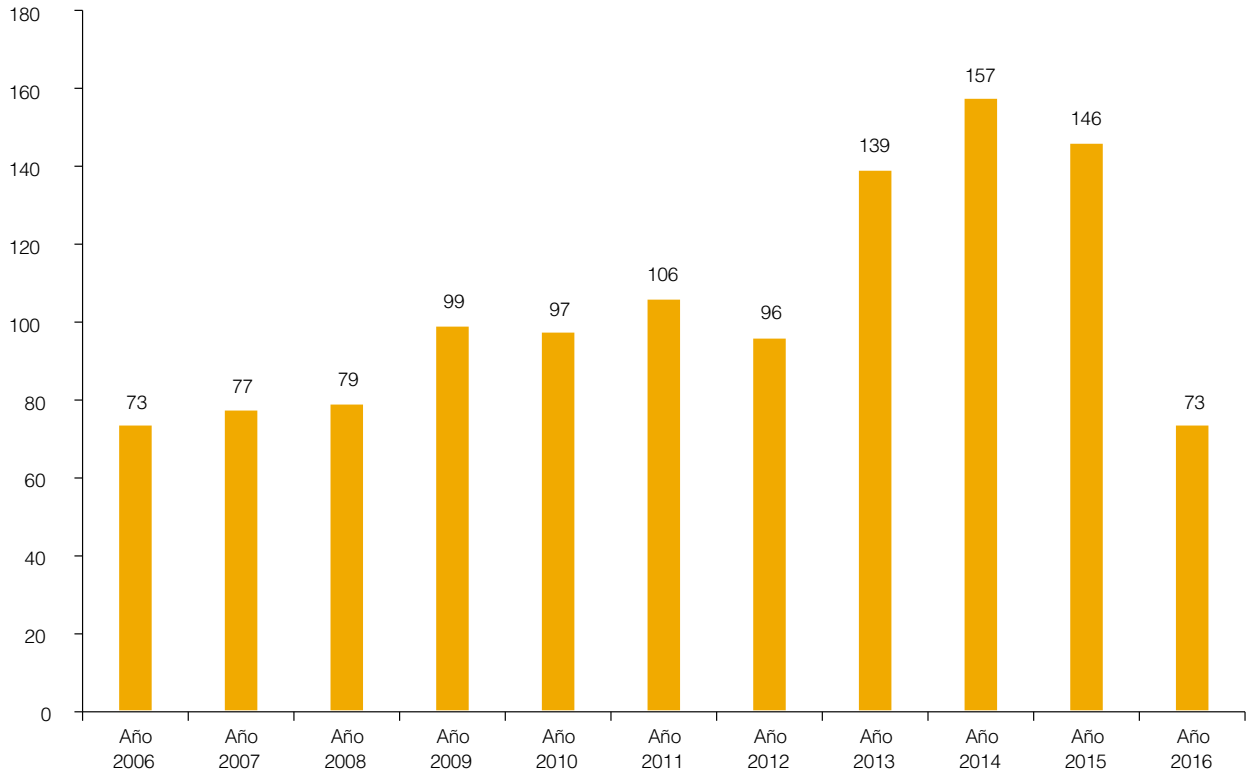
EVOLUCIÓN DE CONSULTAS POR SECTORES (2016-2015)



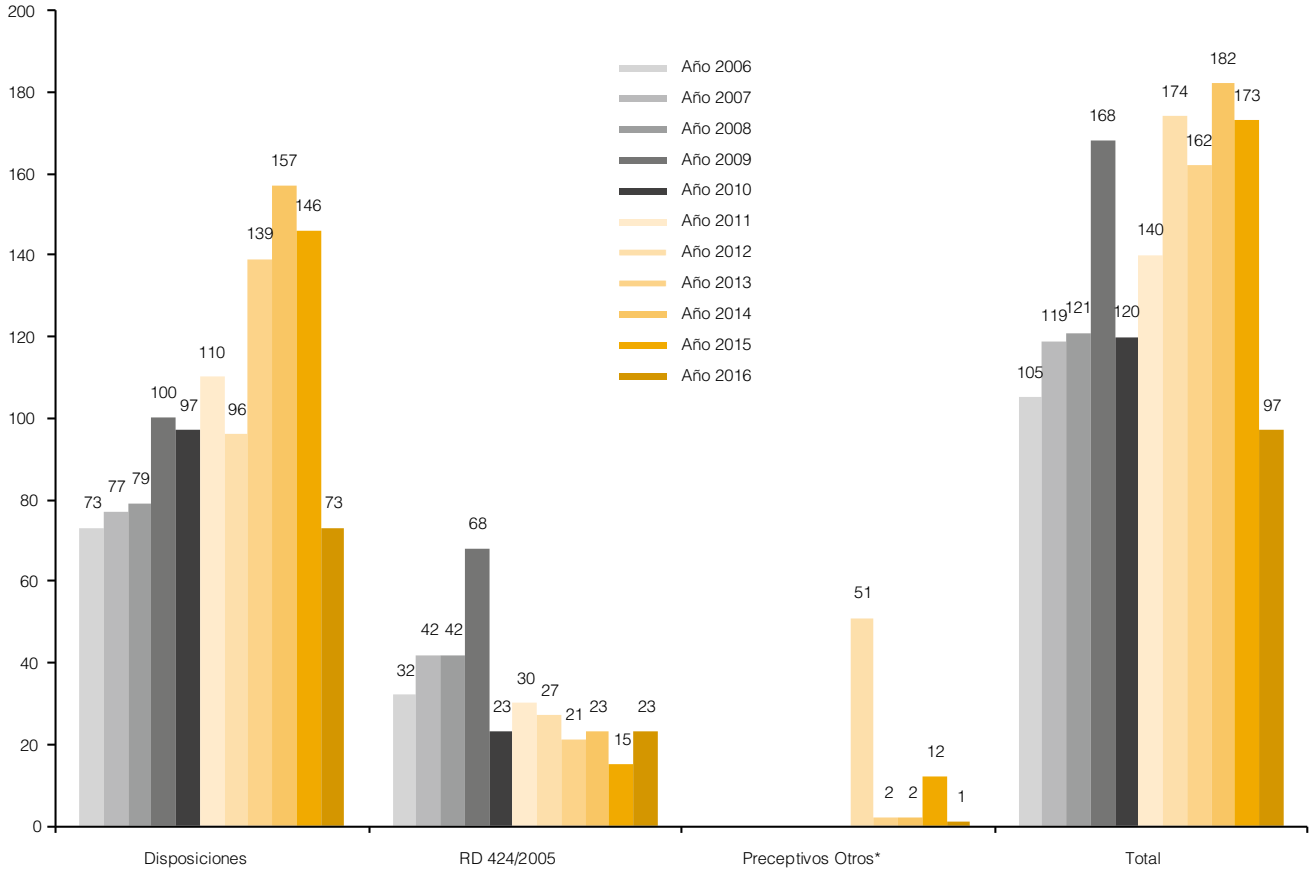
EVOLUCIÓN CONSULTAS POR MATERIAS (2016-2015)



EVOLUCIÓN DE INFORMES PRECEPTIVOS A DISPOSICIONES GENERALES (2006-2016)

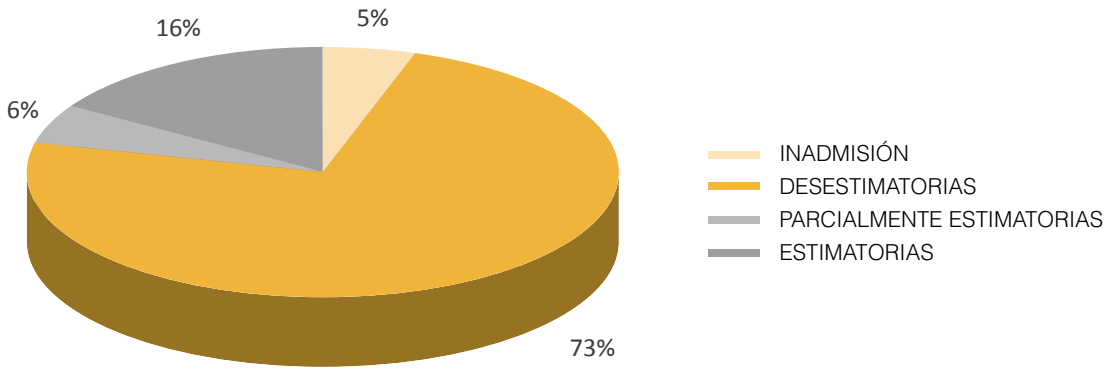


EVOLUCIÓN DE INFORMES PRECEPTIVOS (2006-2016)

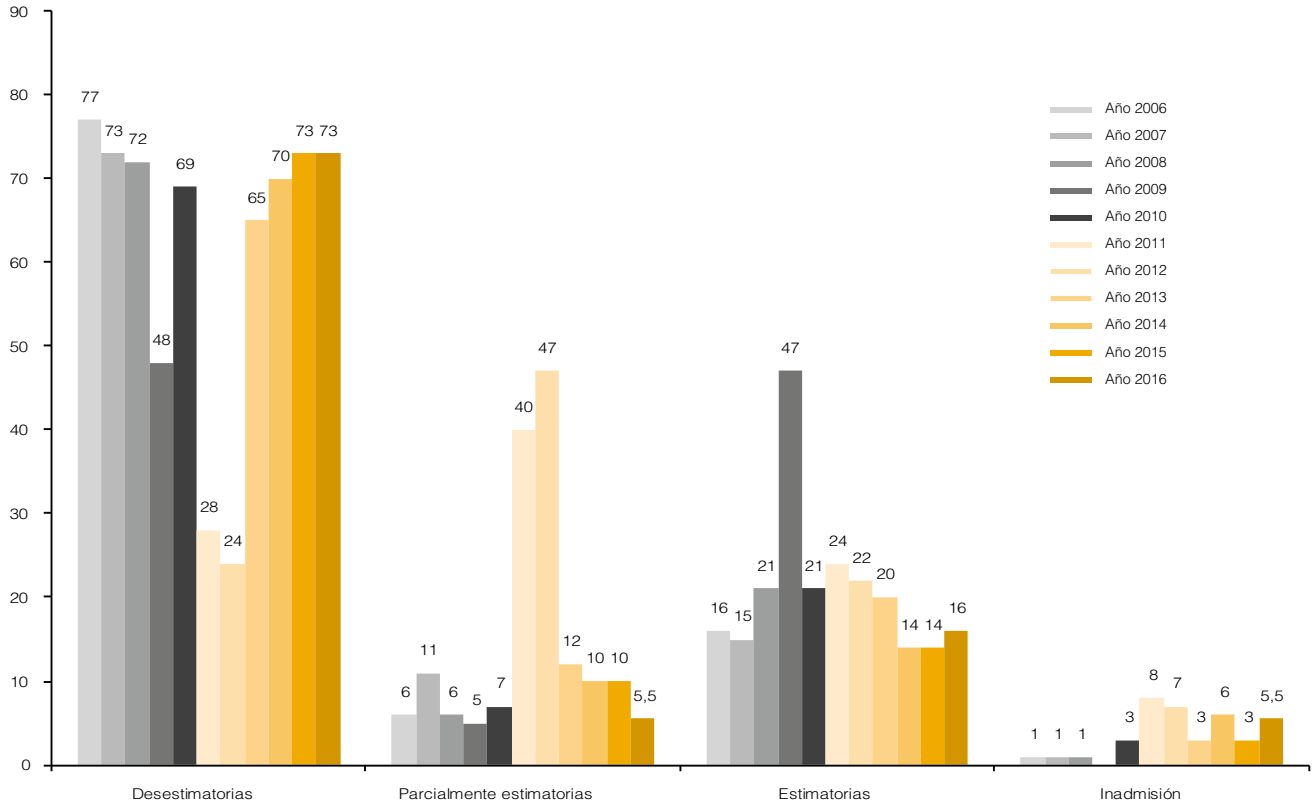


* Derivados de la Ley de Regulación del juego y la Ley de Prevención del blanqueo de capitales y de la financiación del terrorismo.

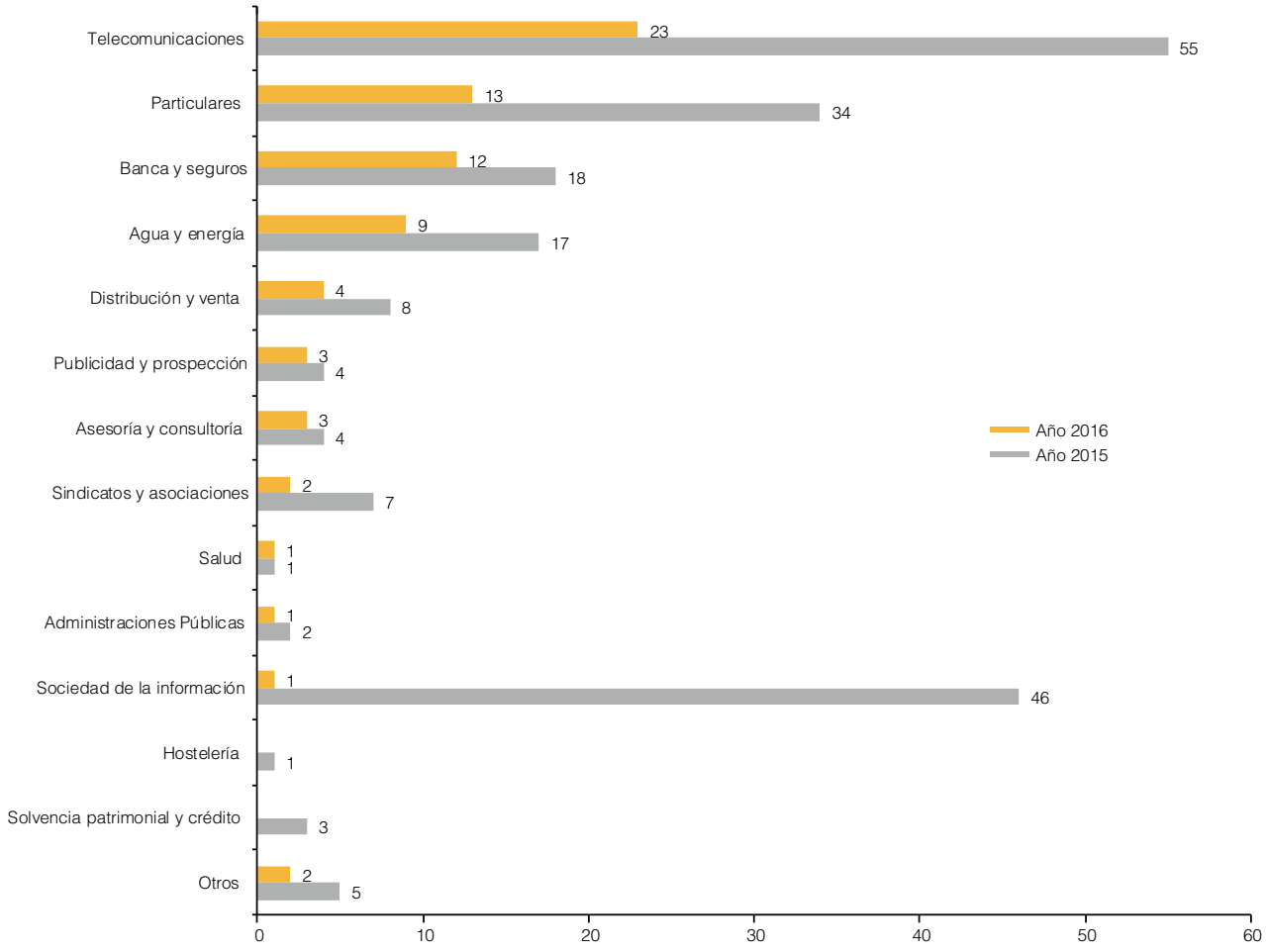
SENTENCIAS DE LA AUDIENCIA NACIONAL 2016



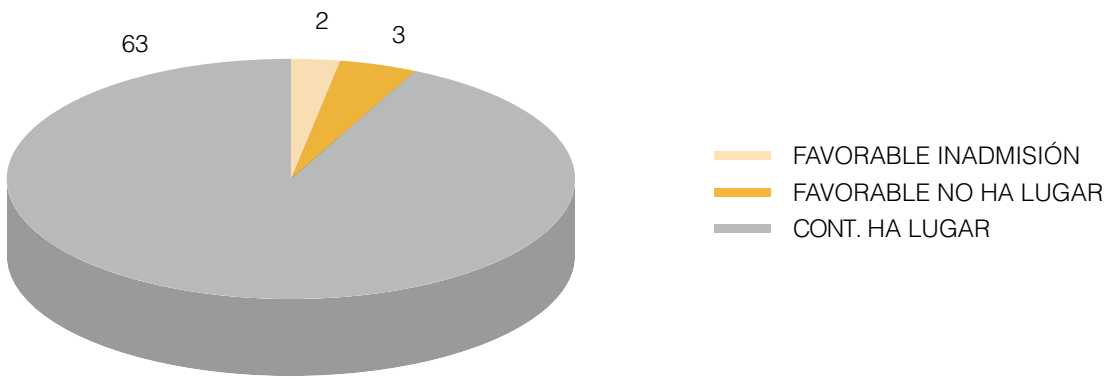
EVOLUCIÓN POR SENTIDO DEL FALLO EN PORCENTAJES (2006-2016)



COMPARATIVA POR SECTOR DEL RECURRENTE (2016-2015)



SENTENCIAS DEL TRIBUNAL SUPREMO EN 2016



ATENCIÓN AL CIUDADANO

CONSULTAS TOTALES PLANTEADAS ANTE EL ÁREA DE ATENCIÓN AL CIUDADANO

	ATENCIÓN PRESENCIAL	TELÉFONO	POR ESCRITO	SEDE ELECTRÓNICA	RESPUESTA AUTOMÁTICA FAQs	TOTAL
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
AÑO 2016	4.183	76.869	552	8.054	147.297	236.955
INCREMENTO 2015-2016	**11,04%**	**3,51%**	**0,36%**	**14,17%**	**10,99%**	**8,52%**

VISITAS A LA WEB www.agpd.es

AÑO	2014	2015	2016
Visitas	5.706.488	4.952.945	5.534.282
Promedio diario	**7.816**	**6.766**	**7.560**

ACCESOS AL PORTAL DE VÍDEOS 'PROTEGE TUS DATOS EN INTERNET'

Accesos al canal	25.150
Visualizaciones de vídeos	43.587*

* Se puede acceder a los vídeos directamente sin pasar por el canal, entrando desde la web www.tudecideseninternet.es.

ACCESOS A LA WEB www.tudecideseninternet.es

VISITANTES DISTINTOS[1]	NÚMERO DE VISITAS[2]
32.911	48.938

[1] Visitantes distintos: se refiere a una visita que ha solicitado al menos una página. Si este visitante ingresa numerosas veces solo contará como una.

[2] 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*

	TEMA DE CONSULTA	ACCESOS
1	Videovigilancia	6.632
2	En qué te podemos ayudar y en qué no	5.600
3	Comunidades de propietarios	5.655
4	Inscripción de ficheros	4.992
5	Ficheros solvencia patrimonial	4.975
6	Denuncias/reclamaciones	2.508
7	Tratamiento de datos en el ámbito laboral	2.480

* Datos contabilizados desde la renovación del catálogo de preguntas frecuentes (julio de 2016).

TEMAS MÁS CONSULTADOS EN LA ATENCIÓN PRESENCIAL Y TELEFÓNICA

TEMAS	%
Inscripción de ficheros	26,34
Denuncias	3,33
Ficheros de morosidad	4,55
Videovigilancia	5,41
Comunidades de vecinos	1,63
Derechos ARCO y 'derecho al olvido'	8,06
Cesión de datos	1,90
Otros (*)	48,78

* Incluye temas como requisitos acerca del cumplimiento de la LOPD, transferencias internacionales, medidas de seguridad, etc.

ANÁLISIS DE CONSULTAS TELEFÓNICAS Y PRESENCIALES SOBRE DERECHOS ARCO

DERECHOS	%
Acceso	7,92
Rectificación	2,68
Cancelación	53,34
Oposición	9,50
'Derecho al olvido'	26,56

CONSULTAS ESPECIALIZADAS SOBRE EL TRATAMIENTO DE DATOS DE MENORES

CANALES	N.º CONSULTAS
Teléfono	166
WhatsApp	129
Correo electrónico	163
Sede electrónica	218

EVOLUCIÓN DEL REGISTRO DE ENTRADA/SALIDA DE DOCUMENTOS

	2014	2015	2016
ENTRADA	520.286	506.670	433.484
SALIDA	346.694	328.830	369.794
TOTAL	866.980	835.500	803.278

DISTRIBUCIÓN DE LOS DOCUMENTOS REGISTRADOS EN 2016 SEGÚN EL MEDIO UTILIZADO

REGISTRO DE ENTRADAS	2016	%
Por medios electrónicos	406.086	93,68
Con certificado electrónico	*247.042*	
Sin certificado electrónico	*159.044*	
Por otros medios*	27.398	6,32
TOTAL ENTRADAS	**433.484**	**100,00**

REGISTRO DE SALIDAS	2016	%
Por medios electrónicos	87.584	23,68
Comparecencia en sede	*34.123*	
Dirección Electrónica Habilitada	*53.461*	
Por otros medios*	282.210	76,32
TOTAL SALIDAS	**369.794**	**100,00**

* Correo electrónico, correo postal, en mano, mensajería…

USO DE MEDIOS ELECTRÓNICOS EN LA PRESENTACIÓN DE DOCUMENTOS

TIPO DE PROCEDIMIENTO	2014	2015	2016
Entradas con certificado	8.051	10.863	98.113*
Entradas sin certificado	14.240	16.273	96.076*
TOTAL	**22.291**	**27.136**	**194.189***

* El aumento es debido a que se han contabilizado las notificaciones de ficheros.

SOLICITUDES DE ACCESO A INFORMACIÓN PÚBLICA

RECIBIDAS	INADMITIDAS*	CONCEDIDAS	DESISTIMIENTO	CONSULTAS**	DENEGADAS
60	16	28	2	13	1

* Causas de inadmisión (Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno): abuso de derecho; reelaboración y peticiones repetidas (art. 18 Ley de Transparencia) Disposición adicional 1.ª de la citada ley.

** No se trataba de peticiones de acceso a la información sino de consultas sobre protección de datos.

CONTENIDOS ELECTRÓNICOS

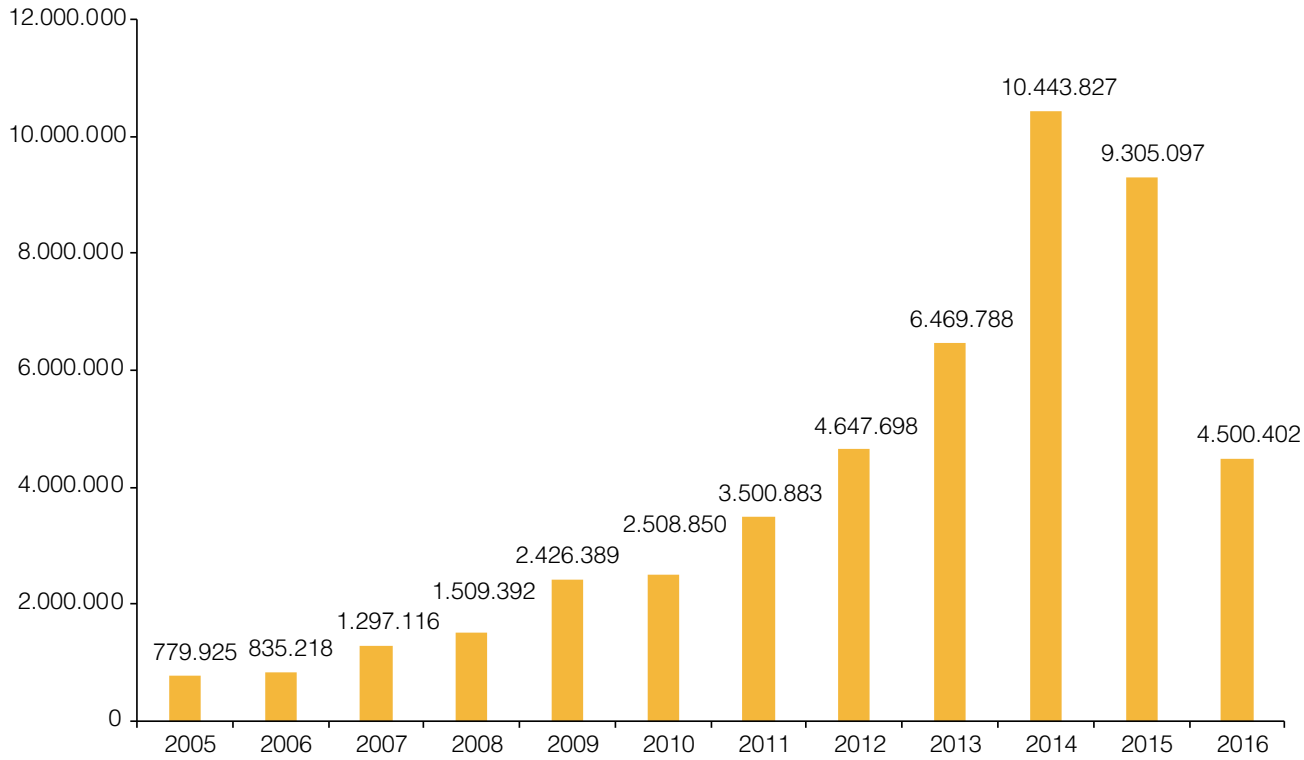
	2016
Accesos web	5.534.282
Accesos al Portal de Transparencia	305.538
Consultas FAQ's	147.297
Consultas electrónicas de ciudadanos	8.054
Accesos herramienta NOTA	372.525
Solicitud de copias de contenido de ficheros	15.269
Accesos herramienta EVALÚA	9.432
Accesos herramienta DISPONE	5.062
Guía de privacidad y seguridad en Internet*	**72.008**
Guía de seguridad de datos	28.183
Modelo del documento de seguridad	22.578
El derecho fundamental a la protección de datos: guía para el ciudadano	26.111
Guía del responsable de ficheros	36.712
Guías de videovigilancia	48.841
Guía 'La protección de datos en las relaciones laborales'	31.828
Guía para clientes que contraten servicios de *cloud computing*	18.804
Orientaciones para prestadores de servicios de *cloud computing*	2.713
Guía sobre el uso de las *cookies*	461.192
Guía sobre seguridad y privacidad de las tecnologías RFID	8.423
Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)	13.606
Documentos Plan Estratégico AEPD	11.774
Inspección sectorial de oficio sobre servicios de *cloud computing* en el sector educativo	3.210
El Reglamento General de Protección de Datos en 12 preguntas*	**28.532**
Implicaciones prácticas del RGPD para entidades en el periodo de transición*	**10.561**
Orientaciones sobre protección de datos en la reutilización de la información del sector público*	**3.781**
Orientaciones y garantías en los procedimientos de anonimización*	**5.267**
Cómo gestionar una fuga de información en un despacho de abogados*	**2.079**

* Contenidos incorporados a la página web en 2016.

REGISTRO GENERAL DE PROTECCIÓN DE DATOS

DERECHO DE CONSULTA AL REGISTRO

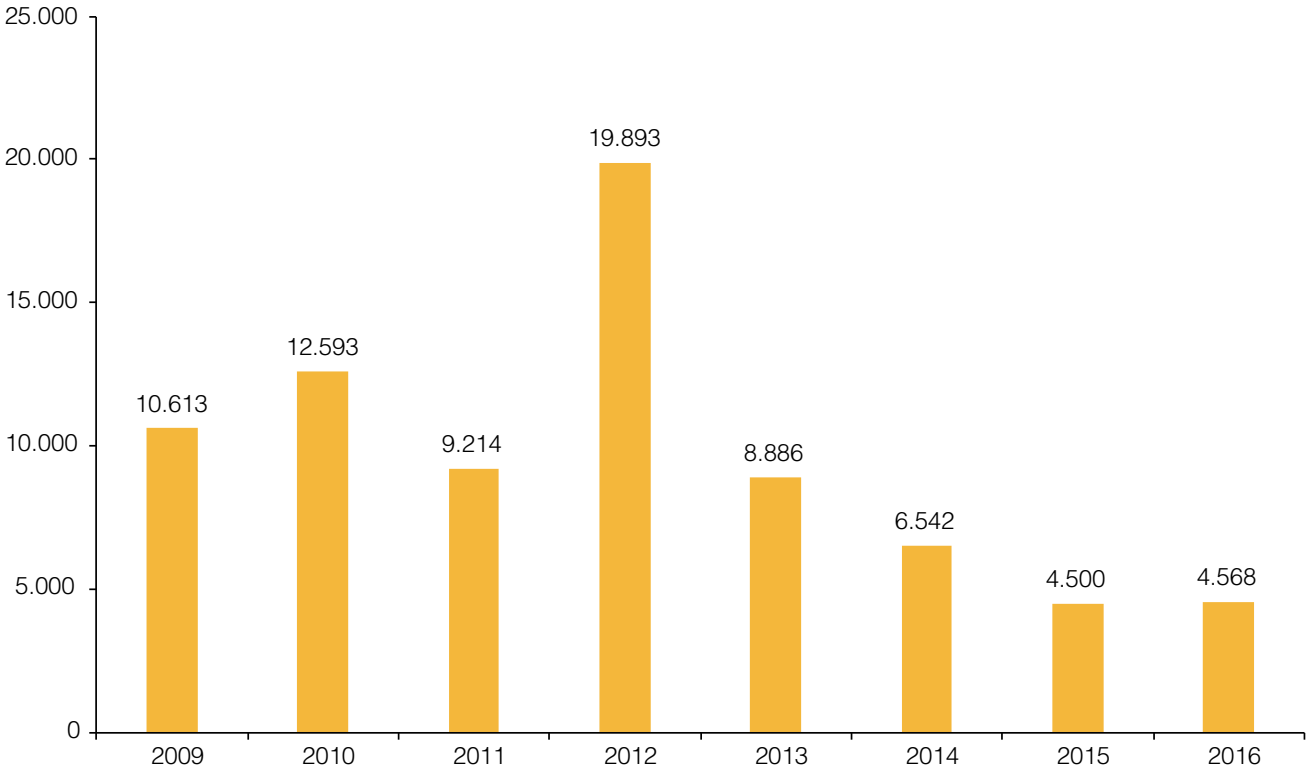
TITULARIDAD	2015	2016
Privada	6.804.638	2.733.169
Pública	2.500.459	1.767.233
TOTAL	9.305.097	4.500.402



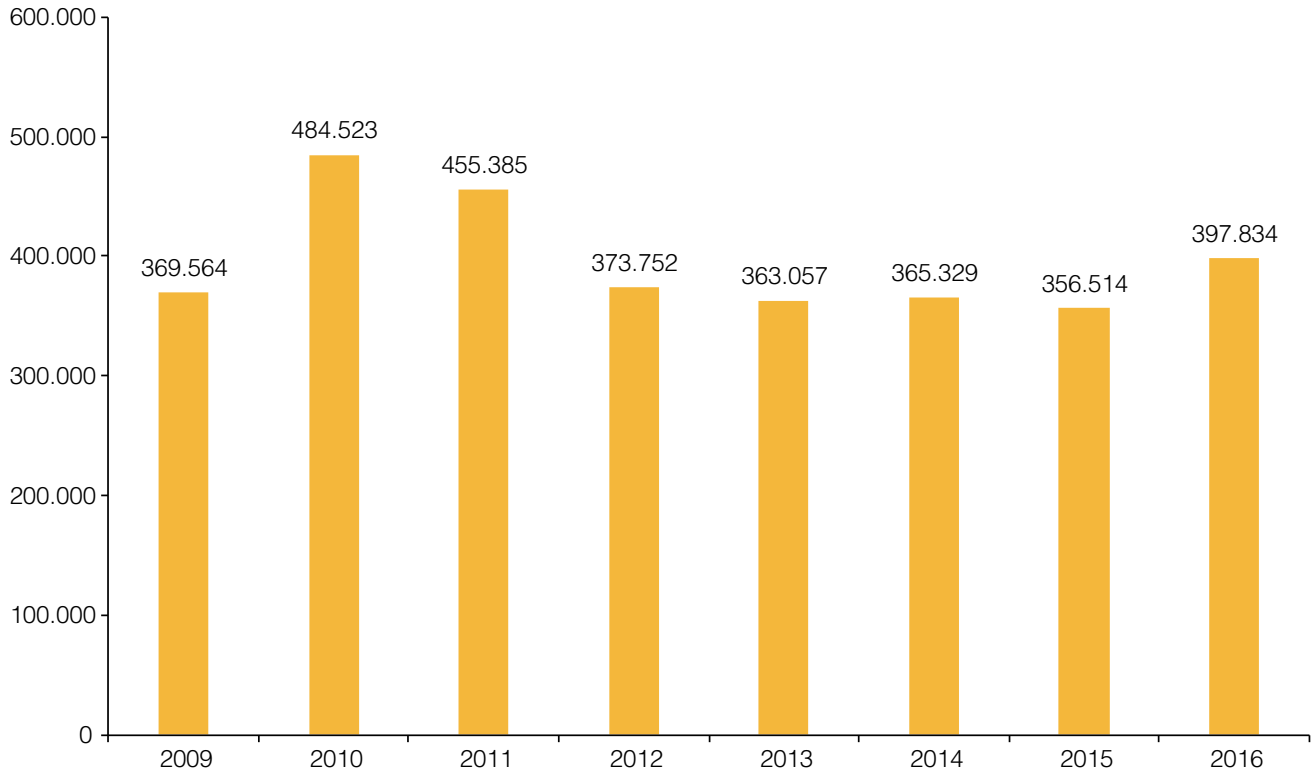
EVOLUCIÓN DE LA INSCRIPCIÓN DE FICHEROS EN EL RGPD

A 31 DE DIC.	2009	2010	2011	2012	2013	2014	2015	2016
Tit. Pública	95.696	108.289	117.503	137.396	146.282	152.824	157.324	161.892
Tit. Privada	1.552.060	2.036.583	2.491.968	2.865.720	3.228.777	3.594.106	3.950.620	4.348.454
TOTAL	**1.647.756**	**2.144.872**	**2.609.471**	**3.003.116**	**3.375.059**	**3.746.930**	**4.107.944**	**4.510.346**

INCREMENTO ANUAL DE FICHEROS TITULARIDAD PÚBLICA



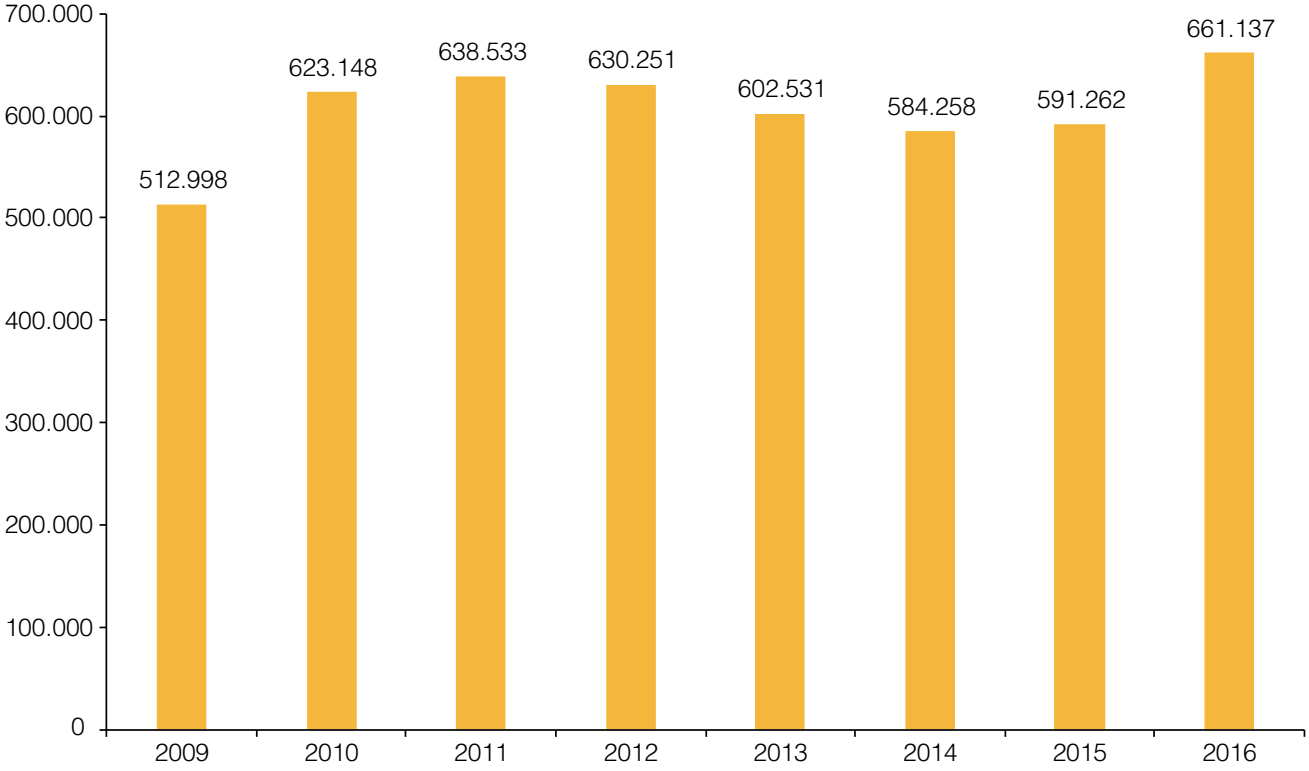
INCREMENTO ANUAL DE FICHEROS TITULARIDAD PRIVADA



OPERACIONES DE INSCRIPCIÓN

	2015	2016	% VARIACIÓN 2015/2016	MEDIA DIARIA EN 2015	MEDIA DIARIA EN 2016
Operaciones de inscripción	591.262	661.137	+12	2.464	2.755
TOTAL DE FICHEROS INSCRITOS	**4.107.944**	**4.510.346**	**+11**	**1.504**	**1.677**

EVOLUCIÓN ANUAL DE LAS OPERACIONES DE INSCRIPCIÓN



INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN TERRITORIAL DE FICHEROS

	RESPONSABLES		FICHEROS	
	2016	TOTAL	2016	TOTAL
Comunidad Autónoma de Andalucía	**38.652**	**223.762**	**96.922**	**697.748**
Almería	3.903	20.791	9.678	68.467
Cádiz	5.086	28.571	13.734	90.252
Córdoba	3.929	20.781	10.053	65.396
Granada	5.302	29.664	12.944	96.047
Huelva	1.421	9.666	3.293	28.748
Jaén	2.606	16.734	7.107	57.441
Málaga	8.297	50.942	22.832	159.255
Sevilla	8.146	47.511	17.281	132.142
Comunidad Autónoma de Aragón	**6.423**	**48.806**	**13.920**	**124.137**
Huesca	1.019	9.320	2.495	23.055
Teruel	426	4.357	1.195	12.001
Zaragoza	4.980	35.195	10.230	89.081
Comunidad Autónoma del Principado de Asturias	**7.052**	**44.451**	**17.503**	**134.214**
Comunidad Autónoma de Canarias	**7.107**	**47.778**	**18.772**	**155.489**
Las Palmas	3.345	22.734	9.219	75.514
Santa Cruz de Tenerife	3.764	25.133	9.553	79.975
Comunidad Autónoma de Cantabria	**3.137**	**18.220**	**7.195**	**48.520**
Comunidad Autónoma de Castilla y León	**9.782**	**74.572**	**22.729**	**210.187**
Ávila	693	4.900	1.506	12.404
Burgos	1.384	11.448	2.806	28.524
León	1.818	14.055	4.036	39.138
Palencia	772	5.428	1.907	16.071
Salamanca	1.069	9.190	2.713	25.411
Segovia	876	6.254	2.537	20.404
Soria	338	3.146	902	9.041
Valladolid	2.342	15.593	5.085	44.478
Zamora	500	4.729	1.237	14.716

	RESPONSABLES		FICHEROS	
	2016	TOTAL	2016	TOTAL
Comunidad Autónoma de Castilla-La Mancha	**8.034**	**55.302**	**19.422**	**165.558**
Albacete	2.155	14.403	5.127	45.020
Ciudad Real	1.882	12.707	4.956	38.942
Cuenca	829	5.468	2.082	15.571
Guadalajara	883	6.122	2.140	16.470
Toledo	2.287	16.695	5.117	49.555
Comunidad Autónoma de Cataluña	**35.106**	**271.594**	**84.684**	**734.816**
Barcelona	27.017	203.057	63.174	539.637
Girona	3.201	30.969	8.273	86.767
Lleida	1.576	13.928	4.038	37.002
Tarragona	3.324	24.085	9.199	71.410
Comunidad de Madrid	**43.656**	**253.676**	**97.380**	**673.862**
Comunitat Valenciana	**27.458**	**178.076**	**59.889**	**492.603**
Alicante / Alacant	11.950	63.880	25.709	173.554
Castellón / Castelló	2.707	20.472	5.986	58.667
Valencia / València	12.811	93.919	28.194	260.382
Comunidad Autónoma de Extremadura	**4.073**	**26.769**	**9.811**	**79.250**
Badajoz	2.566	16.710	5.870	49.112
Cáceres	1.509	10.098	3.941	30.138
Comunidad Autónoma de Galicia	**16.346**	**106.617**	**34.826**	**303.087**
A Coruña	7.938	46.785	16.097	131.742
Lugo	1.601	13.221	3.759	36.610
Ourense	1.515	11.493	3.378	30.928
Pontevedra	5.297	35.384	11.592	103.807
Comunidad Autónoma de las Illes Balears	**6.331**	**35.820**	**18.425**	**129.010**
Comunidad Foral de Navarra	**2.772**	**16.675**	**7.124**	**50.228**
Comunidad Autónoma del País Vasco	**10.724**	**63.978**	**25.472**	**176.817**
Araba / Álava	1.499	8.968	3.172	23.285
Gipuzkoa	3.902	20.388	10.374	60.750
Bizkaia	5.331	34.741	11.926	92.782
Comunidad Autónoma de La Rioja	**1.414**	**12.750**	**3.198**	**32.936**
Comunidad Autónoma de la Región de Murcia	**7.205**	**46.514**	**16.095**	**131.857**
Ciudad Autónoma de Ceuta	**107**	**983**	**256**	**2.728**
Ciudad Autónoma de Melilla	**205**	**1.080**	**539**	**5.033**

DISTRIBUCIÓN DE FICHEROS SEGÚN TIPOS DE DATOS

	2016	TOTAL
Datos especialmente protegidos (ideología, creencias, religión y afiliación sindical)	5.330	91.694
Otros datos especialmente protegidos (origen racial, salud y vida sexual)	36.471	461.075
Datos de carácter identificativo	460.868	4.348.454
Datos de características personales	193.864	1.932.502
Datos de circunstancias sociales	131.347	1.161.270
Datos académicos y profesionales	104.482	1.085.459
Detalles de empleo y carrera administrativa	114.443	1.296.459
Datos de información comercial	139.016	1.240.827
Datos económico-financieros	241.594	2.443.251
Datos de transacciones	190.084	1.843.408
Otros tipos de datos	24.590	208.659

DISTRIBUCIÓN DE FICHEROS SEGÚN SU FINALIDAD

	2016	TOTAL	% VARIACIÓN 2016 TOTAL
Gestión de clientes, contable, fiscal y administrativa	242.191	2.515.785	+9,63
Recursos humanos	93.341	962.402	+9,70
Gestión de nóminas	64.193	705.726	+9,10
Publicidad y prospección comercial	63.802	418.303	+15,25
Videovigilancia	50.107	290.023	+17,28
Prevención de riesgos laborales	47.760	395.123	+12,09
Comercio electrónico	31.536	153.934	+20,49
Gestión y control sanitario	14.744	165.993	+8,88
Seguridad y control de acceso a edificios	13.431	77.544	+17,32
Análisis de perfiles	11.224	68.524	+16,38
Historial clínico	10.895	119.955	+9,08
Gestión de actividades asociativas, culturales, recreativas, deportivas y sociales	5.563	61.473	+9,05
Educación	4.983	52.306	+9,53
Seguridad privada	4.585	30.558	+15,00
Servicios económicos-financieros y seguros	4.082	74.075	+5,51
Prestación de servicios de comunicaciones electrónicas	4.025	28.303	+14,22
Cumplimiento/incumplimiento de obligaciones dinerarias	3.945	54.555	+7,23
Fines estadísticos, históricos o científicos	3.921	93.266	+4,20
Guías/repertorios de servicios de comunicaciones electrónicas	2.128	19.428	+10,95
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	1.589	22.434	+7,08
Gestión de asistencia social	1.075	16.328	+6,58
Prestación de servicios de solvencia patrimonial y crédito	609	9.529	+6,39
Investigación epidemiológica y actividades análogas	578	9.905	+5,84
Prestación de servicios de certificación electrónica	506	4.178	+12,11
Otras finalidades	89.602	715.602	+12,52

DISTRIBUCIÓN DE FICHEROS SEGÚN EL SECTOR DE ACTIVIDAD

	2016	TOTAL	% VARIACIÓN 2016 TOTAL
Comunidades de propietarios	76.243	584.150	+13,05
Comercio	49.168	509.669	+9,65
Sanidad	34.665	322.395	+10,75
Turismo y hostelería	28.938	223.971	+12,92
Actividades inmobiliarias	12.598	129.279	+9,74
Educación	11.751	107.069	+10,98
Contabilidad, auditoría y asesoría fiscal	11.380	171.094	+6,65
Construcción	10.753	149.057	+7,21
Asociaciones y clubes	10.099	93.461	+10,81
Actividades jurídicas, notarios y registradores	8.187	101.984	+8,03
Transporte	7.955	92.333	+8,62
Comercio y servicios electrónicos	5.830	29.397	+19,83
Activ. de organizaciones empresariales, profesionales y patronales	5.206	28.247	+18,43
Activ. relacionadas con los productos alimenticios, bebidas y tabacos	5.145	52.364	+9,83
Servicios informáticos	4.976	60.179	+8,27
Agricultura, ganadería, explotación forestal, caza, pesca	4.380	47.495	+9,22
Actividades diversas de servicios personales	4.338	43.179	+10,05
Industria química y farmacéutica	4.007	57.661	+6,95
Seguros privados	2.744	36.349	+7,55
Actividades de servicios sociales	2.570	31.939	+8,05
Maquinaria y medios de transporte	2.521	48.615	+5,19
Producción de bienes de consumo	1.956	30.645	+6,38
Sector energético	1.560	25.791	+6,05
Servicios de telecomunicaciones	1.549	18.259	+8,48
Actividades relacionadas con los juegos de azar y apuestas	935	10.806	+8,65
Actividades políticas, sindicales o religiosas	915	22.335	+4,10
Publicidad directa	895	13.323	+6,72
Entidades bancarias y financieras	714	13.882	+5,14
Seguridad	684	9.334	+7,33
Organización de ferias, exhibiciones, congresos y otras activ. relac.	523	5.253	+9,96
Inspección técnica de vehículos y otros análisis técnicos	466	4.683	+9,95
Investigación y desarrollo (i+d)	466	5.369	+8,68
Activ. postales y de correo (oper. postales, serv. post., transport.).	392	3.723	+10,53
Selección de personal	328	5.170	+6,34
Solvencia patrimonial y crédito	61	1.195	+5,10
Mutualidades colaboradoras de los organismos de la seguridad social	13	849	+1,53
Otras actividades	145.957	1.226.585	+11,90

INSCRIPCIÓN DE TITULARIDAD PÚBLICA

DISTRIBUCIÓN DE FICHEROS POR TIPO DE ADMINISTRACIÓN

	2016	TOTAL
Administración General	956	8.931
Administración CC.AA.	1.499	30.386
Administración Local	3.941	94.334
Otras personas jurídico-públicas	495	28.241
TOTAL	**6.891**	**161.892**

DISTRIBUCIÓN DE FICHEROS DE LA ADMINISTRACIÓN GENERAL

	FICHEROS
Presidencia del Gobierno	10
Ministerio de Asuntos Exteriores y de Cooperación	556
Ministerio de Justicia	150
Ministerio de Defensa	2.159
Ministerio de Hacienda y Función Pública	463
Ministerio del Interior	236
Ministerio de Fomento	600
Ministerio de Educación, Cultura y Deporte	299
Ministerio de Empleo y Seguridad Social	2.034
Ministerio de Energía, Turismo y Agenda Digital	185
Ministerio de Agricultura y Pesca, Alimentación y Medio Ambiente	447
Ministerio de la Presidencia y para las Administraciones Territoriales	670
Ministerio de Economía, Industria y Competitividad	528
Ministerio de Sanidad, Servicios Sociales e Igualdad	594
TOTAL	**8.931**

DISTRIBUCIÓN DE FICHEROS DE TITULARIDAD PÚBLICA - CCAA

	2016	FICHEROS
Comunidad Autónoma de Andalucía	115	1.941
Comunidad Autónoma de Aragón	8	412
Comunidad Autónoma del Principado de Asturias	8	531
Comunidad Autónoma de Canarias	22	486
Comunidad Autónoma de Cantabria	2	237
Comunidad Autónoma de Castilla y León	17	886
Comunidad Autónoma de Castilla-La Mancha	33	940
Comunidad Autónoma de Cataluña	28	10.286
Comunidad de Madrid	755	10.020
Comunitat Valenciana	17	591
Comunidad Autónoma de Extremadura	–	521
Comunidad Autónoma de Galicia	9	340
Comunidad Autónoma de las Illes Balears	121	689
Comunidad Foral de Navarra	7	185
Comunidad Autónoma del País Vasco	143	1.328
Comunidad Autónoma de La Rioja	173	370
Comunidad Autónoma de la Región de Murcia	13	453
Ciudad Autónoma de Ceuta	21	71
Ciudad Autónoma de Melilla	7	99
TOTAL	**1.499**	**30.386**

DISTRIBUCIÓN DE FICHEROS DE TITULARIDAD PÚBLICA - ADMINISTRACIÓN LOCAL

	ENTIDADES	FICHEROS
Comunidad Autónoma de Andalucía	**873**	**11.336**
Almería	111	1.276
Cádiz	51	882
Córdoba	95	974
Granada	195	1.602
Huelva	88	1.290
Jaén	92	870
Málaga	113	2.405
Sevilla	128	2.037
Comunidad Autónoma de Aragón	**589**	**5.982**
Huesca	201	1.836
Teruel	78	552
Zaragoza	311	3.594
Comunidad Autónoma del Principado de Asturias	**96**	**1.836**
Comunidad Autónoma de Canarias	**119**	**2.075**
Las Palmas	53	1.036
Santa Cruz de Tenerife	66	1.039
Comunidad Autónoma de Cantabria	**72**	**981**
Comunidad Autónoma de Castilla y León	**1.223**	**10.882**
Ávila	105	1.242
Burgos	347	2.603
León	209	1.371
Palencia	122	1.312
Salamanca	94	573
Segovia	69	853
Soria	17	108
Valladolid	208	2.506
Zamora	52	314
Comunidad Autónoma de Castilla-La Mancha	**596**	**8.349**
Albacete	101	3.433
Ciudad Real	110	932
Cuenca	205	1.781
Guadalajara	45	632
Toledo	135	1.571

	ENTIDADES	FICHEROS
Comunidad Autónoma de Cataluña	**1.076**	**13.074**
Barcelona	445	5.935
Girona	232	3.011
Lleida	221	2.212
Tarragona	179	1.916
Comunidad de Madrid	**238**	**4.734**
Comunitat Valenciana	**531**	**7.563**
Alicante / Alacant	165	2.512
Castellón / Castelló	112	1.187
Valencia / València	255	3.864
Comunidad Autónoma de Extremadura	**341**	**8.245**
Badajoz	199	6.214
Cáceres	142	2.031
Comunidad Autónoma de Galicia	**334**	**4.923**
A Coruña	101	1.876
Lugo	71	921
Ourense	91	1.056
Pontevedra	71	1.070
Comunidad Autónoma de las Illes Balears	**86**	**1.694**
Comunidad Foral de Navarra	**262**	**3.049**
Comunidad Autónoma del País Vasco	**359**	**7.786**
Araba / Álava	66	764
Gipuzkoa	123	2.222
Bizkaia	170	4.800
Comunidad Autónoma de La Rioja	**44**	**454**
Comunidad Autónoma de la Región de Murcia	**54**	**1.371**

DISTRIBUCIÓN DE FICHEROS DE TITULARIDAD PÚBLICA - OTRAS PERSONAS JURÍDICO-PÚBLICAS

	TOTAL
Cámaras Oficiales de Comercio e Industria	495
Notariado	8.340
Universidades	1.552
Colegios profesionales	2.849
Otros	15.005
TOTAL	**28.241**

DISTRIBUCIÓN DE FICHEROS SEGÚN TIPOS DE DATOS - TITULARIDAD PÚBLICA

	2016	TOTAL
Datos especialmente protegidos (ideología, creencias, religión y afiliación sindical)	275	19.867
Otros datos especialmente protegidos (origen racial, salud y vida sexual)	1.251	39.531
Datos relativos a infracciones	679	27.888
Datos de carácter identificativo	6.891	161.892
Datos de características personales	3.440	83.879
Datos de circunstancias sociales	1.637	44.627
Datos académicos y profesionales	2.531	54.065
Detalles de empleo y carrera administrativa	1.980	48.073
Datos de información comercial	717	20.781
Datos económico-financieros	2.777	71.455
Datos de transacciones	835	30.791
Otros tipos de datos	1.034	24.469

DISTRIBUCIÓN DE FICHEROS CON DATOS SENSIBLES - TITULARIDAD PÚBLICA

	2016	TOTAL
Datos especialmente protegidos	**275**	**19.867**
Ideología	80	9.595
Creencias	56	8.726
Religión	82	9.134
Afiliación sindical	179	18.158
Otros datos especialmente protegidos	**1.251**	**39.531**
Origen racial	340	12.448
Salud	1.243	39.351
Vida sexual	102	9.746
Datos relativos a infracciones	**679**	**27.888**
Infracciones penales	260	18.544
Infracciones administrativas	650	26.968

DISTRIBUCIÓN DE FICHEROS SEGÚN SU FINALIDAD - TITULARIDAD PÚBLICA

	2016	TOTAL	% 2016/TOTAL
Procedimiento administrativo	1.773	52.285	+3,39
Educación y cultura	1.234	18.298	+6,74
Recursos humanos	848	27.909	+3,04
Gestión contable, fiscal y administrativa	580	23.255	+2,49
Servicios sociales	547	10.200	+5,36
Gestión de nómina	279	13.560	+2,06
Videovigilancia	269	3.127	+8,60
Gestión económica-financiera pública	250	7.061	+3,54
Seguridad y control de acceso a edificios	218	4.037	+5,40
Hacienda pública y gestión de administración tributaria	217	10.653	+2,04
Gestión sancionadora	207	6.218	+3,33
Prevención de riesgos laborales	206	3.896	+5,29
Trabajo y gestión de empleo	203	5.799	+3,50
Fines históricos, estadísticos o científicos	185	19.815	+0,93
Función estadística pública	178	12.755	+1,40
Gestión y control sanitario	137	3.888	+3,52
Padrón de habitantes	125	6.808	+1,84
Seguridad pública y defensa	121	4.108	+2,95
Publicaciones	113	2.862	+3,95
Justicia	87	10.654	+0,82
Historial clínico	75	2.125	+3,53
Actuaciones de fuerzas y cuerpos de seguridad con fines policiales	70	2.617	+2,67
Investigación epidemiológica y actividades análogas	47	1.546	+3,04
Prestación de servicios de certificación electrónica	38	1.734	+2,19
Gestión de censo promocional	28	1.072	+2,61
Otras finalidades	2.450	46.961	+5,22

TRANSFERENCIAS INTERNACIONALES DE DATOS

RESOLUCIONES DE AUTORIZACIÓN

		2000-2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	TOTAL AUT.
Estados Unidos (811)	EEUU	93	31	28	25	40	62	47	51	30	404	811
Iberoamérica (519)	Panamá	2	–	–	–	–	–	1	3	2	1	9
	Colombia	14	4	12	22	23	17	21	23	10	9	155
	Chile	17	1	8	9	7	1	–	–	2	2	47
	Uruguay	3	4	3	13	–	2	–	–	–	–	25
	Perú	9	4	19	20	30	23	23	5	5	6	144
	Guatemala	1	1	1	–	–	2	1	–	–	–	6
	Paraguay	2	4	4	1	4	2	–	–	–	–	17
	Brasil	1	3	–	1	2	2	3	1	1	5	19
	El Salvador	1	–	–	–	–	–	–	–	–	1	2
	Costa Rica	1	1	–	1	1	2	1	–	3	1	11
	Nicaragua	1	–	–	–	–	–	–	–	–	–	1
	México	–	3	8	20	12	14	7	2	6	9	81
	Ecuador	–	–	–	1	–	–	–	–	–	–	1
	Venezuela	–	–	–	–	–	–	–	1	–	–	1
India (310)	India	9	30	28	14	29	27	42	53	39	39	310
Otros países (378)	Marruecos	8	3	8	7	4	10	13	9	7	7	76
	Singapur	4	–	–	1	2	4	1	6	3	7	28
	Japón	2	–	1	1	3	4	7	7	1	7	33
	Malasia	3	–	3	–	–	2	1	5	2	4	20
	Tailandia	2	–	–	–	–	1	–	–	–	–	3
	Filipinas	4	5	4	3	5	9	8	5	6	5	54
	China	2	3	3	1	14	4	6	–	2	8	43
	Hong Kong	1	–	1	1	–	1	2	–	2	5	13
	Egipto	1	–	–	–	–	1	1	–	1	–	4
	Nigeria	1	–	–	–	–	–	–	–	–	–	1
	Túnez	1	–	–	2	–	3	–	–	2	1	9
	Sudáfrica	–	3	–	–	–	3	–	1	1	–	8
	Australia	1	–	7	–	–	3	4	3	1	8	27
	Canadá	1	–	–	–	–	1	–	2	–	2	6
	Rep. Bielorrusa	–	3		–	–	–	–	–	–	–	3
	Mónaco	–	–	1	–	–	–	–	–	–	–	1
	Israel	–	–	1	6	2	–	–	–	–	–	9

		2000-2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	TOTAL AUT.
Otros países (378)	Vietnam	–	–	–	3	–	1	–	–	–	–	4
	Barbados	–	–	–	3	–	–	–	–	–	–	3
	Andorra	–	–	–	1	–	–	–	–	–	–	1
	Mauricio	–	–	–	–	1	–	–	–	–	–	1
	Kenia	–	–	–	–	–	1	–	–	–	–	1
	Serbia	–	–	–	–	–	1	–	–	1	–	2
	Taiwan	–	–	–	–	–	2	–	1	–	1	4
	Croacia	–	–	–	–	–	1	–	–	–	–	1
	Turquía	–	–	–	–	–	1	–	–	–	1	2
	Ucrania	–	–	–	–	–	1	–	–	–	–	1
	Bermudas	–	–	–	1	–	1	–	–	–	–	2
	Nueva Zelanda	–	–	–	–	–	1	–	1	–	–	2
	Rep. de Corea	–	–	–	–	–	1	–	1	–	–	2
	Federación Rusa	–	–	–	–	–	1	1	–	–	1	3
	Emiratos Árabes	–	–	–	–	–	–	1	–	–	2	3
	Arabia Saudí	–	–	–	–	–	–	–	–	1	4	5
	Indonesia	–	–	–	–	–	–	–	–	–	1	1
	Puerto Rico	–	–	–	–	–	–	–	–	–	2	2
Internacional (45)	Internacional	–	–	–	3	1	3	8	2	8	20	45
	Solicitudes presentadas	314	137	166	197	201	224	192	187	128	737	2.483
	Archivadas	120	42	24	31	16	52	15	26	29	91	446
	Total Autorizaciones	**174**	**103**	**128**	**155**	**175**	**177**	**170**	**150**	**108**	**499**	**1.838**

FICHEROS INSCRITOS CON TRANSFERENCIAS INTERNACIONALES SEGÚN TITULARIDAD

	FICHEROS
Titularidad privada	17.407
Titularidad pública	8.414
TOTAL	**25.821**

EVOLUCIÓN DE LAS AUTORIZACIONES DE TRANSFERENCIAS INTERNACIONALES SEGÚN LAS GARANTÍAS APORTADAS (TIPO DE CONTRATO Y NORMAS CORPORATIVAS VINCULANTES –BCR–)

	2010	2011	2012	2013	2014	2015	2016
2001/497/CE[1]	80	112	167	195	226	246	379
2002/16/CE[2] – 2010/87/UE[3]	475	619	735	861	966	1.037	1.364
Normas Corporativas Vinculantes (BCR)	–	1	8	17	23	34	61
Cláusulas Encargado-Subencargado[4]	–		2	9	16	22	32
Contrato ad hoc	–		–	–	1	1	2

[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	2016	TOTAL
Ficheros	1	1.561	1.625	20	32	2.788
Responsables	1	454	437	8	26	833

TRANSFERENCIAS INTERNACIONALES DE DATOS AMPARADAS EN LA AUTORIZACIÓN DE TRANSFERENCIAS INTERNACIONALES BASADAS EN CONTRATO «AD HOC»

	2014	2015	2016	TOTAL
Ficheros	59	27	543	629
Responsables	14	9	146	169

ACTUACIONES COMO AUTORIDAD CORREVISORA DE NORMAS CORPORATIVAS VINCULANTES (BCR)

	2010	2011	2012	2013	2014	2015	2016	TOTAL
Revisión BCR'S	1	4	7	3	9	10	8	42

EVOLUCIÓN DE LA INSCRIPCIÓN DE LOS FICHEROS DE VIDEOVIGILANCIA*

AÑO DE INSCRIPCIÓN	TITULARIDAD PRIVADA	TITULARIDAD PÚBLICA
1994-2009	33.181	505
2010	29.389	748
2011	33.849	436
2012	33.524	532
2013	36.514	418
2014	37.862	457
2015	41.183	438
2016	50.630	328
TOTAL	**296.132**	**3.862**

* 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	2015	2016	% VARIACIÓN 2015-2016
Otras actividades	73.242	88.074	+20,26
Comercio	57.691	66.918	+15,99
Turismo y hostelería	29.347	35.033	+19,38
Comunidades de propietarios	21.354	27.009	+26,48
Sanidad	13.827	16.583	+19,93
Activ. relacionadas con los productos alimenticios, bebidas y tabacos	4.962	6.025	+21,42
Construcción	4.797	5.457	+13,76
Transporte	4.200	4.878	+16,14
Industria química y farmacéutica	3.766	4.172	+10,78
Actividades inmobiliarias	3.249	3.925	+20,81
Educación	3.217	3.773	+17,28
Maquinaria y medios de transporte	2.543	2.880	+13,25
Contabilidad, auditoría y asesoría fiscal	2.361	2.788	+18,09
Agricultura, ganadería, explotación forestal, caza, pesca	2.279	2.736	+20,05
Servicios informáticos	2.426	2.727	+12,41
Asociaciones y clubes	2.135	2.483	+16,30
Actividades relacionadas con los juegos de azar y apuestas	2.079	2.305	+10,87
Sector energético	1.942	2.127	+9,53
Seguridad	1.794	1.937	+7,97
Producción de bienes de consumo	1.645	1.853	+12,64
Actividades diversas de servicios personales	1.435	1.777	+23,83
Actividades jurídicas, notarios y registradores	1.252	1.552	+23,96
Servicios de telecomunicaciones	1.323	1.467	+10,88
Actividades de servicios sociales	1.221	1.410	+15,48
Comercio y servicios electrónicos	1.059	1.400	+32,20
Activ. de organizaciones empresariales, profesionales y patronales	887	1.172	+32,13
Entidades bancarias y financieras	824	983	+19,30
Seguros privados	537	632	+17,69
Actividades políticas, sindicales o religiosas	496	594	+19,76
Inspección técnica de vehículos y otros análisis técnicos	317	390	+23,03
Publicidad directa	247	293	+18,62
Organización de ferias, exhibiciones, congresos y otras activ. relac.	210	232	+10,48
Investigación y desarrollo (i+d)	194	216	+11,34
Activ. postales y de correo (oper. postales, serv. post., transport.	166	214	+28,92
Selección de personal	55	65	+18,18
Mutualidades colaboradoras de los organismos de la seguridad social	29	30	+3,45
Solvencia patrimonial y crédito	16	22	+37,50
TOTAL	**249.124**	**296.132**	**+18,87**

PRESENCIA INTERNACIONAL DE LA AEPD EN 2016

REUNIÓN	NÚMERO DE REUNIONES	LUGAR
Sesiones Plenarias del Grupo de Trabajo del artículo 29 (GT29)	5	Bruselas (Bélgica)
Plenario extraordinario FabLab y GDPR Workshop	1	
Subgrupo Futuro de la privacidad (FoP)	4	
Subgrupo Futuro de la privacidad. Workshops: Mutual assistance and joint operations workshop OSS and Consistency workshop Administrative fines workshop	1	
Subgrupo Cooperación	5	
Tecnología (TS)	4	
Subgrupo Fronteras, Viajeros y Cumplimiento (BTLE)	3	
Subgrupo Disposiciones Clave	3	
Subgrupo E-Government	3	
Subgrupo Enforcement	1	
Autoridades Comunes de Control		
Reunión JSB EUROPOL	2	Bruselas (Bélgica)
Grupos de Supervisión Coordinada de los sistemas VIS, SIS II y EURODAC	2	
Comité Schengen	1	
Evaluación Schengen	1	Zagreb (Croacia)
CIS, JSB, JSA Customs	1	Bruselas (Bélgica)
EUROJUST –Inspección–	1	La Haya (Países Bajos)

OTRAS REUNIONES	FECHA	LUGAR
Otras reuniones		
Nueva política de privacidad de Google	4 y 5 de febrero	París (Francia)
Workshop on Data Analytics	16 de febrero	Bruselas (Bélgica)
IAPP Brussels. GDPR Comprehensive Brussels	22 y 23 de febrero	Bruselas (Bélgica)
Reunión REPER traducción Reglamento	7 de marzo 18 de marzo	Bruselas (Bélgica)
CIPL GDPR Project	15 y 16 marzo 19 de septiembre	Ámsterdam (Países Bajos) París (Francia)
Meeting with CNA review of e-Privacy Directive	19 de abril	Bruselas (Bélgica)
Conferencia de primavera de Autoridades Europeas de Protección de Datos	26 y 27 de mayo	Budapest (Hungría)
Taller «Privacidad y acción humanitaria»	16 y 17 de junio	La Antigua (Guatemala)
Reunión grupo redacción «Reglas procedimiento interno EDPB»	12 de julio 14 de septiembre	Bruselas (Bélgica)
Plan de Oficio «Visados» (Casablanca)	18 al 23 de septiembre	Casablanca (Marruecos)
38.ª Conferencia Internacional de Autoridades de Protección de Datos	17, 18, 19 y 20 de octubre	Marrakech (Marruecos)
40th DPO´s - EDPS Network meeting	26 de octubre	Alicante (España)
Meeting on the Right to de-listing	30 de noviembre	París (Francia)
Grupo de telecomunicaciones de Berlín	22 de noviembre	Berlín (Alemania)

SECRETARÍA GENERAL

GESTIÓN DE RECURSOS HUMANOS

	DOTACIÓN 31/12/2016	CUBIERTOS 31/12/2016
Funcionarios	159	143
Laborales	4	4
Laborales fuera de Convenio	2	2
Alto cargo	1	1
	166	**150**

MUJERES	80
HOMBRES	70

NIVEL	30	29	28	26	24	22	20	18	17	16	15	14
Efectivos	6	2	21	44	0	20	3	12	2	7	12	14

GRUPO	A1	A2	C1	C2
Efectivos	30	43	26	44

EVOLUCIÓN DEL PRESUPUESTO

	CRÉDITO EJERCICIO 2013	CRÉDITO EJERCICIO 2014	CRÉDITO EJERCICIO 2015	CRÉDITO EJERCICIO 2016
CAPITULO I	6.672.660	6.672.660	7.295.520	7.305.820
CAPITULO II	5.024.000	5.224.000	5.224.000	4.896.060
CAPITULO III	432.450	232.450	232.450	232.450
CAPITULO IV	–	–	–	267.940
CAPITULO VI	1.372.160	1.316.000	1.316.000	1.316.000
CAPITULO VIII	22.800	22.800	22.800	22.800
TOTAL	**13.524.070**	**13.467.910**	**14.090.770**	**14.101.070**

Los datos de todos los capítulos son siempre referidos a créditos definitivos.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

MEMORIA AEPD 2016

ISSN 2254-691X