agencia española protección datos

MEMORIA AEPD 2019

prólogo

Me complace un año más presentar la Memoria anual de la Agencia Española de Protección de Datos, que recoge en detalle las actividades realizadas por este organismo durante 2019 en todas sus áreas, un análisis de las tendencias más relevantes, una exposición y valoración de los retos presentes y futuros y una evaluación de las iniciativas puestas en marcha durante el año para dar respuesta al cambio de modelo, tanto interno como externo, que ha supuesto el Reglamento General de Protección de Datos (RGPD).

Como se explica en páginas posteriores, el Plan Estratégico -presentado al inicio de mi mandato en 2015- ha finalizado en este 2019 con 150 acciones que han tratado de dar respuesta a un nuevo escenario normativo y contribuir a acompañar, facilitar y preparar a los diferentes actores implicados. La visión de la Agencia que incorporaba el Plan se ha proyectado este 2020 en la presentación del Marco de Actuación en materia de Responsabilidad Social y Sostenibilidad, que incluye un plan de acción con más de 100 iniciativas para los próximos cinco años, todas ellas alineadas con los ODS de la Agenda 2030. Esta decisión supone asumir unos compromisos adicionales con los ciudadanos, además de un cambio de cultura organizativa y de gestión interna.

En esta línea, uno de los hitos más relevantes en el plano preventivo por su impacto social ha sido el lanzamiento del Canal prioritario para solicitar la eliminación urgente de contenidos violentos o sexuales en internet que, acompañado de una campaña de concienciación a la que han colaborado de forma desinteresada numerosos actores públicos y privados, ha posicionado a la AEPD como la única autoridad europea de protección de datos que ofrece este servicio pionero para combatir la violencia de género y, más ampliamente, la llamada violencia digital, que afecta especialmente a las mujeres y a los jóvenes en el entorno escolar.

Esta acción ha estado acompañada de múltiples iniciativas en diversos ámbitos, tanto para promover la concienciación como para ayudar a las administraciones públicas, empresas y, sobre todo, pymes y micropymes a cumplir con las previsiones del RGPD. En las páginas posteriores de esta Memoria podrán profundizar con detalle en las iniciativas lanzadas y las acciones realizadas por la Agencia para tratar de facilitar e impulsar el cumplimiento de la normativa. También es importante hacer mención al trabajo llevado a cabo por responsables y encargados para la aplicación del principio de responsabilidad proactiva. Este año es el primero en el que la aplicación del Reglamento cubre su totalidad, y es importante reseñar el importante papel que juega en el cumplimiento la figura del Delegado de Protección de Datos. Al cierre del ejercicio, se habían notificado a la Agencia un total de 50.326 Delegados de Protección de Datos.

Siguiendo con cifras, el Gabinete jurídico de la Agencia ha respondido 152 consultas y realizado 76 informes preceptivos. En este punto, merece una mención específica en este prólogo la Circular que lanzó la Agencia sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral. El texto de la Circular fijó los criterios de actuación en la aplicación de la normativa de protección de datos al amparo del artículo 58 bis de la LOREG, con el marco del RGPD y conforme a lo establecido en la Constitución Española. La Circular, que fijaba obligaciones adicionales, mantuvo una interpretación restrictiva de la modificación de la LOREG. Con posterioridad, el Pleno del Tribunal Constitucional declaró

inconstitucional, por unanimidad, el artículo 58.bis.1 de la LOREG.
Por otro lado, el Reglamento también ha supuesto modificaciones importantes en la forma de trabajar de las Autoridades. Ello se aprecia de manera significativa en todas las áreas de la Agencia, potenciando la parte preventiva y de concienciación sin dejar de lado, como no podía ser de otra forma, las funciones de supervisión y control.

En 2019 se han presentado ante la Agencia 11.590 reclamaciones, un 11% menos que el año anterior. En este descenso hay que tener en cuenta el número de reclamaciones que se presentaban ante la Agencia con anterioridad al importante incremento experimentado en 2018 tras la amplia difusión del RGPD. En cambio, los procedimientos transfronterizos han subido en 2019 un 33% y las notificaciones de brechas de seguridad trasladadas a inspección han crecido de las 16 de 2018 a las 79 de 2019, lo que supone un incremento de casi un 400%. En el caso de las reclamaciones, es importante hacer una referencia a los traslados, un trámite promovido por el RGPD y la LOPDGDD que tiene como objetivo facilitar la resolución amistosa de reclamaciones. Los traslados permiten que estas pueden resolverse más rápidamente, ofreciendo una respuesta satisfactoria al ciudadano en menor tiempo.

En cuanto a los procedimientos transfronterizos, hay que destacar que los casos liderados por la AEPD como autoridad principal han pasado de 15 en 2018 a 21 de 2019 y, en la cooperación como autoridad interesada, se ha pasado de 229 a 565 casos, un incremento del 147%. Asimismo, las entradas recibidas por el procedimiento de cooperación han ascendido hasta las 1.052, con un crecimiento del 68%.

Con carácter general, en cuanto a los tiempos medios de tramitación de actuaciones de cada una de las fases relacionadas con la gestión de las reclamaciones, se puede observar una disminución de un 55% en los tiempos medios. El personal de la Agencia ha hecho un gran esfuerzo para intentar mantener y en algunos casos mejorar esos tiempos medios de tramitación, a la vez que se han puesto en marcha iniciativas novedosas y que requieren de respuesta urgente como el Canal prioritario, o potenciando además el lanzamiento de guías, herramientas y otras soluciones para concienciar y ayudar tanto a los ciudadanos como a aquellos que tratan datos. En este entorno debo destacar también la Unidad de Evaluación y Estudios Tecnológicos, que realiza una importante labor de prospección en un entorno cambiante en el que es imprescindible seguir de cerca los nuevos desarrollos tecnológicos y que va a permitir, junto al resto de unidades, que la Agencia continúe estando en la vanguardia europea de las autoridades de protección de datos.

Para finalizar es imprescindible hacer referencia a áreas menos susceptibles de cuantificación, como aquellas que están orientadas a la concienciación de la ciudadanía y de los sujetos obligados o al desarrollo y puesta en marcha de nuevos proyectos. La parte sancionadora, aunque necesaria, no puede representar por sí sola a la Agencia Española de Protección de Datos. Este organismo ha trabajado de forma intensa en los últimos años para potenciar la parte preventiva, ofreciendo colaboración, formación y soluciones en múltiples ámbitos. Estoy convencida de que la verdadera protección de datos sólo puede conseguirse si se trabaja en ambos planos, y es una tarea con la que estamos firmemente comprometidos.

Mar España Martí
Directora de la Agencia Española de Protección de Datos

índice

Memoria 2019

Anexo. La Agencia en cifras

1. Principales hitos del 2019

El año 2019 ha supuesto la finalización del Plan estratégico lanzado en 2015 por la Agencia y en el que se establecía una duración de cuatro años. Este Plan, que va a tener continuidad en el Marco de sostenibilidad ya presentado por la AEPD, supuso que, por primera vez en la historia de la Agencia, se pudiesen recoger de forma sistemática las líneas de su actividad con una programación temporal y una definición de sus objetivos, posibilitando su evaluación tanto dentro de la organización como externamente. Y, lo que es más importante, ha sido el principal instrumento con el que ha contado la AEPD para llevar a cabo su adaptación al nuevo marco europeo.

Cuando se diseñó el Plan estratégico, en noviembre de 2015, tanto en lo que se refiere a la estructura del plan, como al conjunto de las 113 acciones que inicialmente lo integraron (finalmente han sido 150), se tuvo muy presente la aprobación del nuevo marco europeo de protección de datos que se produciría unos meses después, el 25 de mayo de 2016. En esa medida, el Plan estratégico anticipaba y sentaba las bases de lo que iba a resultar finalmente el nuevo escenario, contribuyendo a acompañar, facilitar y preparar con antelación a los diferentes actores implicados. Era fundamental prever esta nueva situación y sus posibles efectos, y para ello se aprobó el Plan, cuyo balance, cuando han finalizado los cuatro años de vigencia del mismo, ha sido positivo, tal como expondremos de forma detallada en el epígrafe correspondiente de esta Memoria.

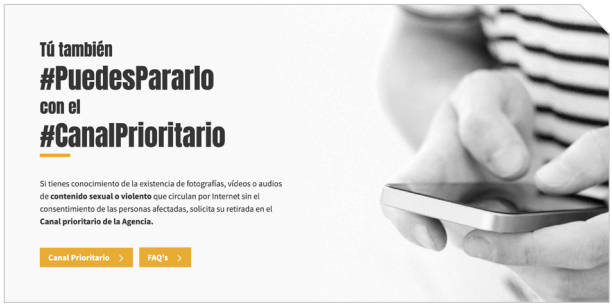
En este apartado de la Memoria se va llevar a cabo un balance global del cumplimiento del Plan estratégico con las principales iniciativas promovidas durante cuatro años, incluyendo en relación con cada uno de los cinco ejes que lo integran aquella o aquellas que, por su mayor impacto o su trascendencia social, se han considerado oportuno destacar. Al respecto, cabe señalar que la gran mayoría de las medidas previstas para el ejercicio 2019 tenían un carácter plurianual, es decir, eran continuidad de actuaciones iniciadas en períodos anteriores, completándose durante dicho año, motivo por el cual la evaluación de su cumplimiento se ha llevado a cabo en el marco de la evaluación final de la totalidad del plan. En todo caso, a lo largo de la presente Memoria se encontrarán referencias detalladas a las diferentes medidas, bien en el apartado correspondiente al balance global del Plan, como en otras partes de la Memoria.

Ahora bien, como se ha señalado con anterioridad, simultáneamente a la finalización del Plan estratégico se ha abierto una etapa nueva en la Agencia con la aprobación, en el mes de marzo, del **Marco de Actuación en materia de Responsabilidad Social y Sostenibilidad**, acompañado de un plan de acción con más de 100 iniciativas para los próximos cinco años, todas ellas alineadas con los Objetivos de Desarrollo Sostenible de la Agenda 2030. Esta decisión supone asumir unos mayores compromisos con los ciudadanos y con otros agentes (empresas, Administraciones Públicas, profesionales, etc). Viniendo de un organismo público que tutela un derecho fundamental, dicha decisión constituye una evolución añadida del proceso de garantía de este derecho

Este nuevo paso implica además un cambio de cultura organizativa y de los modos de gestión interna ya que, desde el mismo momento en que se está definiendo cualquier iniciativa, se exige tener en cuenta criterios de responsabilidad social en consonancia con alguno de los ODS de la Agenda 2030. En definitiva, supone una nueva forma de planificar y evaluar el impacto de las medidas a adoptar y sus potenciales beneficiarios, cuyos efectos se empezarán a apreciar en los próximos años. Es cierto que ello implica una mayor complejidad en la gestión y un mayor esfuerzo, pero sus objetivos han pasado a formar parte de los compromisos éticos de esta institución.

En este ámbito, a lo largo de 2019 hay que reseñar especialmente el conjunto de medidas que desde la Agencia se han impulsado en relación con la igualdad de género. Y entre ellas, destaca, como la más relevante, la creación del Canal

prioritario para solicitar la eliminación urgente de contenidos violentos o sexuales en internet, que ha tenido una acogida muy favorable y cuya difusión se está potenciando mediante una campaña de concienciación masiva puesta en marcha a principios de 2020. Esta iniciativa ha posicionado a la AEPD como autoridad de referencia a nivel europeo y mundial a la hora de combatir la lacra de la violencia de género, y, más ampliamente, la llamada "violencia digital" que afecta especialmente a las mujeres y a los jóvenes en el entorno escolar. Pero, en dicho ejercicio, ha habido más medidas en esta misma dirección, como son, entre otras, la creación de una web sobre violencia de género; la aprobación del Protocolo de la AEPD contra el acoso sexual y de las recomendaciones a empresas sobre obligaciones en caso de violencia digital o el impulso de un nuevo premio sobre Protección de Datos y Violencia de género. A cada una de ellas se aludirá con detalle en este apartado de la Memoria.



Otro gran hito del año ha sido el primer aniversario, en mayo, de la plena entrada en vigor del Reglamento europeo, y, en diciembre, de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), cuyo balance se presentó en el acto celebrado el 5 de diciembre en la sede española de la Comisión Europea.

Al respecto, hay que destacar, en primer término, las iniciativas puestas en marcha para concienciar a los menores en su entorno educativo sobre el uso responsable de internet, colaborando con las Administraciones Educativas en la puesta a disposición de materiales que ayuden en la prevención, detección y erradicación de conductas violentas en el entorno escolar. En particular, la Agencia se ha implicado especialmente en el desarrollo de la previsión del artículo 83 de la Ley Orgánica 3/2018, que contiene la obligación de que las Administraciones educativas incluyan en el diseño del bloque de asignaturas de libre configuración la competencia digital, así como los elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la Red. En este sentido, bajo la coordinación del Ministerio de Educación, a través del INTEF, con la aportación de muy diversos actores, públicos y privados (AEPD, INCIBE, Facebook, Fundación La Mutua, etc.), se han presentado los materiales curriculares -a través de la Web AseguraTIC- que se han puesto a disposición de las Autoridades educativas para que sirvan de base para el diseño de los correspondientes programas y materiales.

Asimismo, en esta misma perspectiva preventiva, debe destacarse el amplio número de guías y herramientas que la Agencia ha puesto a disposición del sector público, privado y de la ciudadanía para ayudar en la garantía y sensibilización del valor de la privacidad y la importancia del tratamiento de los datos personales, en especial, los nuevos derechos que recoge el Reglamento, ofreciéndoles una información completa y accesible sobre la forma más efectiva para ejercerlos. En particular, durante 2019 destacan las Guías para pacientes y usuarios de la sanidad y de Privacidad desde el diseño y para la protección de datos para operadores de drones, junto con las herramientas de análisis de riesgos y de evaluación de impacto en protección de datos (EIPD) para pymes (Gestiona_EIPD) y para Administraciones Públicas (ASSI). Y han quedado prácticamente ultimadas, para su presentación en 2020, las Guías sobre protección de datos personales en el ámbito de las relaciones laborales, de Administración Electrónica, de cookies y de instituciones y profesionales sanitarios, así como la adaptación de la herramienta Facilita_RGPD al ámbito de los emprendedores (Facilita_EMPRENDE).

Otro de los ámbitos donde la Agencia ha encauzado su faceta preventiva, para tratar de ofrecer una mayor protección de los derechos, ha sido mediante la implantación de nuevos mecanismos para la resolución extrajudicial de las reclamaciones en ámbitos de fuerte

impacto ciudadano. Entre ellos, hay que aludir especialmente al arbitrado a través de la intervención del Delegado de Protección de Datos. Por esta vía, en 2019 se ha dado traslado de las reclamaciones presentadas al responsable o al DPD para su resolución en el plazo de un mes, garantizando así de forma más rápida y efectiva los derechos de los interesados y evitando la iniciación de procedimientos de infracción. En todo caso, la Agencia mantiene la potestad de supervisión continua si una entidad incumple de manera continuada.

El otro gran reto que ha planteado el Reglamento europeo es el cambio del modelo de cumplimiento normativo, con la correlativa exigencia para las Autoridades de control de velar principalmente por la aplicación del principio de responsabilidad proactiva por parte de los responsables y encargados, con especial incidencia en los principios de privacidad desde el diseño y por defecto y en el pleno desarrollo de la figura del Delegado de Protección de Datos, entre otras medidas. Así, a cierre del ejercicio, se habían notificado a la Agencia un total de 50.326 Delegados de Protección de Datos (44.069 del sector privado y 6.257 del sector público).

En esta misma perspectiva proactiva, ha de destacarse la importante función de prospección desarrollada por la Unidad de Evaluación y Estudios Tecnológicos, cuya creación, hace tres años, ha demostrado su eficacia, hasta el punto de consolidarse hoy día como una de las unidades estratégicas de la Agencia. Entre sus actividades, destacan varios estudios y colaboraciones con relación a la protección de datos en los dispositivos móviles y los servicios de Internet en general. Las conclusiones obtenidas han evidenciado que existen importantes carencias en el cumplimiento normativo de los tratamientos de datos que se realiza a través de smartphones. Los problemas se centran en la falta de transparencia en de los momentos en que se realizan la recogida de datos y en los mecanismos de seguimiento de los usuarios, una información incompleta sobre los tratamiento realizados, un esquema de permisos para comunicación de datos personales entre aplicaciones que permite el filtrado de datos a terceros, la existencia de numerosas aplicaciones preinstaladas en los dispositivos que no pueden ser controladas por el usuario o el empleo de librerías por parte de desarrolladores de aplicaciones que no cumplen con las medidas de privacidad desde el diseño o por defecto. Este problema no se acota a intervinientes puntuales, sino que afecta a la globalidad del modelo de negocio basado en tecnologías móviles: fabricantes, distribuidores, operadoras, desarrolladores y proveedores de servicios a nivel global. A través de sus publicaciones la AEPD ha emitido recomendaciones para aplicar los principios de trasparencia y responsabilidad proactiva del RGPD, en particular, medidas de privacidad desde el diseño y por defecto. Además, ha trasladado las conclusiones obtenidas a los intervinientes españoles en dicho modelo, a los usuarios con indicaciones específicas para gestionar su privacidad, como finalmente al Comité Europeo de Protección de Datos para que se tomen acciones en integrales que realmente preserven los derechos de los ciudadanos.

En otro apartado de esta Memoria se expondrán de forma minuciosa las numerosas actividades emprendidas por la UEET durante el presente año.

Finalmente, se incluye una referencia a la transformación operada por la Agencia en su estructura y su modo de funcionamiento interno para adaptarse a los importantes cambios introducidos por el Reglamento europeo en cuanto al modelo de supervisión. Un ejemplo de ello es el caso de los procedimientos transfronterizos, donde las diversas Autoridades europeas de protección de datos, desde su condición de Autoridades principales o interesadas, deben necesariamente cooperar en la aplicación de la normativa de protección de datos. En este ámbito, destaca la labor del Comité Europeo de Protección de Datos (EDPB, por sus siglas en inglés) que, transcurrido su primer año de su funcionamiento, constituye una pieza clave para asegurar la aplicación coherente del Reglamento y canalizar la cooperación entre las Autoridades de protección de datos. De todo ello, y del papel desempeñado por la Agencia Española durante el primer año de funcionamiento del Comité, se informará con detalle en la presente Memoria.

2. Plan Estratégico

2.1 La ejecución del Plan Estratégico

El año 2019 se corresponde con él último año de ejecución del Plan Estratégico, y, por tanto, es necesario hacer balance final de lo que ha supuesto para la Agencia sus cuatro años de aplicación y cuáles han sido las iniciativas realizadas.

Por lo que se refiere a las cifras, aparecen con detalle en la parte final de esta Memoria, así como en el sitio web de la AEPD dedicado al Plan Estratégico. Como se ha señalado, el balance global ha sido positivo, al haberse pasado de una previsión inicial de 113 acciones a las 150 finales, lo que supone un incremento de casi un 33% sobre los objetivos fijados en el momento de aprobarse el Plan.

En cuanto a su grado de cumplimiento, si bien el número de iniciativas finalmente ejecutadas, sumadas las previstas inicialmente (113) y las incorporadas posteriormente (39), ha sido de 152, a ellas hay que restarle las 2 iniciativas que, por los motivos que luego se explicitarán, no han podido ejecutarse, lo que da un total de 150 iniciativas finalizadas en el período 2015-2019.

Como grandes cifras de este balance final del Plan Estratégico, pueden destacarse las siguientes:

1. **Creación del Canal Prioritario para solicitar la eliminación urgente de contenidos violentos o sensibles en internet**

- 8.000.000 de jóvenes y las mujeres víctimas de violencia de género como potenciales beneficiados

2. **Herramienta FACILITA_RGPD**

- Más de 800.000 pymes y autónomos han accedido a ella
- Más de 200.000 empresas han obtenido los documentos mínimos para el cumplimiento

3. **Materiales curriculares para la educación digital en planes de enseñanza**

- 8.000.000 de alumnos y sus familias como potenciales beneficiados

4. **Programa de Teletrabajo para conciliar la vida laboral, personal y familiar de los empleados**

- El 60% de los empleados de la AEPD se han acogido a este programa

5. **Promoción y apoyo a los Delegados de Protección de Datos**

- Casi 50.000 Delegados de Protección de Datos notificados a la AEPD
- 200 Delegados de Protección de Datos en el Esquema AEPD/ENAC

6. **Creación de la Unidad de Evaluación y Estudios Tecnológicos**

- Análisis de 1.700 brechas de seguridad

7. **Procedimientos de resolución voluntaria (mediación) de las reclamaciones.**

- Más de 47.000 reclamaciones recibidas, con un incremento del 20% desde el RGPD
- Resueltas favorablemente el 74% de los 267 procedimientos de mediación con operadoras de telecomunicaciones desde enero de 2018
- Un 33% de las reclamaciones recibidas han sido gestionadas por los DPD
- Un 45% resueltas por la empresa reclamada en menos de 90 días

8. **Refuerzo de la información a los ciudadanos para mejorar el conocimiento de sus derechos y a los responsables y profesionales para facilitar el cumplimiento.**

- Más de 1.000.000 de usuarios inscritos en la Lista Robinson, el 50% desde el RGPD
- 26.493.400 usuarios únicos visitaron www.aepd.es
- 1.800.000 de consultas recibidas en el Servicio de Atención al Ciudadano

  4.359 de consultas de alumnos, profesores y padres recibidas en el Canal Joven
- 1.500.000 consultas recibidas en la sección de preguntas frecuentes (FAQS) de la Sede Electrónica, la mitad en 2018
- 5.500 consultas de responsables, profesionales y DPD se han recibido en el canal INFORMA_RGPD desde marzo de 2018
- Más de 3.000.000 de descargas de las principales Guías para ciudadanos y responsables.
- Casi 4.000 actuaciones del Gabinete de Prensa para informar y atender a medios de comunicación
- 155.147.943 de impactos de la campaña de publicidad del RGPD declarada como servicio público por la CNMC

9. **Guías y herramientas.**

- 76 guías y herramientas para ciudadanos y responsables

10. **Difusión y formación en el RGPD entre Administraciones Públicas y sus empleados.**

- Más de 200 eventos públicos de información sobre el RGPD
- 5.000 empleados públicos beneficiarios de los programas de formación en el RGPD

Expuestas las cifras más significativas del Plan, procede a continuación enumerar las iniciativas más destacadas durante estos cuatro años, en relación con cada uno de los cinco ejes en que se estructuró el mismo.

Eje 1.
Prevención para una protección más eficaz

Una parte significativa de las acciones previstas en el Plan, tanto en su previsión inicial como en su desarrollo posterior, ha tenido como objetivo fundamental promover entre los ciudadanos una cultura de protección de datos y reforzar progresivamente sus derechos para garantizar un mayor control de sus datos personales.

Ello se ha traducido en un importante esfuerzo desplegado por la Agencia en diseñar el mayor número posible de guías, herramientas y materiales para dar a conocer a los ciudadanos sus derechos, en especial a raíz de la entrada en vigor del nuevo marco europeo que los refuerza.

Uno de los aspectos en los que más se ha trabajado en estos años ha sido en la **protección de los derechos de los menores**, especialmente en el campo educativo. Así, desde los inicios del Plan, con fecha 13 de octubre de 2015, se suscribió un Convenio Marco de colaboración con el Ministerio de Educación, con la inclusión de actuaciones dirigidas a la educación y concienciación de los menores sobre el valor de la privacidad y la importancia del uso de la información personal, especialmente en internet, mediante la colaboración en la elaboración de materiales y recursos y su difusión. Asimismo, en este mismo marco de colaboración, se han cuidado especialmente las relaciones con las Comunidades Autónomas a través de la participación en la Comisión General de Directores Generales de Educación preparatoria de la Conferencia Sectorial de Educación, donde la Agencia ha informado de distintas iniciativas.

Este convenio se ha renovado a finales de 2019, con el fin de seguir impulsando estas relaciones. Un ejemplo de ello es la iniciativa, coordinada por el Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF), para la elaboración de los materiales curriculares que las Administraciones educativas deberán incluir en el diseño del bloque de asignaturas de libre configuración que se detallará posteriormente.

En particular, los recursos y materiales más destacados en este ámbito han sido:

- Guía de protección de datos para Centros Educativos
- Videos Tú controlas en internet
- Infografía Protege sus datos en la vuelta a clase
- Videos Historias para concienciar a los menores
- Videos Talleres para familias sobre los menores y su cibermundo
- Guía Se legal en internet
- Guía Enséñales a ser legales en internet
- Guía No te enredes en internet
- Guíales en internet
- Informe sobre la utilización por parte de profesores y alumnos de apps en la nube

De otra parte, hay que destacar la puesta en marcha del canal de atención a los menores, profesores y padres, en el que se han atendido un gran número de consultas de parte de toda la comunidad educativa. Entre las consultas más frecuentes, cabe destacar las siguientes:

- La difusión de imágenes de los menores a través de Internet por centros educativos, clubes deportivos, federaciones deportivas o asociaciones.
- La grabación de imágenes de los menores por familiares en eventos en colegios, asociaciones, clubes (obras de fin de curso, competiciones deportivas, etc.
- La discrepancia entre progenitores sobre el consentimiento para subir imágenes de sus hijos a las redes sociales.

Las consultas subieron en 2018 como consecuencia de la aplicación de la nueva normativa de protección de datos y de la difusión que se realizó, y se mantienen en 2019.

AÑOS	SEDE ELECTRÓNICA	CANAL JOVEN	WHATSAPP	TELÉFONO	TOTAL
2016	**218**	**163**	**129**	**166**	**676**
2017	**224**	**246**	**247**	**178**	**895**
2018	**195**	**388**	**384**	**597**	**1564**
2019*	**135**	**321**	**337**	**431**	**1224**
TOTAL	**772**	**1118**	**1097**	**1372**	**4359**

** Datos a fecha de cierre del Plan Estratégico.*

Finalmente, en este ámbito, hay que reseñar la ingente tarea llevada a cabo por el Ministerio de Educación, a través del INTEF, con la colaboración activa de la Agencia Española de Protección de Datos, en la elaboración de materiales curriculares para la prevención de los menores sobre los riesgos en internet, mediante la puesta en marcha de la iniciativa AseguraTIC, de la que se hablará con detalle en el apartado siguiente, relativo al marco de responsabilidad social de la AEPD.

Eje 2.
Innovación y Protección de Datos: factor de confianza y garantía de calidad

En este apartado hay que destacar la creación, a principios de 2016, de la **Unidad de Evaluación y Estudios Tecnológicos (UEET)**.

La creación de la UEET respondió a la necesidad de la AEPD de dotarse de una unidad especializada que hiciese frente a los retos que planteaba el nuevo enfoque del RGPD hacia la responsabilidad proactiva y el estado del arte de los nuevos tratamientos de datos que involucran el uso de tecnologías disruptivas. Se buscaba con ello desarrollar una de las funciones clave que el RGPD asigna a las Autoridades de Control, la de impulsar una labor proactiva que permita detectar el impacto que los nuevos desarrollos tecnológicos pueden tener en la privacidad de los ciudadanos, promoviendo una concepción de la privacidad como activo de las organizaciones públicas y privadas, y como elemento distintivo de la competitividad en el mercado (art. 57.1.i).

En cumplimiento de esta función de prospección, la actividad de la UEET durante estos años se ha centrado en el estudio, investigación y desarrollo de proyectos relacionados con la privacidad y las nuevas tecnologías, en especial con los fenómenos vinculados con internet. De esta forma, la AEPD seguía el ejemplo de otras autoridades como la CNIL francesa, que dispone de una Dirección de Tecnologías e Innovación, o el ICO británico, que dispone de una Dirección Ejecutiva de Innovación y Política Tecnológica, entre otros.

Las funciones asumidas por la UEET desde su creación han sido las siguientes:

- **Asesorar a la Dirección de la AEPD, así como a sus distintas unidades, sobre los temas tecnológicos** que tienen relevancia en la protección de datos de carácter personal, y para ello, analizar las implicaciones y alternativas del estado de arte de la tecnología y generar el conocimiento necesario para anticiparse a los cambios de la misma.
- **Impulsar la protección de datos como un factor de confianza y garantía de calidad en beneficio del desarrollo económico de la sociedad** con el objeto de promover la sensibilización de responsables y ciudadanos, incluido el desarrollo y mantenimiento de herramientas de ayuda para el cumplimiento por parte de los mismos y la elaboración de guías que impulsen el cumplimiento del principio de responsabilidad activa del RGPD en el ámbito tecnológico, según su artículo 57.1. b) y d).
- **Impulsar las medidas que garanticen la compatibilidad del desarrollo tecnológico con la privacidad** asegurando los derechos de los ciudadanos según lo previsto en el artículo 57.1.i) del RGPD. En particular: el asesoramiento a emprendedores y desarrolladores tecnológicos, la realización de estudios de prospección tecnológica, informar y asesorar a los proyectos tecnológicos con implicaciones en el derecho a la protección de datos de las personas, participar en proyectos tecnológicos de ámbito internacional de interés público sobre la base del derecho de la Unión Europea o de los Estados Miembros y promover la colaboración con las universidades con el fin de impulsar la protección de datos en proyectos y contenidos curriculares jurídicos y técnicos.
- **Gestionar el Registro de brechas de seguridad** para facilitar a los responsables el cumplimiento de lo previsto en el artículo 33 del RGPD. Analizar y clasificar las brechas de seguridad y, en su caso, proponer motivadamente a la Dirección la iniciación de una investigación cuando aprecie indicios de la comisión de una infracción.
- **Emitir informes, recomendaciones y dictámenes sobre las consultas previas** relativas a la Evaluación de Impacto para Protección de Datos realizadas por los responsables conforme al artículo 36 del RGPD, en virtud de lo previsto en su artículo 57.1.l).

- La elaboración de una lista positiva y otra negativa de tratamientos que requieren la realización de evaluaciones de impacto según lo previsto en el artículo 57.1.k RGPD.

Las actuaciones más destacables de la UEET en estos cuatro años han sido las siguientes:

1. Guías y notas técnicas
2. Brechas de seguridad
3. Consultas previas de evaluaciones de impacto
4. Colaboraciones con las Administraciones Públicas, la Universidad y otras entidades e instituciones públicas
5. Herramientas para la adaptación al RGPD
6. Acciones de impulso a la responsabilidad proactiva
7. Acciones internacionales
8. Certificación

El detalle de estas actividades se recoge en Informe Balance Final del Plan Estratégico disponible en la web de la Agencia.

Eje 3.
Una Agencia colaboradora, transparente y participativa

Otra de las líneas prioritarias que la Agencia ha seguido estos años ha sido la potenciación de los **canales de información y comunicación** con el objetivo de seguir promoviendo un mejor conocimiento por los ciudadanos de sus derechos, y, en último término, una mayor protección de los mismos.

En este sentido, cabe destacar, por un lado, la labor desarrollada por el **Servicio de Atención al Ciudadano** cuyo funcionamiento se ha ido reforzando durante estos cuatro años, en paralelo con otras medidas para mejorar los niveles de transparencia e información de las actividades de la Agencia a los ciudadanos (nueva web, refuerzo de la agenda de actividades, puesta en marcha del blog de la Agencia, incremento significativo de las Sección de Preguntas Frecuentes de la Sede Electrónica, etc,).

En cifras, las consultas de los ciudadanos a través de este canal han sido las siguientes:

AÑOS	CONSULTAS PRESENCIALES	CONSULTAS TELEFÓNICAS	ACCESOS FAQS	CONSULTAS ESCRITAS	CORREO	BUZÓN SEDE	TOTAL
2016	**4.183**	**76.869**	**147.297**	**8.606**	**552**	**8.054**	**245.561**
2017	**3.699**	**73.501**	**170.754**	**7.954**	**516**	**7.438**	**263.862**
2018	**3.455**	**88.302**	**651.650**	**9.729**	**453**	**5.160**	**758.749**
2019*	**2.140**	**51.979**	**441.888**	**4.377**	**-**	**3.164**	**503.548**
TOTAL	**13.477**	**290.651**	**1.411.589**	**30.666**	**1.521**	**23.816**	**1.771.720**

** Datos a fecha de cierre del Plan Estratégico.*

Por otro lado, la actividad de la Agencia en relación con los medios de comunicación durante estos cuatro años ha sido intensa, pero, como era previsible, experimentó un incremento significativo durante los años 2018 y 2019 como consecuencia directa de la labor de difusión de la Agencia para promover y facilitar la aplicación del RGPD, y posteriormente de la Ley Orgánica 3/2018, entre los ciudadanos, los responsables y los profesionales.

Eje 4.
Una Agencia cercana a los responsables y a los profesionales de la privacidad

El bloque de iniciativas del Plan que ha tenido un mayor desarrollo durante los cuatro años de su aplicación ha sido, sin duda, las orientadas a facilitar una mejor adaptación de los responsables -públicos y privados- al nuevo modelo de cumplimiento establecido por el reglamento europeo de protección de datos. En otros términos, aquellas iniciativas en las que el plan estratégico ha actuado como instrumento para promover la proactividad y la prevención entre los responsables y los profesionales de la privacidad.

En cumplimiento de este objetivo, hay que reseñar, en primer término, la numerosa producción de guías, herramientas y materiales para facilitar el cumplimiento del RGPD por los responsables, especialmente las pymes y las administraciones locales de menor tamaño, y de todas ellas la más destacable ha sido la **herramienta** FACILITA_RGPD, no sólo por su amplia repercusión y aceptación por parte de sus principales beneficiarios, las pymes que realizan tratamientos de bajo riesgo (a continuación se expondrán las cifras), sino también por lo que ha supuesto como ejemplo de buena práctica de referencia a nivel europeo y mundial por parte de una Autoridad de Control a la hora de facilitar el cumplimiento por los responsables de sus obligaciones legales en materia de protección de datos. Así lo han reconocido otras instancias nacionales e internacionales al premiar a la AEPD por dicha práctica, como son, en el ámbito nacional, el accésit concedido en la XII edición de los 'Premios a la Calidad e Innovación en la Gestión Pública', en su modalidad del 'Premio Ciudadanía', que otorga el Ministerio de Política Territorial y Función Pública. Y, en el ámbito internacional, los obtenidos premios en la 46ª Conferencia Internacional de Autoridades de Protección de Datos y de Privacidad, como se describe en otro apartado de la Memoria.

El otro grupo de iniciativas que ha de destacarse en este ámbito, orientadas promover la mayor difusión posible de las novedades que incorporaba el Reglamento en los distintos sectores económicos y profesionales, así como en las diferentes Administraciones Públicas, ha sido el completo programa de **acciones de información y de formación en el RGPD** destinado a los colectivos, grupos de interés y organizaciones, públicas y privadas, que se consideraron más directamente afectadas con la plena entrada en vigor de la nueva norma europea, con especial atención a las pymes y a las entidades locales de menor tamaño.

Esta iniciativa se llevó a cabo en estrecha colaboración con las organizaciones y asociaciones más representativas de cada ámbito de actuación, a través de distintos protocolos de colaboración suscritos a tal fin. Así, en el ámbito empresarial, con la CEOE y CEPYME; en el profesional, con Unión Profesional y ASCOM, y en el sector público, estatal, autonómico o local, en colaboración con el INAP, la CNMC, las respectivas Administraciones Autonómicas, la FEMP y las Diputaciones Provinciales.

La relación detallada de las numerosas actividades y eventos que se llevaron a cabo por la AEPD con esta finalidad, especialmente durante los años 2017 y 2018, figuran detallados en el Informe Final del Plan Estratégico disponible en el site correspondiente de la web de la Agencia, destacándose en otros apartados los más relevantes de 2019.

Una mención especial en este apartado, por lo que se supuso de novedad en el momento de su presentación, en julio de 2017, fue la aprobación del **Esquema de certificación de Delegados de Protección de Datos** impulsado por la AEPD, en colaboración con la Entidad Nacional de Acreditación (ENAC), convirtiéndose en la primera Autoridad europea de Protección de datos en promover un marco de referencia para esta figura.

En la elaboración y posterior seguimiento del Esquema se ha contado con el asesoramiento de un Comité Técnico de Expertos de 23 miembros, formado por representantes de sectores y asociaciones profesionales, empresariales, universidades y AAPP. Asimismo, han formado parte la Autoridad Catalana y la Agencia Vasca de Protección de Datos.

La AEPD ha optado por promover un sistema de certificación de DPD para ofrecer seguridad y fiabilidad tanto a los profesionales de la privacidad como a las empresas y entidades que van a incorporar esta figura a sus organizaciones, ofreciendo un mecanismo que permite certificar que los DPD reúnen la cualificación profesional y los conocimientos requeridos. Las certificaciones serán otorgadas por entidades certificadoras debidamente acreditadas por ENAC, siguiendo criterios elaborados por la AEPD en colaboración con los sectores afectados.

Eje 5.
Una Agencia más ágil y eficiente

El Reglamento contempla un nuevo modelo de supervisión, que busca superar la tradicional respuesta reactiva mediante la imposición de sanciones económicas ante las denuncias de los afectados. Este nuevo modelo recoge así de forma equilibrada un amplio abanico de medidas correctoras de posibles incumplimientos de la norma tales como la advertencia, un apercibimiento aplicable con gran flexibilidad, ordenar una actuación específica en un plazo determinado o imponer una limitación temporal o definitiva del tratamiento de los datos.

Para afrontar estos cambios en el nuevo modelo de supervisión que dibuja el Reglamento europeo, el primer reto que se plantea es la adaptación de la propia AEPD en cuanto a su modo de funcionamiento y de gestión interna, además de los requerimientos propios como sujeto obligado.

En este sentido para hacer frente a los desafíos que planteaba el RGPD en las mejores condiciones posibles, el Plan Estratégico, en su Eje 5, ya fijaba, entre sus objetivos, la necesidad de acometer un profundo proceso de mejora de la organización y de la gestión, especialmente a través de la simplificación de los procedimientos y de la reducción de los plazos de tramitación.

Para poner en marcha estas medidas, y conocer con detalle cuál era el punto de partida, se realizó en 2106, a petición de la propia Agencia, una auditoría por parte de la Inspección General de Servicios de la AGE, centrada específicamente en los modos de gestión de la Subdirección General de Inspección de Datos, que aglutina una parte significativa de los procedimientos y de los recursos materiales y personales de la Agencia.

La Auditoría detectó una serie de aspectos de mejora en cuanto al funcionamiento y a los tiempos medios de tramitación de los expedientes, debido en gran parte a la enorme carga de trabajo que soportaba en ese momento la Subdirección General de Inspección de Datos, provocada por el crecimiento constante de las denuncias y reclamaciones y una plantilla congelada desde 2008, proponiendo un conjunto de recomendaciones para la mejora de dicha situación. A raíz de las conclusiones de dicha auditoría, y con vistas a la aplicación del RGPD, se adoptaron por la Dirección de la Agencia un conjunto de decisiones encaminadas a mejorar la estructura y el modo de funcionamiento interno de la Subdirección que han supuesto que, en los últimos tres años se haya producido una reducción importante de la bolsa de expedientes pendientes y, por otro lado, una reducción significativa de los plazos medios de tramitación de los expedientes, que indudablemente ha repercutido directamente en esa reducción, a la que ha contribuido también de forma significativa la progresiva implantación de los procedimientos de la Administración Electrónica.

La otra estrategia seguida por la Agencia no sólo para reducir la cifra de expedientes pendientes de tramitación, sino también, y sobre todo, para satisfacer mejor y de forma más rápida las pretensiones de los ciudadanos, y, en esa medida, ofrecer a éstos una mayor protección de sus derechos, ha sido la implantación de nuevos mecanismos de carácter preventivo para la resolución de las reclamaciones de los ciudadanos en ámbitos de fuerte impacto

ciudadano por su gran volumen de reclamaciones, como son la contratación irregular (en especial, por la suplantación de identidad) en los servicios de telecomunicaciones y la publicidad no deseada, o a través del papel atribuido por la nueva Ley Orgánica 3/2018 a los Delegados de Protección de Datos para conocer previamente las reclamaciones planteadas ante la Agencia, a efectos de buscar una solución amistosa de las mismas posibilitando con ello que la Agencia pueda dedicarse a otros ámbitos más propios de su nueva posición tras el Reglamento europeo.

Entre estos procedimientos de resolución extrajudicial de conflictos, hay que aludir en primer término al nuevo sistema voluntario de mediación que puso en marcha la AEPD, a partir de 1 de enero de 2018, en colaboración con la Asociación para la Autorregulación de la Comunicación Comercial (AUTOCONTROL), al que se han adherido las operadoras de telecomunicaciones de los principales Grupos que operan en España (Orange, Telefónica, Vodafone y Más Móvil).

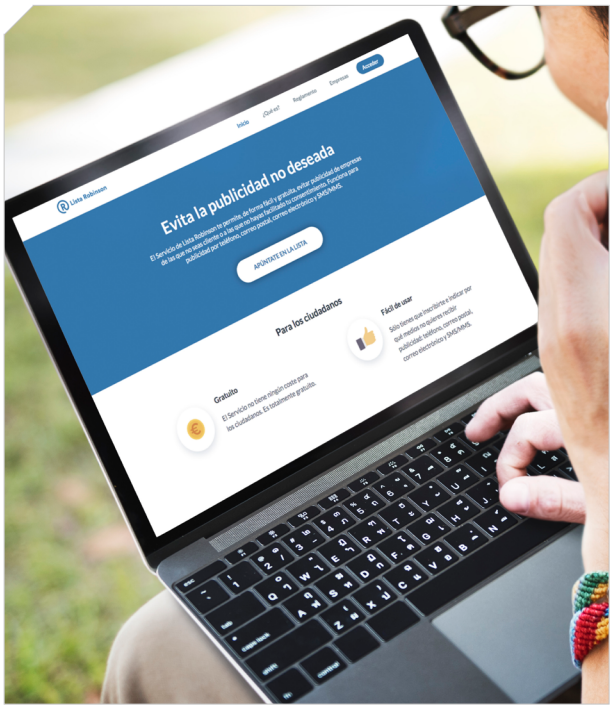
Su justificación está en el propio Reglamento europeo, entre cuyos requerimientos contempla la obligación de que las Autoridades competentes promuevan la elaboración de códigos de conducta que aseguren la correcta aplicación de la normativa de protección de datos. Entre los objetivos de los códigos de conducta está expresamente la posibilidad de articular procedimientos extrajudiciales y otros procesos de resolución de conflictos que permitan resolver las reclamaciones de los ciudadanos ante quienes tratan sus datos (art. 40.2, k RGPD).

El sistema está dirigido a resolver ágilmente reclamaciones sobre la recepción de publicidad no deseada, la suplantación de identidad o el tratamiento de datos para la recepción de facturas tras haber solicitado la baja del servicio. Esta iniciativa es voluntaria para los ciudadanos y es independiente de las reclamaciones que los ciudadanos pueden seguir interponiendo ante la AEPD si consideran que se han vulnerado sus derechos.

Otra de las vías utilizadas para reforzar las actuaciones preventivas en esta materia, ha sido la potenciación de los sistemas de exclusión publicitaria, y, en particular, el único existente hasta la fecha en España, el de la llamada **Lista Robinson** creado y gestionado por la Asociación Española de Economía Digital (ADIGITAL), para proteger los datos personales de los ciudadanos y facilitar a las empresas el cumplimiento de la normativa de protección de datos. Estos sistemas están regulados en la Ley Orgánica 3/2018 (art. 23).

La inscripción de los datos en la Lista Robinson puede ser una buena solución para evitar la llamada publicidad no deseada procedente de las que no se sea cliente. Al inscribirse en la Lista Robinson se puede elegir el medio o canal de comunicación a través del cual no se desea recibir publicidad (correo postal, llamadas telefónicas, correo electrónico u otro medio).

La Lista Robinson, que ya cuenta con más de un millón de usuarios registrados, nació en 1993 como una herramienta de autorregulación que permitía a éstos oponerse al envío de publicidad por correo postal. En 2009, evolucionó para incluir nuevas opciones de oposición a recibir publicidad por teléfono (llamadas, email y SMS).



En 2019 se presentaron algunas novedades para promover su mayor utilización por usuarios y empresas. En concreto, se introduce una nueva funcionalidad: la posibilidad de que los ciudadanos limiten la recepción de publicidad de forma gratuita no solo por canales (teléfono, SMS, email o postal), como ya ocurría, sino también por sectores publicitarios. A esto se une un nuevo servicio de gestión de reclamaciones de los usuarios. Asimismo, se han incorporado nuevas soluciones que permiten a las pymes tratar y normalizar los datos de los clientes a los que quieren dirigir sus comunicaciones publicitarias para agilizar la consulta de la Lista Robinson. El Servicio no tiene coste para pymes y autónomos hasta 30.000 registros consultados al año.

Y, en tercer lugar, hay que aludir al procedimiento arbitrado para posibilitar que las reclamaciones puedan ser solventadas satisfactoriamente por parte del responsable directamente, o a través de la **intervención del Delegado de Protección de Datos**, sin necesidad de que tenga que intervenir la AEPD, regulado en el artículo 37 LOPDGDD. En concreto, por lo que se refiere a las reclamaciones que se presentan ante la Agencia, ésta analiza previamente si la reclamación no se ha planteado ante el responsable del tratamiento (o su DPD), o sí se planteó, pero el responsable/DPD no respondió, o la respuesta no satisfizo al reclamante, en cuyo caso se traslada la reclamación al responsable (a la atención del DPD, en caso de haberse designado).

Asimismo, la información obtenida puede utilizarse para evaluar la eficacia de los protocolos de actuación y de las medidas correctoras aplicadas para deducir, en su caso, las responsabilidades previstas en el Reglamento.

Por lo que se refiere a las cifras de utilización de este nuevo tipo de procedimiento, figuran en el Anexo de esta Memoria.

2.2 Del Plan Estratégico al Marco de Responsabilidad Social y Sostenibilidad. La AEPD y la Agenda 2030

Expuesto lo anterior, pese a que el balance de cumplimiento del Plan Estratégico durante estos años ha sido satisfactorio, sin embargo, faltaba dar un paso más, reforzando el compromiso con la sociedad, con la ciudadanía y con las personas en relación con la privacidad y la protección de sus datos personales. Este compromiso viniendo de un organismo regulador y del ámbito público adquiere una especial responsabilidad, en lo que supone de orientar su actividad hacia fines distintos a los meramente correctores y sancionadores. Es precisamente este compromiso con determinados valores y principios de responsabilidad social lo que da sentido a la actividad de un organismo público que tiene como razón de ser la defensa y la garantía efectiva de un derecho fundamental.

Para hacer realidad este objetivo y llevar a cabo este compromiso no existe mejor marco que la Agenda 2030 y los Objetivos de Desarrollo Sostenible

Y para ello la Agencia solicitó la colaboración del Pacto Mundial de Naciones Unidas. El trabajo conjunto que se ha desarrollado con el Pacto Mundial de Naciones Unidas ha conseguido alinear el Plan Estratégico con la Agenda 2030 y fruto de este proceso se ha incorporado un sexto Eje al Plan Estratégico, bajo el título de “Una Agencia socialmente responsable y sostenible”.

Se ha evaluado el impacto social de todas las iniciativas del Plan Estratégico que estaban contempladas a fecha de diciembre de 2018 y cómo se relacionan con los 17 objetivos de desarrollo sostenible y las 169 metas de la Agenda 2030, constatando que la Agencia impacta de manera especial en tres ODS:

- ODS 16: paz, justicia e instituciones sólidas.
- ODS 12: producción y consumo responsables.
- ODS 17: alianzas para lograr los objetivos.

Resulta evidente que los planes de responsabilidad social implican necesariamente un firme compromiso de las organizaciones que acuerden implantarlos, primero con ellas mismas, en sus procesos internos, y luego con respecto a los destinatarios de sus acciones. Esto da una idea de cómo la gestión de la privacidad impacta en aspectos muy relevantes para el desarrollo de nuestra sociedad y de nuestra economía.

Los cinco ejes que conforman el Plan Estratégico ayudan a conseguir también otros objetivos y metas de la Agenda 2030, además de los tres mencionados.

Por ejemplo, en el ODS 10, Reducción de las Desigualdades, ya que la actividad de responsabilidad social de la Agencia influye en promover la inclusión social, económica y política de todas las personas, independientemente de su edad, sexo, discapacidad, raza, etnia, origen, religión o situación económica u otra condición. O en el ODS 5, Igualdad de Sexos, ya que, como luego podremos constatar a través de distintas iniciativas puestas en marcha, la Agencia influye en asegurar la participación plena y efectiva de las mujeres y la igualdad de oportunidades de liderazgo a todos los niveles decisorios en la vida política, económica y pública.

Estas iniciativas se han traducido en la aprobación del Marco de Actuación y de un Plan para el período 2019-2024 en el que se han identificado un total de 103 acciones de las cuales el porcentaje mayoritario, un 70%, responden a compromisos con la Sociedad, tratando de impulsar alianzas para combatir la violencia en internet de manera integral, con especial énfasis en los menores y en su entorno educativo, en la igualdad de género, y, en suma, en los colectivos más vulnerables para que sientan que su privacidad y sus datos personales están debidamente garantizados y protegidos. Y que, asimismo, promueve la innovación y el emprendimiento tecnológico en lo que se refiere a la privacidad y a la protección de datos.

El 13% son compromisos con nuestros empleados, un 10% con el respeto al medio ambiente y un 7% están relacionadas con el buen gobierno y la transparencia. Ambos documentos están disponibles en la sección sobre sostenibilidad de la página de la Agencia.

El proceso seguido para su elaboración ha sido abierto y participativo porque ha sido compartido con los empleados de la Agencia, así como con los ciudadanos y con las organizaciones mediante el correspondiente periodo de información pública, incorporando todas las opiniones y sugerencias recibidas durante el mismo, así como las que puedan serlo en cualquier momento a través del buzón de sugerencias abierto al efecto.

En definitiva, con el Marco de Actuación de Responsabilidad Social de la AEPD se pretende seguir avanzando como organismo público comprometido con las necesidades de los ciudadanos, de las empresas, de las administraciones públicas y de los profesionales de la privacidad, poniendo a su servicio un conjunto de iniciativas encaminadas a facilitar sus relaciones con esta Agencia. Estas acciones vienen así a ampliar nuestra capacidad de actuación y nuestras obligaciones como Autoridad independiente de supervisión y control en materia de protección de datos personales.

Compromiso con la sociedad

El compromiso con la Sociedad nace de la propia razón de ser de la Agencia como organismo público que tiene como misión tutelar un derecho fundamental. Partiendo de esta premisa, se ha asumido una responsabilidad con los ciudadanos y con los sujetos obligados al cumplimiento de la legislación de protección de datos que se plasma bajo tres grandes líneas de actuación:

- La prevención para una protección más eficaz de los derechos de los ciudadanos, especialmente de los menores.
- La igualdad de género para combatir de modo especial la violencia en internet, especialmente contra las mujeres.
- La innovación y el emprendimiento en el terrero de la protección de datos para favorecer el desarrollo de la economía digital.

Este compromiso con la sociedad debe articularse a través de alianzas con organizaciones públicas y privadas para apoyar los ODS ya mencionados anteriormente.

Una de las líneas de actuación fundamentales donde la Agencia puede desarrollar un papel destacado en el campo de la responsabilidad social es la igualdad de género. En esta área resulta fundamental trabajar de la mano de actores como el Ministerio del Interior, la Fiscalía y la Delegación del Gobierno para la Violencia de Género, impulsando protocolos de colaboración para el desarrollo de acciones que contribuyan a combatir esta lacra social, poniendo a disposición de las víctimas aquellos recursos y herramientas que la Agencia, como autoridad pública, tiene legalmente atribuidos, y que, movilizados de forma urgente, pueden resultar sumamente eficaces, dado que en determinadas situaciones -como pueden ser el acceso y la divulgación sin consentimiento de información sensible, de fotografías o videos de carácter íntimo; la vigilancia y monitorización de actividades en línea, o las conductas conocidas como “sextorsión” o el acoso sexual online-, los daños infligidos a la víctima son mucho mayores cuando se difunden por internet.

En este sentido, las características de las TIC han dado lugar a nuevas amenazas para la mujer víctima de violencia, derivadas, entre otras, de la velocidad con la que la información se difunde en este entorno, la posibilidad de acceder a la información gracias a los motores de búsqueda y las dificultades para su eliminación. La viralidad y perdurabilidad en el entorno en línea entrañan, sin duda, nuevas situaciones de riesgo que han de afrontarse con todos los medios disponibles, desde la mayor colaboración posible entre las instituciones implicadas y, de manera especial, con los grandes prestadores de servicios en internet.

En el terreno educativo, se hace imprescindible la colaboración con el Ministerio de Educación y también con la Delegación de Gobierno para la Violencia de Género para la elaboración de materiales curriculares que ayuden a prevenir, detectar y erradicar este tipo de conductas violentas en el entorno escolar. En este sentido, cabe destacar la puesta en marcha de la Web AseguraTIC, impulsada por el Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF), en el que han aportado sus recursos un gran número de instituciones y entidades del ámbito privado y público.

Pero, sin duda, una de las iniciativas más relevantes, por su evidente impacto social, ha sido la puesta en marcha del Canal prioritario de la AEPD para comunicar la difusión de contenido sensible en internet y solicitar su retirada.

La AEPD ha desarrollado una iniciativa pionera en la que se ha trabajado desde hace un año y medio cuando se constituyó en su seno el Grupo de Trabajo de Violencia en Internet con el fin de garantizar su eficacia y la colaboración efectiva de todos los actores -públicos y privados- implicados. En concreto se comprometió, entre otras medidas, a elaborar un protocolo de actuación a disposición de las víctimas, para que sean informadas de la posibilidad de acudir gratuitamente a la Agencia en tutela de derechos en el caso de que sea vulnerada su privacidad, comprometiéndose a dar prioridad en la gestión de este tipo de reclamaciones.

Mediante la puesta en marcha del Canal prioritario, la AEPD ha tratado de ofrecer una respuesta rápida en situaciones excepcionalmente delicadas, como aquellas que incluyen la difusión de contenido sexual o violento

El objetivo es establecer una vía en la que las reclamaciones recibidas serán analizadas de forma prioritaria, permitiendo que la Agencia, como autoridad independiente, pueda adoptar, si es preciso, medidas urgentes que limiten la difusión y el acceso de los datos personales. El detalle de las medidas adoptadas para su funcionamiento, así como para promover su difusión se detallan posteriormente.

La creación del canal prioritario se enmarca así en una política integral de la organización de compromiso activo con la igualdad de género y de lucha contra cualesquiera conductas que resulten contrarias a la misma, en sus diversas formas.

En este sentido, hay que destacar otras iniciativas presentadas recientemente que persiguen esta misma finalidad de prevención y lucha contra la violencia de las mujeres en internet. Así, pueden mencionarse la siguientes:

- La creación de un espacio web de ayuda a la protección de la privacidad de las víctimas de violencia de género, con la que se trata de evitar que una mujer que esté sometida a cualquier tipo de violencia de género sea víctima del daño que supone el acoso digital.

Así, en la sección se ofrecen una serie de pautas para que pueda detectar si alguien ha podido manipular su móvil e instalar aplicaciones ocultas que permitan acceder a datos como la geolocalización del dispositivo. Además, se proporcionan consejos para proteger la privacidad en dispositivos móviles, recomendando aplicaciones y herramientas para implementar barreras de seguridad. La página también contiene indicaciones sobre qué hacer en caso de que se estén difundiendo en internet datos personales de la mujer sin su consentimiento. En ocasiones, las mujeres víctimas de violencia física también sufren la vulneración de su privacidad con la grabación y difusión de sus imágenes en internet. A este respecto, además de la posible responsabilidad penal de algunas de estas conductas, los agresores pueden incurrir también en responsabilidad administrativa por vulneración de la privacidad de la víctima, lo que podría implicar la apertura de un procedimiento sancionador por parte de la Agencia. En este sentido, junto con la información sobre cómo solicitar la retirada de contenidos directamente ante los buscadores, foros, blogs y redes sociales más populares, la Agencia recomienda utilizar el Canal prioritario de la AEPD.

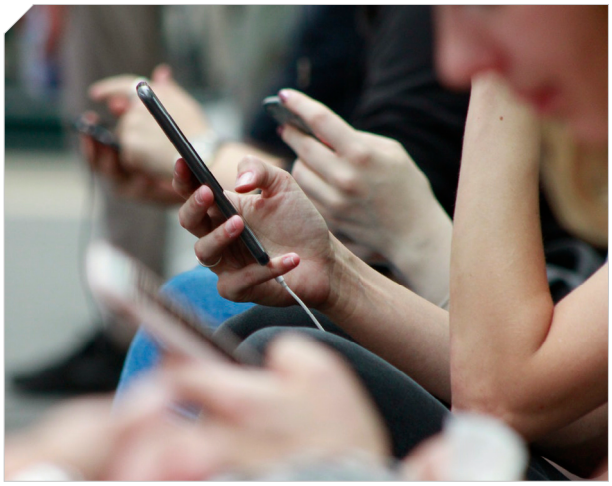
- Junto a la web de ayuda, hay que hacer también una especial mención a las **Recomendaciones para la protección de datos en las políticas de prevención del acoso digital**, un documento con el que se pretende fomentar que empresas y administraciones públicas incorporen a sus políticas de prevención del acoso digital medidas orientadas a la prevención y erradicación de este en los centros de trabajo.

Las Recomendaciones enumeran en primer término las conductas que suponen ciberacoso sexual y por razón de sexo, especialmente cuando se realizan mediante el uso de datos personales. El trabajador que realice estas conductas puede tener responsabilidad civil, penal, administrativa por infracción de protección de datos y laboral por acoso digital. Por su parte, la empresa podría incumplir la Ley de Prevención de Riesgos Laborales y enfrentarse a multas de hasta 187.000 euros.

El documento también pone el foco en que el ciberacoso no sólo supone la comisión de un ilícito por parte de quien lo comete, sino también para la empresa o administración pública que, teniendo conocimiento de estos tratamientos de datos ilícitos, no actúe para erradicarlos. Así, además de una declaración inequívoca del compromiso de la organización con la protección de datos y con la igualdad de género, la Agencia recomienda medidas orientadas a la prevención, como formación al personal y medidas de reacción, como el deber de denunciar que tienen las organizaciones cuando sean conocedoras de situaciones de ciberacoso en casos de violencia de género o el deber de poner en marcha los mecanismos de actuación previstos en sus políticas, iniciando las actuaciones disciplinarias pertinentes contra los trabajadores que hubieran llevado a cabo estas conductas.

- Asimismo, la Agencia ha creado dos nuevas categorías en sus premios anuales para reconocer y apoyar las buenas prácticas en relación con iniciativas del ámbito público y privado dirigidas, una a la protección en internet de la privacidad de las mujeres víctimas de violencia por razón de género y, otra, al emprendimiento en la protección de datos personales, “Angela Ruiz Robles”.

Todas estas medidas están dirigidas especialmente a reforzar la protección a los colectivos de mujeres y menores así como a proteger ante otras a conductas especialmente graves como en los casos de racismo y la homofobia, por citar algunos casos relevantes.



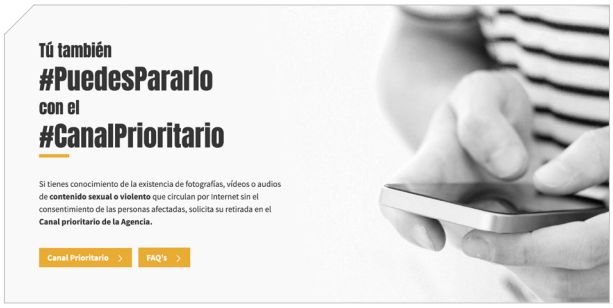
2.3 Canal prioritario para comunicar la difusión de contenidos sensibles en internet y solicitar su retirada

A pesar de las innumerables ventajas que proporcionan las nuevas tecnologías, estas proporcionan infraestructuras que pueden servir de cauce para dañar de forma grave la privacidad de las personas. Con la extensión y el uso intensivo de dispositivos móviles e internet, redes sociales y otros servicios ha proliferado la difusión de formas de violencia que persiguen, además, la humillación pública de las víctimas.

Para hacer frente a este grave problema, la Agencia Española de Protección de Datos puso en marcha el 24 de septiembre el Canal Prioritario para solicitar la retirada urgente de contenidos sexuales o violentos que circulan en la Red, ofreciendo una rápida respuesta para aquellas situaciones excepcionalmente delicadas y gravosas que afectan, en su gran mayoría, a mujeres, menores y colectivos expuestos a situaciones de vulnerabilidad, víctimas de lo que se puede denominar violencia digital.

En el caso de plantear una reclamación por estas situaciones, el ciudadano deberá describir las circunstancias en que se ha producido la difusión no consentida de las imágenes, indicando en particular si la persona afectada es víctima de violencia de género, abuso o agresión sexual o acoso, o si pertenece a cualquier otro colectivo especialmente vulnerable como el de los menores de edad, personas discriminadas por su orientación sexual o raza, personas con discapacidad o enfermedad grave o en riesgo de exclusión social, así como especificando la dirección o direcciones web en las que se han publicado.

Las reclamaciones recibidas se analizan de forma prioritaria, permitiendo que la Agencia, como autoridad independiente, pueda adoptar, si es preciso, medidas urgentes que limiten la difusión y el acceso de los datos personales.



La denuncia o comunicación se puede realizar no sólo por las víctimas, sino también por terceras personas que conozcan de estas situaciones.

En cuanto a la presentación de las reclamaciones, es necesario disponer de certificado electrónico para la comunicación a través de la Sede (vía más rápida), pero si no se dispone de certificado también se puede presentar en papel para lo que en la web se facilita un formulario. Los/las menores de edad pero mayores de 14 años no necesitan certificado electrónico para formular la denuncia o comunicación.

Tras el análisis de la reclamación formulada, la Agencia podrá determinar la posible adopción urgente de medidas provisionales para evitar la continuidad del tratamiento ilegítimo de los datos personales en casos particularmente graves. Este tipo de medida se materializa en una orden que la Agencia dirige a la plataforma, página web o empresa prestadora del servicio de internet para que retire el contenido denunciado inmediatamente de tal forma que no pueda ser visualizado ni redifundido, pero debiendo conservarlo internamente a efectos de su valor probatorio en el ámbito administrativo o judicial.

Las empresas Facebook, Google y Twitter han mostrado una actitud proactiva para la ejecución de las medidas cautelares incluidas en esta iniciativa.

Asimismo, la Agencia puede realizar actuaciones de investigación que puedan dar lugar a la apertura de un procedimiento sancionador contra el o los usuarios responsables de haber realizado el tratamiento ilegítimo de datos correspondiente.

El Canal prioritario se apoya en seis instrumentos de colaboración –un Convenio y 5 Protocolos– firmados el 24 de septiembre en el acto de presentación del Canal, y cuyo contenido se resume a continuación:

El **Convenio de colaboración entre el Ministerio de Presidencia, Relaciones con las Cortes e Igualdad y la AEPD**, además de la realización de acciones conjuntas de sensibilización e información sobre uso seguro de Internet y redes sociales y prevención de la violencia contra la mujer y de la vulneración de su derecho a la protección de datos, articula la colaboración entre el servicio 016 de información y asesoramiento jurídico en materia de violencia de género y el servicio de atención telefónica de la Agencia Española de Protección de Datos.

El **Protocolo de actuación entre el Ministerio del Interior y la AEPD** se ha suscrito para incrementar la eficacia de la atención que se presta a las personas cuyos datos se han difundido online, especialmente en el caso de imágenes, vídeos o audios que incluyan datos sensibles, y particularmente en los casos de violencia contra la mujer. Así, cuando se presente una denuncia ante la Policía o ante la Guardia Civil, si de los hechos declarados se desprendiesen indicios de conductas que vulneran la legislación en materia de protección de datos, se informará a la persona denunciante acerca de su derecho a presentar una reclamación gratuita ante la Agencia Española de Protección de Datos.

El **Protocolo de actuación entre el Ministerio de Educación y Formación Profesional y la AEPD** articula la colaboración para dar a conocer y difundir en los centros escolares, entre madres, padres, profesores y alumnos, las consecuencias de la obtención y difusión ilegítima de imágenes sensibles a través de Internet, que es uno de los instrumentos más usados en los casos de acoso en el entorno escolar –bullying y cyberbullying– y de acoso sexual a menores –grooming o consecuencias derivadas del sexting–. También se difundirá la forma de presentar una reclamación ante la Agencia Española de Protección de Datos.

El **Protocolo de actuación entre el Ministerio de Trabajo, Migraciones y Seguridad Social y la AEPD** articula la colaboración entre estos organismos para, entre otras actuaciones, contribuir a la prevención y sensibilización en caso de actos de violencia contra la persona trabajadora, y particularmente en casos de violencia sobre la mujer siempre que exista conexión o se produzca en el entorno laboral. Además, el Ministerio impulsará la elaboración y la adopción de planes de igualdad y de protocolos contra el acoso, incluido el acoso laboral, en el tejido empresarial español, con la finalidad de que todas las empresas dispongan de estos instrumentos, que contemplarán el funcionamiento concreto de los sistemas de denuncia dentro de las empresas para casos de esta naturaleza, y se informará sobre la posibilidad de recurrir ante la AEPD si los hechos pudieran constituir una vulneración de la normativa en materia de protección de datos.

El **Protocolo de actuación entre la Fiscalía General del Estado y la AEPD** se ha firmado para incrementar la eficacia de las medidas de atención a las personas afectadas por este tipo de hechos, particularmente en los casos de violencia contra la mujer. Estas medidas se concretan en el traslado inminente a la Fiscalía por parte de la AEPD cuando esta última aprecie la existencia de indicios de la comisión de un ilícito penal, de toda la información y documentación que se hubiera recabado a fin de que la Fiscalía lleve a cabo las actuaciones pertinentes.

El **Protocolo de actuación entre el Consejo General de la Abogacía y la AEPD** tiene entre sus objetivos principales ofrecer información a los afectados sobre cómo presentar una reclamación ante la Agencia. Así, cuando a raíz de los hechos que declarase la persona a la que el abogado asesore o defienda, se detectasen indicios de conductas que vulneren la legislación en materia de protección de datos, se le informará acerca de su derecho a presentar una reclamación gratuita ante la AEPD.

Estos instrumentos de colaboración tienen por objeto establecer las pautas de actuación para atender a las personas cuyos datos personales sensibles o comprometidos, de carácter sexual o violento, se hayan difundido ilegítimamente en internet.

Se han celebrado las reuniones constitutivas de las correspondientes Comisiones de Seguimiento y se han determinado las actuaciones a realizar en desarrollo de los citados instrumentos de colaboración.

Complementariamente, se han establecido alianzas con otras entidades, fundaciones y organizaciones con las que se comparten objetivos que incluyen la suscripción de instrumentos de colaboración que hagan más asequible su consecución, y cuya firma está prevista para principios de 2020:

- Protocolo General de Actuación con la Fundación ANAR
- Protocolo General de Actuación con la Fundación Mutua Madrileña
- Protocolo General de Actuación con UNESPA
- Protocolo General de Actuación con la Asociación Española de Fundaciones

A finales de 2019, se analizaron las posibles mejores para la consecución de los objetivos de este canal que han concluido a principios de 2020.

Como consecuencia de este análisis, a principios de 2020 el servicio se ha ampliado mediante la puesta en funcionamiento de un nuevo formulario, dirigido a menores de edad (a partir de los 14 años), más sencillo y comprensible para este segmento de población. Se pretende con ello facilitar a los menores la posibilidad de comunicar este tipo de casos, para que la Agencia pueda analizarlos lo antes posible y actuar dentro del marco de sus competencias.

Por lo que respecta a las reclamaciones recibidas a través del Canal Prioritario durante el año 2019, fueron 51, de las cuales sólo en 6 reclamaciones, referentes a 5 casos, se reunían los factores que se están valorando para considerar el supuesto urgente y para tramitarse con prioridad. Se emitieron 18 órdenes de medida provisional urgente, y en todos los casos se alcanzó el objetivo de retirar el contenido original para que no continuase estando a disposición general en la plataforma o red social.

Con el fin de promover su difusión, en 2019 se valoró la necesidad de desarrollar una campaña informativa en colaboración con un amplio abanico de medios de comunicación y otras entidades que posibilitaran el conocimiento de este canal en amplios sectores de la ciudadanía.

Atendiendo a la especial importancia de esta iniciativa, se incluye a continuación información detallada sobre las actuaciones realizadas en 2020.

La Agencia Española de Protección de Datos presentó el día 28 de enero de 2020 la campaña **'Por todo lo que hay detrás'**, dirigida a promover la utilización del Canal prioritario de la Agencia. Para ello, en el último trimestre de 2019 se comenzaron a realizar multitud de gestiones con diversas organizaciones, tanto públicas como privadas. Con fecha 23 de diciembre de 2019 se registró en el Registro de la Comisión Nacional de los Mercados y la Competencia (CNMC) un escrito de la Agencia por el que solicitaba la exención de cómputo publicitario para la difusión en televisión del anuncio de la campaña.

La CNMC consideró que reunía los requisitos exigidos por la Ley para la exención de cómputo publicitario al tratarse de un anuncio en el que puede apreciarse características y valores de interés público y que, a su vez, carece de valor comercial. Para que este anuncio pueda beneficiarse de dicha condición y no sea considerado mensaje publicitario, su difusión ha sido gratuita.

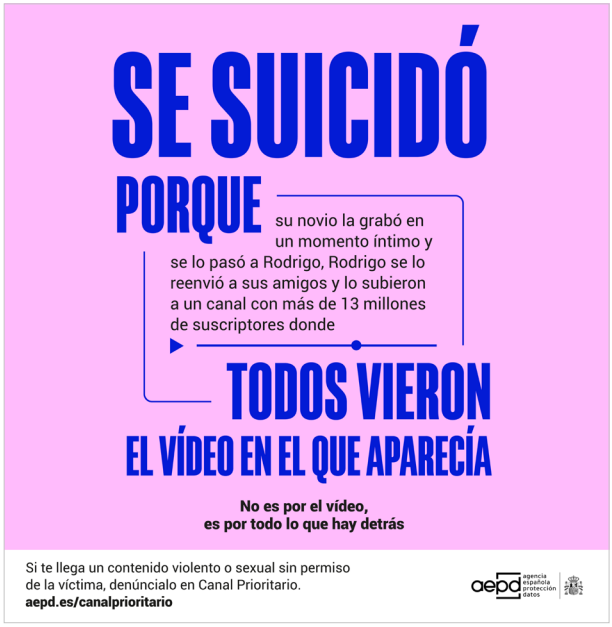
Para llevar a cabo la difusión de esta campaña se contó, entre otros, con el apoyo de entidades como Atresmedia, Mediaset y RTVE, Fundación Mutua Madrileña, Fundación ANAR, FAD, EMT y Metro de Madrid, Más móvil, Clear Channel o Google. Como ejemplos de la repercusión que ha tenido

esta campaña se pueden citar los siguientes: la emisión del spot en televisión por parte de las tres principales cadenas de televisión de ámbito nacional ha obtenido más de 50 millones de impactos. Asimismo, en cuanto a la difusión realizada en medios de transporte, la Empresa Municipal de Transportes (EMT Madrid) cedió gratuitamente durante 15 días el espacio de sus pantallas en 212 líneas, con un alcance potencial de un millón y medio de viajeros de media diaria. Asimismo, el Ayuntamiento de Santander también cedió gratuitamente el espacio digital de sus autobuses para la emisión de la campaña.

En cuanto a Metro de Madrid, además de dos vídeos emitidos por el Canal Metro, se colocaron de forma gratuita en su circuito de transporte 258 carteles. La campaña se mantuvo desde el 28 de enero al 10 de marzo. Cada día Metro de Madrid es utilizado por 1,8 millones de personas, contabilizando más de 2,3 millones de viajes al día. Otro ejemplo de la difusión de la campaña en colaboración con otras entidades ha sido Mutua Madrileña, que a la difusión de los 40.000 ejemplares de su revista de papel suma los casi 3 millones de usuarios del mailing digital realizado a sus clientes.

Asimismo, desde el día 29 de enero se intensificó la campaña en redes sociales, poniéndose en marcha un reto en Instagram y Twitter en el que se animaba a actuar de manera directa contra la publicación sin consentimiento de contenido sensible -no compartiéndolo y denunciándolo en el Canal prioritario- bajo el hashtag #PuedesPararlo.

Empresas, organismos, administraciones y personajes públicos se sumaron a la campaña retuiteando las publicaciones de la AEPD y en algunos casos realizando publicaciones propias que ayudaron a incrementar el impacto y difusión de la campaña. Esta contó también con la participación de colaboradores externos, que consiguieron más de dos millones de impresiones de la campaña.



2.4 Otros objetivos de RSC

Otra de las líneas prioritarias de la política de RS es, sin duda, la apuesta por apoyar y acompañar todas aquellas iniciativas que favorezcan la innovación en lo que se refiere a la privacidad y a la protección de datos. Con el desarrollo tecnológico actual (redes sociales) y de futuro (internet de las cosas, blockchain e inteligencia artificial) la privacidad como concepto y derecho fundamental ocupa cada vez más espacio en la vida de los ciudadanos. Así lo confirma el CIS de mayo de 2018, que destaca que este tema preocupa mucho o bastante a tres de cada cuatro encuestados.

Uno de sus objetivos fundamentales es seguir muy de cerca los avances tecnológicos para actuar de manera rápida en la inclusión correcta de políticas de privacidad y de protección de datos. Este objetivo pasa necesariamente por la potenciación de la Unidad de Evaluación y Estudios Tecnológicos para poder ofrecer un alto valor añadido a los desarrollos tecnológicos en cuestiones de privacidad.

Para innovar es necesario colaborar y por ello la Agencia está siendo proactiva en la colaboración con Universidades y con actores que financian y promueven investigaciones, además de trabajar con empresas y fundaciones que favorezcan acuerdos con emprendedores y startups sobre aspectos que inciden muy directamente en la privacidad, como blockchain, big data o la inteligencia artificial.

La ejecución de estas acciones se está llevando a cabo en unos casos con recursos propios, y en otros, en alianza con organizaciones -públicas y privadas- que sean estratégicas en sus respectivos ámbitos de actuación y con una contrastada trayectoria dentro de la RSC.

Ello está en plena sintonía con el ODS 17 de la Agenda 2030 por su capacidad para fomentar y promover la constitución de alianzas eficaces en las esferas pública, público-privada y de la sociedad civil, aprovechando la experiencia y las estrategias de obtención de recursos de tales alianzas, tal y como se menciona en la meta 17 de este ODS.

Este objetivo no resulta en modo alguno extraño a esta Agencia, cuya actuación cotidiana está basada, precisamente, en la búsqueda continua de espacios de colaboración con los destinatarios de nuestras acciones: los responsables, públicos y privados, y los profesionales de la privacidad, a través de sus organizaciones, con vistas a facilitarles en lo posible el cumplimiento de sus obligaciones. Y, en sentido inverso, sin la implicación y la complicidad de estos colectivos no es posible llevar a cabo una actuación efectiva para proteger este derecho fundamental.

Así, pueden destacarse en este sentido la presencia por primera vez de la AEPD en la edición de este año de la Summer Summit, o la colaboración que hemos iniciado con algunas instituciones punteras en este campo, como la Fundación Koplowitz.

Compromiso con la ética y la integridad pública, la transparencia y el buen gobierno. La apuesta por una política de cumplimiento (compliance) en el sector público

Otro de los objetivos prioritarios que se pretende cubrir con el Marco de Responsabilidad Social es la adopción de un conjunto de medidas que, desde la perspectiva de la ética y la integridad públicas, que son los pilares básicos de la gobernanza pública, contribuyan a fortalecer su posición institucional y a mejorar la confianza de los ciudadanos en nuestra institución.

En particular, este plan realiza una apuesta firme por impulsar "una adecuada política de cumplimiento normativo (compliance), en colaboración con las asociaciones profesionales, basada en los valores de la Transparencia, el Buen Gobierno, la integridad, la rendición de cuentas, la participación, la profesionalidad y el servicio público.

En este sentido, resulta necesario destacar la regulación contenida en el artículo 24 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, a iniciativa de la AEPD, en el que se posibilitan los sistemas de información de denuncias internas.

Asimismo, la Agencia se ha dotado de un **Código Ético** para directivos y empleados con el que se explicita el firme compromiso por promover una cultura de integridad pública que favorezca el desarrollo de marcos internos de gestión, así como de modos de relación con los sectores afectados por su actividad (sector privado, sector público, sociedad civil y profesionales), que sean respetuosos con los mencionados objetivos y principios.

Más allá de las exigencias normativas y legales, con la aprobación de este Código se pretende estimular un modo de comportamiento que apunte hacia elevadas cotas de excelencia profesional, estableciendo los valores y principios que deben guiar las actuaciones y decisiones de los empleados de la Agencia. Es, por tanto, un instrumento que persigue la mejora del servicio público, mediante el buen hacer profesional y la innovación sistemática. Aspira también a reforzar la cultura organizativa de la Agencia, a estimular el orgullo de pertenencia a la misma; y a servir de ejemplo y referente para el resto de las instituciones públicas.

Es, además, fruto del convencimiento de que sólo desde la integridad de la función pública podremos, como Autoridad Administrativa Independiente, contribuir eficazmente a nuestro compromiso con la mejora social, económica y medioambiental, así como con los Objetivos de Desarrollo Sostenible de Naciones Unidas y las metas de la Agenda 2030, y en particular su ODS 16, que busca crear instituciones responsables, eficaces y transparentes que rindan cuentas (Meta 16.6).

Entre las medidas implantadas por el Código, destaca, sin duda, la puesta en marcha de un canal interno para atender consultas y denuncias de forma anónima sobre conductas contrarias al mismo. Este canal está a disposición tanto de los empleados, como de los ciudadanos y de los grupos de interés a través del espacio habilitado en la web de la Agencia.

Compromiso con los empleados

Centrándonos en los empleados, destacan especialmente las siguientes medidas:

- La aprobación del plan de igualdad, que incluye un protocolo para la prevención del acoso laboral y sexual y ayudas a empleadas víctimas de violencia de género.

- Reforzar el diálogo social con la representación del personal, haciéndoles partícipes de las acciones de responsabilidad social y promoviendo iniciativas de voluntariado corporativo.
- Desarrollar alianzas clave para impulsar el trabajo de las personas con discapacidad y poder adaptar los puestos de trabajo para ellas.

Pero, sin duda, hay que destacar las acciones puestas en marcha para la ampliación y mejora de la conciliación de la vida personal, familiar y laboral de los empleados y empleadas de la Agencia mediante el refuerzo y flexibilización del programa de teletrabajo, que se detalla en otros apartados de esta Memoria.

Con dicho programa, además de favorecer la conciliación de la vida familiar y laboral del empleado, se pretende evolucionar la organización del trabajo en la Agencia, pasando de un modelo basado en términos de presencia en el centro de trabajo a otro basado en la identificación de unos objetivos concretos y medibles y la comprobación de su consecución, independientemente del horario invertido. Como ventajas claras se ha comprobado que el teletrabajo facilita la conciliación de la vida laboral con la personal y familiar.

Este aumento de la capacidad de conciliación de la vida laboral, personal y familiar redunda en una mayor satisfacción del trabajador, y, en esa medida, tiene un impacto directo en otros ámbitos, como, por ejemplo, en la retención, fidelización y atracción del talento.

Otro de los efectos esperados con la conciliación es una mayor motivación y productividad. Este es un elemento muy difícil de medir en términos cuantitativos, especialmente en una organización pública, pero si se analizan las cifras de solicitudes de entrada, se puede observar cómo los empleados públicos han sido capaces de absorber un considerable incremento de un tercio adicional de reclamaciones, a la vez que han disminuido los tiempos medios de resolución. Con una plantilla estable en volumen, este fenómeno no habría podido tener lugar sin una gran motivación del personal y un cambio en la organización del trabajo.

En el programa de seguimiento del teletrabajo se incluye la evaluación sistemática y periódica del programa. Así, en una encuesta realizada a los trabajadores, tanto a las que ya están acogidos al programa como a los que no, los resultados obtenidos no han podido ser más positivos, confirmando la apuesta por seguir ampliando y mejorando su alcance. En concreto, el 83,56% de los teletrabajadores no percibe que haya variado su cantidad de trabajo realizado, y todos los supervisores coinciden en que no ha supuesto una variación en la carga de trabajo ordinaria de las empleados que realizan trabajos presenciales en la Agencia.

Compromiso por la protección del medio ambiente y la lucha contra el cambio climático

En cuanto al compromiso de la Agencia con la protección del medio ambiente, hay que destacar la necesidad de seguir profundizando en las medidas internas orientadas a la promoción de políticas de reciclado, el impulso de acciones de movilidad sostenible para empleados, el uso responsable del papel y una evaluación sobre el uso eficiente de los recursos energéticos.

Y, como medidas externas, se pretende potenciar las alianzas con organizaciones en proyectos medioambientales, y sumarnos a iniciativas, como la Comunidad #PorelClima y la Plataforma Española de Acción Climática, que agrupan a organizaciones públicas y privadas para promover la participación y la alineación de las estrategias de las entidades con las acciones gubernamentales, así como impulsar el Acuerdo de París y la evolución hacia una economía de bajas emisiones.

En este sentido, el Plan de RS realiza una apuesta clara por la adopción de acciones e iniciativas encaminadas a luchar de forma activa contra el cambio climático, bien impulsando programas de formación y de voluntariado ambiental de sus empleados, bien implantando medidas destinadas a reducir de forma significativa el impacto ambiental en todos los ámbitos (luz, agua, transporte, residuos, etc.)

A efectos de llevar a cabo una actuación integradora de todas estas medidas, se ha contratado a una empresa externa especializada para la adopción de la huella de carbono como indicador para medir los niveles de gases de efecto invernadero emitidos por parte de la Agencia y sus empleados.

3. Desafíos para la privacidad

3.1 Jurídicos

3.1.1 Consultas

Al igual que el ejercicio anterior, se observa que continúan las consultas sobre la adaptación al Reglamento General de Protección de datos. Esta tendencia subraya el interés tanto del sector público como del sector privado, no sólo de cumplir el RGPD, sino de estar en condiciones de acreditar dicho cumplimiento. Ello demuestra que, tras un año de aplicación del RGPD, conceptos como el principio de responsabilidad proactiva han influido decisivamente en los sectores implicados en el ámbito del derecho a la protección de datos.

En cuanto a las materias objeto de consulta cabe destacar que la plena aplicación del RGPD y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, sigue dado lugar a que se planteen cuestiones en directa relación con la interpretación de dichas normas, y que han supuesto un cambio respecto de lo realizado hasta ahora.

El nuevo paradigma que ha supuesto este cambio normativo, dando lugar a la pérdida de hegemonía del consentimiento como base jurídica que legitima el tratamiento, ha hecho necesario modificar interpretaciones muy asentadas para dar cabida a las otras bases jurídicas en un plano de igualdad. Por ello se ha hecho necesario revisar la adecuación al RGPD y a la LOPDGDD, de tratamientos de datos, que tradicionalmente encontraban acomodo en el consentimiento.

En este sentido cabe destacar, el **Informe 50/2019** emitido a solicitud del Consejo de Empadronamiento del Instituto Nacional de Estadística, acerca de la posibilidad de expedir certificados colectivos de empadronamiento por parte de los ayuntamientos, cuando no se dispone del consentimiento de todos los inscritos en la misma vivienda, ya sea porque dichas personas ya no viven en el domicilio o porque cuando se empadronaron no marcaron la casilla establecida al efecto en la solicitud de empadronamiento.

En el informe, partiendo de la ausencia de consentimiento, se analizan las restantes normas que les son de aplicación, como las relativas a las que regulan ciertas actividades de los entes locales pues son éstos los encargados de gestionar el padrón, y la interpretación que el Tribunal Constitucional ha realizado al respecto.

Se diferencian dos posibilidades en cuanto a la comunicación de la información que contiene el padrón municipal, dependiendo si los destinatarios son las administraciones públicas o si son los particulares, indicándose que *no constando el consentimiento expreso de los afectados, en el supuesto objeto de consulta el tratamiento únicamente podrá fundamentarse en el interés legítimo del solicitante del certificado o volante de empadronamiento, al amparo de los previsto en la letra f del artículo 6.1. del RGPD.* Asimismo se tiene en cuenta la regulación en la LOPDGDD que prevé en su Disposición Adicional Décima la posibilidad de que las administraciones públicas comuniquen datos a sujetos de derecho privado, cuando se disponga del consentimiento o se aprecie la concurrencia de un interés legítimo. El informe subraya la necesidad de realizar un juicio de ponderación adecuado, entre los derechos afectados y el interés legítimo del solicitante de la información, que compete al responsable del tratamiento, sin perjuicio de que el consultante, dada la variedad casuística que se puede plantear y la experiencia que le avala pueda determinar criterios orientativos que faciliten dicha ponderación.

Otro aspecto para destacar es el impacto que ha tenido la LOPDGDD en materias de gran calado en la población, como son los procesos electorales. Si bien durante 2018 se atendió todo lo relativo a

la aplicación del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, modificado por la disposición final tercera de la LOPDGDD, durante el año 2019 y también fruto de la misma disposición, se emitió el **Informe 21/2019**, relativo a la posibilidad de que los electores se opusieran a que sus datos fueran proporcionados a los representantes de los partidos políticos a los efectos de realizar envíos postales de propaganda electoral.

El informe analiza la naturaleza jurídica de dicha oposición, y la aplicación general y especifica de las normas que la regulan, indicando que los *tratamientos realizados al amparo de la legislación electoral se rigen por su normativa específica y supletoriamente por la normativa sobre protección de datos de carácter personal. Por lo que las solicitudes de los electores que se opongan a su inclusión en las copias del censo electoral que se faciliten a los representantes de las candidaturas para realizar envíos postales de propaganda electoral puede entenderse como una modalidad del derecho de oposición regulado en el artículo 21 del RGPD*.

Asimismo el informe destaca la necesidad de dar cumplimiento al derecho a la información y transparencia, al indicar que deberá informarse a los electores, tanto en las correspondientes oficinas como en la página web, del derecho que les asiste a solicitar su exclusión de las copias del censo electoral a los efectos indicados y subraya la circunstancia de que la ley no configura ninguna causa que legitime la denegación de la exclusión y propone que se de satisfacción a ese derecho en todo caso en el plazo máximo de un mes, prorrogable por otros dos meses atendiendo a la complejidad y al número de solicitudes, en los términos previstos en el artículo 12.3 del RGPD.

Finalmente, el informe recuerda la importancia de cumplir el principio de minimización de datos y limitación de la finalidad respecto de la información que se proporciona a los representantes de las candidaturas para la realización de envíos postales de propaganda electoral.

Como complemento del informe, en marzo de 2019 el Boletín Oficial del Estado publicó la Circular de la Agencia Española de Protección de Datos (AEPD) sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores.

El texto fijó los criterios de actuación de la Agencia en la aplicación de la normativa de protección de datos respecto al tratamiento relativo a opiniones políticas por los partidos al amparo del artículo 58 bis de la LOREG, con el marco del Reglamento General de Protección de Datos (RGPD) y conforme a lo establecido en la Constitución Española, de modo que no conculque derechos fundamentales.

La Circular fija obligaciones adicionales respecto al deber de información y el derecho de oposición, limitando la legitimación de aquellos que quieran ampararse en el 58 bis de la LOREG para tratar datos personales. En consecuencia, la AEPD mantuvo en la Circular su interpretación restrictiva de la modificación de la LOREG.

Sin embargo, la novedad más importante en relación con el tratamiento de datos en procesos electorales ha sido la STC 76/2019, de 22 de mayo, por la que el Pleno del Tribunal Constitucional declaró, por unanimidad, la inconstitucionalidad del artículo 58.bis.1 de la LOREG que había sido incorporado a dicha norma por la LOPDGDD.

La sentencia resolvió favorablemente el recurso interpuesto por el Defensor del Pueblo a solicitud de varias asociaciones civiles y personas vinculadas a ellas que, en atención a estas iniciativas, obtuvieron el Premio 'Buenas prácticas en privacidad y protección de datos personales' del año 2019, concedido por el Consejo Consultivo de la Agencia.

Especial atención merece el **Informe 36/2019** que resuelve las consultas que plantea la Conferencia de Rectores de las Universidades Españolas, para la elaboración de la guía de buenas prácticas en materia de protección de datos y transparencia. El citado informe realiza un análisis exhaustivo sobre el tratamiento de datos personales que se lleva a cabo en el ámbito universitario.

Comenzando por las bases jurídicas que legitiman el tratamiento de datos personales que realizan las universidades y teniendo en cuenta los variados escenarios que se plantean en la gestión universitaria.

Como punto de partida se excluye como base jurídica el consentimiento, pues con carácter general el tratamiento de datos personales derivado de la actividad de las universidades estará basado en las letras c) y e) del artículo 6.1 del RGPD, esto es, en el cumplimiento de una obligación legal o en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, de acuerdo con una norma con rango legal.

La consulta a la que se da respuesta propone determinados escenarios, entre los que cabe destacar, *las cesiones de datos relativos a las cantidades abonadas en concepto de complemento de productividad y gratificaciones* por servicios prestados fuera de la jornada normal de trabajo, así como a las *indemnizaciones por razón del servicio* (dietas) abonadas a personal de la universidad, siendo de aplicación el Criterio interpretativo conjunto del Consejo de Transparencia y Buen Gobierno y de la Agencia Española de Protección de Datos 1/2015 sobre obligaciones del sector público estatal a facilitar información sobre RPT y retribuciones, tanto en el caso de publicidad activa como en el ejercicio del derecho de acceso a la información.

El informe recuerda el criterio seguido en otros anteriores, respecto de la no procedencia de su comunicación a los representantes sindicales, al haber sido derogado tácitamente el último inciso del citado precepto por el artículo 40 de la Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público. Se subraya que en todo caso el acceso a los datos no debe dar lugar a tratamientos posteriores que puedan resultar contrarios a lo dispuesto en la legislación de protección de datos o genere situaciones en que pueda poner en riesgo los derechos de los empleados.

Asimismo para las universidades privadas, se indica que la publicación de los datos de productividad de los empleados podría encontrar su base legal en lo previsto en el artículo 6.1.f), es decir, en la satisfacción del interés legítimo del responsable o de un tercero. Éste podría ser la de incentivar la productividad de sus trabajadores, así como a un interés legítimo de los propios empleados, que de este modo podrán conocer su propio rendimiento en comparación con el resto de compañeros, garantizándose además la transparencia de este dato que tiene su correspondiente repercusión económica, siempre y cuando se adopten las debidas garantías por parte del responsable que permitan que no se identifique a los trabajadores por su nombre y apellidos, y que la exposición se realice en un ámbito al que solo tengan acceso los propios empleados.

Otro aspecto que analiza el Informe es el relativo a la *publicación de la producción científica del personal investigador* de acuerdo con la Ley de Ciencia, Tecnología e Innovación y que, en caso de llevar aparejado tratamiento de datos personales, encontraría su base jurídica en el apartado c) del artículo 6.1 c) RGPD, referido al cumplimiento de una obligación legal, no pudiendo ejercerse el derecho de oposición a dicha publicación.

Otras cuestiones respecto de las que no se exija su publicación en la normativa, el tratamiento podría basarse en el interés público cuando una ley formal así lo prevea, en cuyo caso podría ejercitarse el derecho de oposición. A falta de dicha ley formal, requeriría el consentimiento del afectado.

El informe también analiza otras cuestiones como el *acceso a los datos académicos de cargos públicos y a la publicación de dichos datos en el portal de transparencia de las universidades*, o el acceso a los contenidos de los trabajos de fin de grado, de fin de máster o de tesis, reconduciendo para los primeros a la aplicación de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, y para los segundos, y sin perjuicio de la normativa de propiedad intelectual, se remite a la normativa propia de cada universidad que sea de aplicación.

Especial atención merece otro aspecto de la consulta de gran calado social, como es el al *acceso de los progenitores a las calificaciones de sus hijos, económicamente dependientes*.

El informe reitera el criterio emitido en otras ocasiones, entendiendo apreciable un interés legítimo al amparo de lo previsto en el artículo 6.1.f), tal y como se razona detenidamente en el informe 36/2018.

La consulta plantea otras cuestiones de actualidad, como son la utilización de sistemas de grabación para diversos fines:

La grabación de imágenes en actos públicos organizados por la Universidad y su posterior divulgación en internet. El informe interpreta que si son actos organizados por las propias Universidades de acuerdo con lo previsto en sus Estatutos o en sus normas de organización y funcionamiento, en el ejercicio de su función de realizar el servicio público de la educación superior mediante la investigación, la docencia y el estudio, dicho tratamiento se encontraría amparado a tenor del artículo 6.1. e) del RGPD: "el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento", sin que por ello deba dejarse de informar en los términos previstos en el artículo 13 del RGPD.

El informe también analiza la adecuación a la normativa de protección de datos, la grabación de exámenes orales y de las sesiones de docencia. Respecto de los primeros, se determina que al amparo del artículo 46.3 de la Ley Orgánica de Universidades, éstas establecerán los procedimientos de verificación de conocimientos de sus estudiantes, garantizando los derechos que les asisten. Por lo que dicho tratamiento, encuentra su fundamento en el artículo 6.1 e) RGPD. En cuanto a los segundos, dependerá si se realiza por el propio docente, en cuyo caso se encontraría el mismo fundamento jurídico anterior, o si lo realiza la universidad, a efectos de control laboral, para lo que sería de aplicación la base jurídica prevista en el artículo 6.1 b) RGPD referida a la ejecución de un contrato.

Otros aspectos a destacar que trata el informe es el tratamiento de datos personales *de personas fallecidas, la cesión de datos a organizaciones sindicales y representantes de los trabajadores, la publicación de las calificaciones obtenidas por los alumnos, el tratamiento de datos de salud derivado de proyectos de investigación científica, la comunicación de datos a entidades aseguradoras, o la publicación de listados con identificación de participantes en procedimientos de concurrencia competitiva, cuando la publicación implica conocer situaciones que pueden dar un perfil de las condiciones sociales de una persona o unidad familiar, o suponer el tratamiento de categorías especiales de datos, y también se analiza la aplicación de la LOPDGDD a los censos electorales que publica la universidad*.

Como puede observarse el citado informe analiza prácticamente todos los aspectos derivados del tratamiento de datos personales, ya sea en el ámbito estrictamente universitario, ya sea en otros ámbitos, en la medida en que las universidades actúan en el tráfico jurídico, como empleador, titulares de sistemas de videovigilancia, tomadores de seguros, etc., *siendo extrapolables las conclusiones que en él se indican*.

En definitiva, se trata de un informe extenso y exhaustivo que trata multitud de aspectos referidos a la aplicación e interpretación del RGPD, LOPDGDD y otras normas conexas.

Una materia respecto de la que tradicionalmente se ha sometido a análisis es el tratamiento que realizan las administraciones públicas, destaca el **Informe 74/2019** sobre la adecuación al RGPD y LOPDGDD de las actuaciones de la Comisión de los Mercados y la Competencia en el ejercicio de sus funciones. El informe analiza el tratamiento de datos personales que lleva a cabo una autoridad pública en aspectos generales y sobre todo en el ejercicio de la potestad sancionadora (e inspectora). Del informe deben destacarse los siguientes aspectos:

La diferenciación que establece entre ejercicio de potestades administrativas y obligación legal, para determinar la base jurídica del tratamiento en sus diferentes actuaciones, y encuadrarse dentro del apartado c) (cumplimiento de obligación legal) o dentro del apartado e) (tratamiento necesario para el ejercicio de competencias o cumplimiento del interés público).

La potestad se trata de un poder genérico que sólo a través de su concreto ejercicio puede llegar a actualizarse y traducirse en un poder concreto, es decir, en un verdadero derecho subjetivo exigible por un tercero. Y una de sus características esenciales de la potestad, es la obligatoriedad de su ejercicio. Sin embargo, debe diferenciarse ese deber genérico de las obligaciones concretas que el ordenamiento jurídico pueda atribuir a la Administración. Para ello se acude al concepto de obligación contenido en el artículo 1088 del Código Civil ("toda obligación consiste en dar, hacer o no hacer alguna cosa"), siendo la primera fuente de las obligaciones la ley, según remarca el artículo 1089, añadiendo el artículo 1090 que "Las obligaciones derivadas de la ley no se presumen. Sólo son exigibles las expresamente determinadas en este Código o en leyes especiales, y se regirán por los preceptos de la ley que las hubiere establecido; y, en lo que ésta no hubiere previsto, por las disposiciones del presente libro".

Por ello, la base jurídica prevista en la letra c) del artículo 6.1. del RGPD será de aplicación en aquellos casos en los que una norma con rango de ley imponga a la Administración una obligación específica de dar, hacer o no hacer, que implique el tratamiento de datos de carácter personal (como por ejemplo cuando actúa como empleador, obligado tributario, en materia de transparencia etc.,) y diferente del deber jurídico genérico de la Administración de ejercer las potestades que el ordenamiento jurídico le atribuye para servir con objetividad al interés público (artículo 103 de la Constitución), en cuyo caso se estará ante la base jurídica prevista en la letra e) del artículo 6.1 del RGPD.

El informe cita expresamente que la licitud de los tratamientos de datos de carácter personal que realice la CNMC-DC encontrará su fundamento en la base jurídica del artículo 6.1.c) del RGPD (el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento) únicamente en aquellos casos en los que una norma con rango de ley imponga a la Administración una obligación específica de dar, hacer o no hacer, que implique el tratamiento de datos de carácter personal, y diferente del deber jurídico genérico de la Administración de ejercer las potestades que el ordenamiento jurídico le atribuye para servir con objetividad al interés público.

Se extrae la importante conclusión de que no toda la actuación que realice la administración pública, por estar prevista en la ley, e incluso en ocasiones definidas utilizando términos como *deberán, velarán, promoverán, vigilarán, etc*., encontraran la base jurídica del tratamiento en el cumplimiento de una obligación legal, pues corresponden a potestades genéricas que se situaran al amparo del ejercicio de competencias o del cumplimiento de una misión en interés público previsto por la ley.

Otro aspecto importante del informe son las comunicaciones de datos que contiene datos personales por parte de los ciudadanos, ya sean denunciantes, ya sean inspeccionados a dicha autoridad pública en el seno de los procedimientos que tramita.

Las denuncias y la solicitud de clemencia (un tipo específico de los procedimientos de la CNMC) encuentra su base jurídica en el apartado e) del artículo 6.1 e), sin embargo la contestación a requerimientos de información o la proporción de información en el seno de una inspección, es consecuencia del deber legal de colaboración y por tanto ese tratamiento encontrará su fundamento en la letra c) del artículo 6.1 del RGPD.

El informe también analiza el derecho a la información en el tratamiento de datos, diferenciando dos posibilidades, cuando los datos los recaba directamente la autoridad pública en el curso de sus actuaciones y cuando los datos llegan a dicha autoridad a través de un tercero investigado no titular de dichos datos. en el primer de los casos, se debe informar en los términos del artículo 13 del RGPD (en la primera recogida de datos, y únicamente en posteriores si se modifican aspectos esenciales del tratamiento) , mientras que en el segundo, la entidad que recogiera datos no está en obligación de informar de la eventual cesión a de los mismos a la autoridad cuando se requieran pues no puede considerarse ésta como un "destinatario" (artículo 4.9) del RGPD), respecto de los que se establece la obligación de informar.

Finalmente, en cuanto el ejercicio de derechos por los ciudadanos, (en el marco de las actuaciones de la CNMC, como autoridad pública) la normativa de competencia que es la que se aplica al consultante, no establece limitaciones específicas de los derechos, por eso el informe acude a las cuestiones generales por ejemplo para el derecho de acceso: deberá atenderse a la normativa común de procedimiento administrativo que desarrolla, con trámites específicos, el derecho de los interesados en un procedimiento administrativo a conocer, en cualquier momento, el estado de la tramitación de los procedimientos en los que tengan la condición de interesados y a acceder y a obtener copia de los documentos contenidos en los citados procedimientos recogido en el artículo 53.1.a) de la Ley 39/2015, lo que incluye el acceso a los datos personales que figuren en el procedimiento..

En cuanto al derecho de supresión, no resultará de aplicación conforme al artículo 17.3.b del RGPD, al ser el tratamiento necesario para para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.

En cuanto al derecho de oposición, indica el informe que en principio resultará de aplicación con carácter general, al tratarse de tratamientos legitimados en la letra e) del artículo 6.1. del RGPD, salvo en los supuestos concretos en que el tratamiento se fundamente en la letra c) de dicho precepto, según lo analizado anteriormente. No obstante, podrá denegarse el mismo por "motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado" conforme al artículo 21.1 del RGPD, al perjudicar el ejercicio de la potestad sancionadora e impedir la tramitación de los correspondientes procedimientos, tal y como específicamente ha reconocido el legislador al modificar, mediante la disposición final duodécima de la LOPDGDD el artículo 28.2 de la Ley 39/2015, que indica expresamente que *"No cabrá la oposición cuando la aportación del documento se exigiera en el marco del ejercicio de potestades sancionadoras o de inspección".*

Una consulta que merece especial atención por estar estrechamente vinculada con las posibilidades que ofrecen las nuevas tecnologías al servicio de la sociedad, es la resuelta mediante el **Informe 39/2019**. En la consulta que plantea el Ministerio del Interior, se analiza la adecuación a la normativa de protección de datos respecto del uso de datos personales en llamadas de emergencias a través del empleo AML (Advance Mobile Location) que es un mecanismo, ya desplegado en algunos países, por el que los centros de atención a llamadas de emergencia (servicios 112 y similares, conocidos como PSAP por su siglas en inglés) pueden recibir de forma automática información sobre la ubicación del llamante (cuando éste llama desde un teléfono móvil) con una precisión muy superior a la que puede obtenerse actualmente a través de la información que proporcionan los operadores de telefonía móvil, basada en la ubicación de la estación base desde la que se origina la llamada. AML es independiente del operador, ya que funciona sobre el teléfono móvil (directamente desde el sistema operativo, por lo que no requiere que el usuario descargue una app o realice una configuración previa). Cuando detecta que se está produciendo una llamada a un número de emergencias, AML activa la ubicación del móvil en alta precisión (típicamente obtenida a partir de redes WiFi o Bluetooth cercanas, o de un servicio GNSS, como GPS o Galileo) y genera un mensaje con las coordenadas de la ubicación. Los servicios de emergencias, conscientes de las mejoras que suponen el uso de AML en España, reclaman su puesta en funcionamiento. El informe analiza la aplicación e integración con la normativa de protección de datos, del Real Decreto 903/1997, de 16 de junio, por el que se regula el acceso, mediante redes de telecomunicaciones, al servicio de atención de llamadas de urgencia a través del número telefónico 112, indicando nuestro ordenamiento jurídico establece la obligación de facilitar a los servicios de emergencia los datos de localización, amparándose dicha obligación, entre otras circunstancias, en la necesidad de proteger el interés vital del llamante. El informe concluye que el tratamiento del dato de localización se

encontraría amparado en la letra d) del artículo 6.1. del RGPD: el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, independientemente de quién realice dicho tratamiento, ya que en este caso el factor determinante de la licitud del tratamiento es la protección de un interés esencial para la vida, tal y como destaca el Considerando 46. Asimismo, el informe recuerda el criterio mantenido por esta Agencia en las comunicaciones a las entidades municipales por la Comisión Nacional de los Mercados y la Competencia de los datos de los abonados al servicio telefónico para la prestación del servicio sobre números de abonado en el marco de las llamadas de emergencia. Respecto del derecho a la información en este novedoso sistema, se tiene en cuenta que el servicio no lo presta el operador que dé cobertura a la línea del dispositivo móvil en cuestión, sino que es independiente a este, por lo que las responsabilidades en materia de información, cumplimiento de los principios de minimización y limitación de finalidad, recaerán sobre la compañía titular del sistema operativo del dispositivo.

Un aspecto que tuvo en el 2018 un buen número de consultas y que continúa este ejercicio es el referido a la figura del Delegado de Protección de Datos. En este sentido destacan los informes **8/2019** y **100/2019**, dónde se analiza la figura propuesta por la Generalitat Valenciana y por el Ministerio de Defensa, respectivamente.

En ambos se llega a la conclusión de que el nombramiento y el número de delegados para una o varias unidades, así como sus competencias pueden realizarse en consideración a criterios orgánicos u organizativos, plasmados en normas jurídicas que dispongan la incorporación de esta figura a la estructura organizativa, preservando siempre y en todo caso el estatuto de independencia e imparcialidad de esta figura.

Sin embargo, es preciso destacar lo indicado en el **Informe 100/2019** que pone en valor la figura del delegado de protección de datos al incidir, una vez más, en la importancia que la figura del DPD tiene en el nuevo modelo instaurado por el RGPD y que pivota sobre la base de la responsabilidad proactiva del responsable. De acuerdo con el mismo, en los casos en que resulte obligatorio o así se haya estimado adecuado con carácter voluntario, ha de ser el responsable el que valore la procedencia de designar uno o varios DPD, así como si el mismo ha de pertenecer o no a su propia estructura, garantizando en todo momento su independencia y disponibilidad.

Igualmente corresponde al responsable garantizar que el DPD cumple con los requisitos de capacitación adecuados y que se le dota de los medios personales y materiales necesarios para la realización eficaz de las funciones que tiene encomendadas, que participa de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales y que rinde cuentas al más alto nivel jerárquico, documentando adecuadamente el responsable, conforme al ya citado principio de responsabilidad proactiva, todas las decisiones que adopte a este respecto, para poder demostrarlo a requerimiento de las autoridades de control.

Concluye el informe que únicamente así quedará garantizado que el nombramiento del DPD no se ha realizado con carácter meramente formal y que el mismo cumple eficazmente con las funciones que le asigna el RGPD, siendo el primer interesado en dicha eficacia el propio responsable, que es quien responderá, y no el DPD, en caso de inobservancia del RGPD.

Enlazando con la figura del delegado de protección de datos, y con el principio de responsabilidad activa, este Gabinete Jurídico ha resuelto varias consultas sin analizar el fondo del asunto planteado, pues éstas no acompañaban el criterio del delegado de protección de datos cuando ésta figura era exigible de acuerdo con el artículo 37 del RGPD y artículo 34 de la LOPDGDD.

Tal como indica la Exposición de motivos de la Ley 3/2018 "*la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración,*

adoptar las medidas que procedan", por eso en las consultas referidas, se aclara que le corresponde al delegado de protección de datos "actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto" (apartado e).

En este sentido, hay que indicar que el criterio del Gabinete Jurídico ha sido que son los responsables del tratamiento quienes deben acudir a su delegado de protección de datos, en primer término, y sólo en el caso de que éste tuviera dudas jurídicas, procederá elevar por parte del delegado, la correspondiente consulta a la que acompañar su criterio. Se da si cumplimiento a las funciones y competencias que la norma otorga a esta figura y que es una de las expresiones del principio de responsabilidad activa.

Finalmente hay que indicar en cuanto a la actividad de este Gabinete Jurídico, los **informes 18/2019 y 42/2019**, que testimonian una autentica función de producción normativa que se ha llevado a cabo, en relación con el anteproyecto del nuevo Estatuto de la Agencia Española de Protección de Datos y en relación con la Circular 1/2019, de 7 de marzo, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores.

3.1.2 Informes preceptivos

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.

Entre las disposiciones informadas en el año 2019 cabe mencionar las siguientes:

Proyecto de Orden Ministerial por la que se desarrolla la plataforma electrónica de gestión de residuos de aparatos eléctricos y electrónicos y la oficina de asignación de recogidas.

Real Decreto por el que se aprueba el estatuto de la Agencia Española de Protección de Datos.

Proyecto de Real Decreto de creación de la autoridad macroprudencial consejo de estabilidad financiera y de desarrollo y comunicación de herramientas macroprudenciales que pueden adoptar el Banco de España, a CNMV y la Dirección General de seguros y de fondos de pensiones.

Real decreto por el que se aprueba el reglamento de desarrollo de la Ley 22/2015, de 20 de julio, de auditoría de cuentas.

Proyecto de RD. que modifica el RD. 679/2014, de 1 de agosto, por el que se aprueba el Reglamento de control del comercio exterior de material de defensa, de otro material y de productos y tecnologías de doble uso.

Anteproyecto de Ley de Administración Digital de Galicia.

Proyecto de RD. por el que se desarrolla el reglamento de desarrollo de la Ley 19/2013, de 9 de diciembre, de Transparencia, acceso a la información y buen gobierno.

Proyecto de Real Decreto de establecimiento de un régimen gratuito de cuentas de pago básicas en beneficio del colectivo en situación de vulnerabilidad o con riesgo de exclusión social.

Proyecto de Real Decreto por el que se modifican los Reales Decretos 1850/2009 y 1614/2009.

Proyecto de Real Decreto de desarrollo parcial de la Ley 5/2019, de 15 de marzo, reguladora de los contratos de crédito inmobiliario y otras medidas en materia financiera.

Proyecto de Real Decreto por el que se regulan las condiciones en las que realizan sus funciones los servicios de auxilio en las vías públicas.

Proyecto de Real Decreto de régimen jurídico de los servicios de pago y de las entidades de pago y de modificación del Real Decreto 778/2012, de 4 de mayo, de régimen jurídico de las entidades de dinero electrónico.

Anteproyecto de Ley por la que se modifica el texto refundido de la Ley de Sociedades de capital, aprobado por Real Decreto Legislativo 1/2010, de 2 de julio, y otras normas financieras, en lo que respecta al fomento de la implicación a largo plazo de los accionistas en las sociedades cotizadas.

Proyecto de Real Decreto por el que se desarrolla el Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Asimismo deben citarse como informes preceptivos aquellos emitidos a tenor de lo dispuesto en el artículo 16.4 de la Ley 13/2011 de 27 de mayo de regulación del juego, relativos a la Homologación de los Sistemas Técnicos del Juego, que conforman un total de 32 y suponen un incremento exponencial respecto de los emitidos durante el ejercicio 2018 que se circunscriben a una consulta.

3.1.3 Sentencias

El análisis del grado de seguridad jurídica en la aplicación de la normativa de protección de datos obliga a contemplar en qué medida las Resoluciones de la AEPD son ratificadas o revocadas por los Tribunales.

Durante el año 2019 se han dictado por la Sala de lo contencioso-administrativo de la Audiencia Nacional, 189 sentencias[1], de las cuales:

- 100 fueron desestimatorias de los recursos formulados contra resoluciones de la Agencia (que quedaron plenamente confirmadas) (52%).
- 12 estimaron parcialmente los recursos (7%).
- 57 estimaron íntegramente las pretensiones anulatorias de las resoluciones de la Agencia (30%).
- 20 inadmitieron los recursos interpuestos contra resoluciones de la Agencia (11%).

En cuanto a los sectores de actividad de los recurrentes, de 208 recursos interpuestos frente a las resoluciones de la AEPD, la mayor parte han sido interpuesto por particulares (64.) No obstante, un alto número de ellas son desestimados, bien por la falta de legitimación activa del denunciante cuando únicamente se pretende la imposición de una sanción en un procedimiento, bien porque no se han aportado datos suficientes para abrir una actuación investigadora, o bien porque las cuestiones denunciadas eran ajenas al ámbito competencial de la AEPD.

Seguido del sector banca y seguros (37), y los servicios de la sociedad de la información, entre los que se engloban los prestados a través de internet (26). Tras ellos figuran el sector de la publicidad y prospección comercial (18). Con igual número de recursos (16) están los sectores de telecomunicaciones y lo relacionado con los sistemas de información crediticia (ficheros de solvencia patrimonial). Los restantes sectores

[1] Únicamente se refiere a Sentencias, quedando por tanto excluidos los Auto que resuelven los recursos contencioso-administrativos en los que se ha producido el desistimiento.

como energía, asociaciones sindicales, o distribución y venta de productos, son los menos significativos cuantitativamente y se mantienen en términos similares al ejercicio anterior.

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

En cuanto al ámbito territorial de aplicación de la normativa de protección de datos (LOPD y Directiva 95/46 CE), es preciso citar la Sentencia de 21 de junio de 2019, que resuelve el Recurso nº 342/2017, dónde se analiza la noción de establecimiento.

En concreto se trata de una entidad sin sede en el espacio económico europeo, que contrata a un encargado del tratamiento en España para concesión de préstamos y, en su caso, acciones de recobro.

El tribunal considera varios elementos: la concesión de préstamos por parte del encargado, se realizaba a través de un dominio web .es, que era propiedad de la recurrente, también considera relevante que la inclusión en ficheros de morosidad de los clientes que no abonaban sus préstamos lo realizara dicha entidad, como también se tiene en cuenta que el Boletín Oficial del Registro Mercantil, la citada entidad encargada del tratamiento, tuviera como socio único a la sociedad recurrente, siendo administrador solidario el representante legal de la sociedad recurrente.

En definitiva, las actividades que realizaba la entidad sancionada se llevaban a cabo por otra empresa en virtud de un contrato para la gestión integral de servicios que disponía de los medios necesarios para la prestación de los servicios concretos de que se trate en España, con un domicilio en Madrid diferente al fiscal, para recibir las notificaciones de la recurrente, así como para ejercitar los derechos de acceso, rectificación, cancelación y oposición además de prestar, dicho encargado de tratamiento, los servicios de atención a clientes de aquella, así como la verificación y servicio de cobro de deudas tanto en vía amistosa, como cuando procediera, en vía administrativa.

Considera la sentencia, que la noción de establecimiento se trata de un concepto de carácter funcional, en cuanto supone el ejercicio y desempeño efectivo de las atribuciones determinantes del tratamiento de datos, fijación de los fines y medios. Y concluye que la recurrente dirigía de forma regular actividades y operaciones a través de medios instrumentales radicados en España, adoptando decisiones relativas a los fines y medios del tratamiento de datos, entrando dentro del concepto legal de establecimiento del art. 2.1.a) de la LOPD en relación con el art. 4.1.a) de la Directiva 95/46/CE.

Respecto al concepto de dato de carácter personal, conviene destacar la interesantísima **Sentencia recaída en el Recurso nº 146/2018 de fecha 23 de julio de 2019**, que analiza la denegación de un derecho de acceso por parte de una empresa de seguridad, a los registros (logs) que constataban las veces que el sistema de alarma instalado en la vivienda había saltado por considerar dicha entidad que no eran datos de carácter personal. En concreto se solicita *la información relativa a los registros y señales enviados por el equipo de alarma instalado en su propiedad, así como las copias existentes de los registros contenidos en la memoria interna de la alarma*. El tribunal no comparte esa apreciación y valida el criterio de esta Agencia al considerar que lo esencial, a efectos de la normativa de protección de datos, es que la información haga referencia a una persona física identificable, es decir, que razonablemente y sin grandes esfuerzos sea posible asociar los datos proporcionados a una determinada persona (SSAN de 8 de marzo de 2002 y de 20 de noviembre de 2012, Rec. 188/2011). En el supuesto analizado se trata de una persona física, y por tanto plenamente identificable, que firma un contrato de instalación y mantenimiento de una alarma para la protección de su vivienda con la empresa de seguridad. Asimismo, el derecho de acceso se ejercita respecto de registros y señales captadas y enviadas por el equipo de alarma instalado en un domicilio privado, ejerciéndose precisamente por parte de quien es titular de dicho domicilio que coincide con el titular del contrato, resultando por tanto fácilmente identificable. Por lo que teniendo en cuenta estos elementos la información a la que se pretende acceder, es considerada como dato de carácter personal.

En relación con el tratamiento de categorías especiales de datos, y en concreto, datos de salud, conviene destacar las **Sentencia recaída en el Recurso nº 622/2016 de 29 de noviembre de 2019**, que analiza la publicación de datos – de salud- referidos a víctimas del atentado ocurrido en Madrid el 11 de marzo de 2004. Los datos han sido obtenidos de las sentencias recaídas en diversos procesos judiciales llevados a cabo a raíz del atentado, entrando en juego el derecho a la información previsto en el artículo 20 de la Constitución y el principio de publicidad de las sentencias según la Ley Orgánica del Poder Judicial. Pues bien, la sala de instancia resuelve que dicho principio de publicidad de las sentencias no es absoluto y en el caso analizado debe ceder frente al derecho a la protección de datos, confirmando así el criterio de la AEPD.

Continuando con las *categorías especiales de datos*, y en concreto, si una determinada información puede considerarse tratamiento de datos de salud, procede citar la **Sentencia de 15 de febrero de 2019**, recaída en el recurso 62/2018, que analiza una comunicación interna de una entidad bancaria en la que varios trabajadores hablan sobre el estado de salud mental de una cliente. En concreto se analiza la expresión "*… comentarte que al parecer tiene un trastorno de bipolaridad del que se trata*". El tribunal considera dicha información como mera opinión personal de los trabajadores, subrayando el término "al parecer", excluyendo de la misma cualquier connotación relativa a tratamiento de datos de salud.

En cuanto a la legitimación para el tratamiento de datos, al amparo del artículo 6 de la derogada LOPD, y en concreto los supuestos de existencia de relación jurídica que necesita del tratamiento para su ejecución, conviene citar aquellas sentencias que estiman la existencia de contratación irregular. Como por ejemplo las de **20 de septiembre de 2019** recaída en el recurso nº 263/2017, o la de **7 de junio de 2019**, recaída en el Recurso nº 665/2018.

En este ámbito es preciso destacar la **Sentencia de 11 de octubre de 2019**, que resuelve el recurso nº 236/2018, que considera que no hubo una contratación diligente en el ámbito de un producto de telecomunicaciones, al no cumplirse los requisitos previstos en la Circular 1/2009 de la Comisión del Mercado de Telecomunicaciones, referida a la verificación del consentimiento verbal por tercero independiente.

En lo relativo al tratamiento de datos personales en acciones de *mercadotecnia*, debe tenerse en cuenta que, si bien es un sector importante en la economía, las entidades que lo conforman, no puede dejar de observar los deberes y cautelas que impone la normativa de protección de datos, pues los principales destinatarios de esas acciones serán personas físicas titulares del derecho subjetivo a la protección de datos. Consciente de ese necesario contrapeso, la AEPD ha sancionado conductas contrarias a la normativa de protección de datos que han sido confirmadas por la Audiencia Nacional, entre las que cabe destacar las siguientes:

Destacan en primer lugar los recursos nº,810, 811,812,813, 814,815,816 de 2016 y los recursos nº 222, 223 y 433 de 2017, resueltos en el año 2019, y que tienen como responsable de las diez sanciones a una entidad proveedora de bases de datos para acciones de mercadotecnia y al beneficiario de esa publicidad.

La importancia de estas sanciones impuestas por la AEPD y que son confirmadas por la Audiencia Nacional reside en que la entidad en cuestión llevaba operando en el sector desde hace años y utilizaba un entramado de empresas instrumentales, para comercializar bases de datos que no cumplían la normativa de protección de datos y así evitar cualquier acción de la AEPD y seguir operando con normalidad.

Las sentencias analizan la aplicación de la doctrina del *levantamiento del velo* a los hechos analizados por la AEPD en los procedimientos sancionadores, y resalta la intensa actividad probatoria que se realiza para concluir que la entidad que figura como mero encargado del tratamiento (la entidad sancionada) es realmente la que toma las decisiones y proporciona las bases de datos,

y que la supuesta entidad responsable del fichero utilizado en las campañas publicitarias, es en realidad una empresa instrumental, sin sede física, ni apenas medios materiales y humanos.

En cuanto al fondo del asunto, la sentencias confirman las sanciones que imponen la AEPD tanto, al proveedor de las bases de datos, como a la empresa beneficiaria de la publicidad, en la medida en que del elenco probatorio se acredita que una es la responsable del fichero, y la otra la responsable del tratamiento, en la medida en que determinó los parámetros identificativos de los destinatarios, y contrató con una entidad sin demostrar la diligencia suficiente que requiere el artículo 46.3 del Real Decreto 1720/2007, de 21 de diciembre (RDLOPD)

Asimismo, en estos recursos se analizan cuestiones formales y sustantivas referidas al procedimiento sancionador, como son los cómputos de plazos, las solicitudes de prueba, su admisión y denegación, así como la actuación de la actuación de los servicios de inspección de la AEPD, confirmándose en todos los casos, la postura sostenida por este organismo.

En el mismo sentido, la **Sentencia de fecha 22 de octubre de 2019**, recaída en el Recurso nº 61/2008, destaca la aplicación del citado artículo 46 del RDLOPD, a la hora de determinar la condición de responsable del tratamiento en campañas publicitarias, validando el criterio de la AEPD referente a que la entidad denunciada, ostentaba dicha condición a pesar de no haber tenido contacto con ninguna clase de datos personal, simplemente por haber determinado los parámetros que establecen los destinatarios de las campañas.

Otra sentencia que versa en principio con el tratamiento de datos personales en campañas publicitarias centra su exposición en la sanción por la infracción relativa a la obstrucción a la labor inspectora. Así la **Sentencia de 12 de julio de 2019**, recurso nº 128/2018 considera probada la infracción a la vista de los comunicados del denunciado referidos a que no iba aportar la documentación requerida y teniendo en cuenta que el día de la inspección presencial en la sede de la entidad, se ausentó con la finalidad de eludir la acción de la AEPD a pesar de haber sido notificado de la fecha y hora en que se iba a producir.

En el ámbito de los sistemas de información crediticia, coloquialmente conocidos como ficheros de morosos, se distinguen distintos temas relevantes para dar cumplimiento al principio de calidad del dato o exactitud que debe informar cualquier tratamiento de datos en este ámbito.

Destaca en primer lugar aquellos supuestos cesión de cartera o compra de deuda, en los que el adquiriente de la deuda pasa a ostentar la posición del acreedor y a figurar así en los referidos sistemas de información.

En estos casos, las **Sentencias recaídas en los recursos nº 501y 773 de 2016, y 77, 79, 82, 86 y 134 de 2018,** consideran que no es necesario realizar un requerimiento previo a la inclusión, en aquellos supuestos en los que los datos del deudor ya estuvieran incluidos en el fichero de morosos. Es decir, el nuevo acreedor no tiene la obligación de realizar la notificación prevista en los artículos 38 y siguientes del RDLOPD.

Otro aspecto importante en el ámbito de la compra de deuda es la relación entre el cedente y cesionario y la diligencia de éste a la hora de tratar los datos del deudor e informar los datos a un fichero de solvencia patrimonial. En la **Sentencia de recaída en el Recurso nº 534/2017**, se anula la sanción impuesta por la AEPD, al considerar que el adquiriente de la deuda actúa de buena fe, en el sentido de que el cedente le garantiza por contrato, la existencia relación jurídica con el deudor que dota a la deuda de cierta, vencida y exigible.

Al contrario sucede con la **Sentencia de 15 de octubre de 2019**, recaída en el Recurso nº 521/2017, en la que el cedente informaba en el contrato de cesión de deuda, que el cesionario se abstuviera de incluir los datos en el fichero de morosos, ante la posibilidad de que la deuda fuera discutida.

Un tercer tema recurrente en el tratamiento de datos referido a la inclusión en sistemas de información crediticia, es *la inexistencia de la deuda*.

En estos casos, se suele atribuir la comisión de la infracción del principio del consentimiento (en términos de la derogada LOPD) y la del principio de calidad de datos. En la **Sentencia de 16 de julio de 2017**, recaída en el recurso nº 751/2016, se niega la concurrencia del concurso medial de infracciones que sostenía el recurrente, pues se deja claro que ambas infracciones son independientes, recogiendo así la doctrina consolidada en otras sentencias como las de 29 de enero y de 24 de junio de 2014 (recurso 562/12 y 141/2013).

Otro tema relacionado con el tratamiento de datos personales en sistemas de información crediticia es la consulta de los mismos por terceros sin que concurran los supuestos legales. Así en la **Sentencia de 18 noviembre de 2019** recaída en el recurso nº 260/2018, se analiza el acceso al fichero de morosos por parte de una entidad al amparo del consentimiento otorgado por un cónyuge, considerándose incumplido el artículo 42.1 del RDLOPD.

Finalmente, en cuanto al requisito referido a la inexistencia de reclamación que cuestione la certeza de la deuda, en virtud de la que los datos han sido incluidos en los sistemas de información crediticia, destacan las **Sentencias de 9 de mayo de 2019** (recurso nº 688/2016) **y la de 10 de mayo de 2019** (recurso nº 142/2018). Las citadas resoluciones se refieren a la existencia de un proceso de reclamación en la Secretaria de Estado de Telecomunicaciones derivado de la contratación de un servicio a un operador, y la otra a un proceso civil que impugna las cláusulas abusivas del prestador hipotecario.

En el ámbito de las transferencias internacionales de datos, destacan las **Sentencias de 29 de abril y 17 de mayo de 2019**, recaídas en los recursos 396/2017 y 397/2017 respectivamente. El tribunal confirma las sanciones impuestas por la AEPD en un asunto que genero cierta alarma entre los responsables de tratamiento que tuvieran contratados servicios con entidades ubicadas en Estados Unidos.

La transferencia internacional que se preveía en el contrato de encargado de tratamiento, ubicado en EEUU tenía como base jurídica la Decisión CE 2000//520/CE, sin embargo, desde la invalidez de dicha Decisión por la sentencia del Tribunal de Justicia de la Unión Europea (TJUE) C-362/14, de 6 de octubre de 2015, era necesario que aquellas entidades que hayan transferido datos a Estados Unidos encontrarán amparo legal en el artículo 33 de la LOPD.

Las entidades recurrentes siguieron conservando los datos alojados en servidores en dicho país hasta el mes de septiembre de 2016, sin autorización previa de la Directora de la AEPD, ni amparo legal alguno, incurriendo en la citada infracción. Todo ello a pesar de que tras la Sentencia C-362/14 de 6 de octubre de 2015, la AEPD notificó a los responsables que se encontraran en esa situación, la necesidad de adecuar dicho tratamiento al ordenamiento jurídico vigente.

En cuanto al cumplimiento del deber de secreto, actualmente deber de confidencialidad, destaca la **Sentencia de 27 de septiembre de 2019**, que resuelve el recurso nº 652/2018. Se analiza un *supuesto clásico* en este ámbito, referido a la publicación en tablones de anuncios de una comunidad de vecinos, los datos de aquellos propietarios que tienen deudas con la comunidad.

Otro tema que se ha dado con asiduidad en relación con la vulneración del deber de secreto es el acceso a través del perfil de usuario en internet por parte de un cliente de un servicio de telecomunicación, o de energía, a los datos de otro cliente. La **Sentencia de 14 de mayo de 2019** (recurso nº 944/2018) confirma la sanción impuesta por la AEPD, que no considera que existe falta de culpabilidad por haber acontecido un error informático, como alegaba la recurrente. Se recoge así la doctrina consolidada que determina que el error informático no excluye la antijuridicidad, "son muchas las sentencias en que se ha insistido en que los errores informáticos no son suficientes para eliminar la antijuridicidad de las conductas sancionadas. Así en las sentencias dictadas en los Rec. 110/2013 o 368/2012)".

En lo que respecta al ejercicio de los derechos de acceso, rectificación, cancelación, y oposición (en los términos utilizados por la LOPD, y actualmente sustituidos por los de acceso, rectificación, oposición, supresión, limitación y portabilidad) debe indicarse lo siguiente:

En relación con el derecho de supresión en internet, y en concreto el derecho al olvido en las búsquedas en internet (previsto en la actual LOPDGDD en su artículo 92), el tribunal tiene en cuenta los criterios de ponderación fijados en la Sentencia del TJUE de 13 de mayo de 2013, entrando en liza los derechos fundamentales a la el derecho a la libertad de información y de expresión, consagrados en la Constitución, y el interés legítimo del responsable del buscador como el interés público de los usuarios del mismo, en conocer determinada información en relación con las especiales circunstancias de cada tratamiento y de otro lado, el respeto a la protección de datos y a la intimidad del afectado por el resultado de la búsqueda en internet.

Se confirma el criterio de la AEPD en la **sentencia de 22 de abril de 2019**, que resuelve el recurso nº 343/2017, que ordena suprimir los resultados de búsqueda relativos a la implicación del afectado en un proceso judicial del que finalmente fue absuelto. El tribunal centra sus argumentos en si bien en el momento de su publicación, los datos no eran inexactos, se han convertido en tales; en cuanto datos no actualizados y en definitiva excesivos por el transcurso del tiempo, una vez dictada la sentencia absolutoria de los hechos a los que se refieren las informaciones ofrecida en las referidas URL, ninguna de las cuales lleva a cabo ni la más mínima rectificación, ni tampoco la más mínima alusión a dicha sentencia absolutoria. Se concluye que, en el momento actual, y por los motivos expuestos, no se trata de una persona de relevancia pública que pudiera determinar, ni un especial interés público de dicha información ni justificar un interés preponderante del público en tener acceso a la misma en el marco de una búsqueda a través del nombre de tal interesado.

Por el contrario, son numerosas las sentencias que estiman las pretensiones del recurrente, el responsable del motor de búsqueda, en atención a la relevancia pública del afectado y a que los datos han sido publicados anteriormente por el propio afectado.

Destaca la **Sentencia de 20 de diciembre de 2019** que resuelve el Recurso nº 386/2018 en la que se razona que el derecho a la libertad de expresión (artículo 20 CE), que es más amplia que la libertad de información, al no operar en el ejercicio de aquél el límite interno de veracidad que es aplicable a ésta, se justifica porque tiene por objeto presentar ideas, opiniones o juicios de valor subjetivos que no se prestan a una demostración de su exactitud, ni a sentar hechos o afirmar datos objetivos, ni por su naturaleza abstracta son susceptibles de prueba

Considera el tribunal que dado el escaso tiempo transcurrido desde la publicación del blog cuestionado y el papel desempeñado por el afectado en la vida pública, estaría justificado el interés del público en acceder a la información publicada, por lo que han de prevalecer los derechos de libertad de expresión e información respecto del derecho a la protección de datos personales del afectado, al existir, por los expresados motivos, un interés legítimo de los internautas potencialmente interesados en tener acceso a la información en cuestión, que prevalece sobre el derecho de protección de datos personales del afectado (párrafo 81 de la STJUE de 13/05/2014).

En la **Sentencia de 21 de junio de 2019**, que resuelve el Recurso nº 106/2018, se determina que los datos afectado objeto de publicación remiten a información actual y de relevancia pública incuestionables, que en ningún caso puede considerarse obsoleta.

Concurre en el supuesto analizado por la sentencia una importante elemento a la hora de ponderar los derechos fundamentales en juego, y es que los enlaces en cuestión y el tratamiento de los datos personales que en ellos se efectúa, no se circunscribe y ni siquiera se refiere, a la vida personal del afectado, sino exclusivamente a la vida profesional del mismo, en cuanto Director de una empresa y Consejero Delegado una multinacional ocupando en la actualidad, conforme al Registro Mercantil cargos de responsabilidad hasta en seis sociedades.

Tampoco pueden ser considerados obsoletos, al tratarse de noticias publicadas en la prensa económica especializada en los años 2012 y 2013 que además ha de ser considerada información de interés general, que trasciende del ámbito personal al situarse en un contexto profesional de quien ha ostentado un importante cargo empresarial en la filial española de una empresa nipona. Se trata de presuntas irregularidades contables que parecen transcendentes y que actualmente siguen siendo de interés general.

En el **recurso nº 217/2018**, se analiza la publicación en un diario digital la declaración prestada por el alcalde de un municipio de Galicia, ante la titular del Juzgado de Instrucción nº 3 de Villagarcía de Arousa, en el curso de la investigación de una denuncia interpuesta contra él por una concejal de la misma corporación municipal, por delitos contra la libertad sexual. Considera el tribunal que en dicha noticia no se imputa la comisión de ningún delito sino se da cuenta con objetividad de una denuncia y de las declaraciones realizadas voluntariamente por el propio alcalde tras declarar en el Juzgado en las que alude también al apoyo de sus compañeros de gobierno y a la no convocatoria de un pleno para tratar de dicho asunto como le pedía la oposición.

Debe tenerse en cuenta, como otro de los factores relevantes en la ponderación de intereses a realizar, que se trata de una información referida a una persona de proyección pública, el alcalde de un municipio, como así lo viene a reconocer la propia AEPD "el reclamante es una persona de proyección pública por su cargo político, alcalde de un municipio de Pontevedra". Además, resulta de declaraciones públicas recogidas por otros medios de comunicación, como el Faro de Vigo, obrantes al expediente, el alcalde contribuyó activamente al debate público, al acusar a la oposición de llevar a cabo una campaña de acoso y derribo político contra él. Todo lo cual no viene sino a poner de relieve el interés público de la información.

También relacionado con la publicación de procesos judiciales en los que se relaciona a los afectados, en la **Sentencia de 21 de junio de 2019**, que resuelve el recurso nº: 0000215/2018 pone en valor que los enlaces que muestran los resultados de búsqueda hacen referencia a los procedimientos penales en los que estuvo implicado el codemandado, que no continúan contra él. Añade el tribunal que la libertad de información no viene condicionada por el resultado de los procesos penales -Sentencias de la Sala de lo Civil del Tribunal Supremo de 31 de mayo de 2001, recurso nº. 1.230/1996, y de 16 de octubre de 2012 recurso nº. 2.050/2010-. Maxime la relevancia social que tienen los casos en que estuvo implicado el codemandado. Y tiene en cuenta que siguen apareciendo noticias que relacionan al afectado con implicados en las citadas causas, y en otras. Concluye el tribunal que estamos ante informaciones sobre la actividad profesional del reclamante en su faceta de empresario, con una relevancia profesional en relación con asuntos de penales de muy notoria relevancia social, existiendo un interés legítimo de los internautas en tener acceso a dichas publicaciones, siguiendo con la publicación de noticias sobre la involucración del reclamante en lo investigado judicialmente en los medios de comunicación.

Otro supuesto que la Audiencia Nacional a analizado en relación el derecho de supresión en internet, es la publicación de datos personales de los afectados en listas electorales, y que éstos han solicitado su eliminación.

En la **Sentencia de 9 de mayo de 2019**, recaída en el recurso nº 491/2017 se considera que se trata de una persona que ha realizado una actividad política como integrante de un partido político que ha concurrido a diversas elecciones durante varios años, por lo que existe un interés legítimo de los internautas en tener acceso a dicha información, que ha sido publicada en la prensa local, además de que la publicación de las listas electorales resulta legalmente obligada en determinados medios oficiales. Concluye la sentencia que estamos ante un tratamiento de datos inicialmente lícito por parte del buscador Google, que, dado el contenido de la información, las vicisitudes de una persona dedicada a la actividad política y el poco tiempo trascurrido, continúan siendo necesarios en relación con los fines para los que se recogieron o trataron.

En la **Sentencia de 11 de enero de 2019**, que resuelve el recurso nº 345/2017, se tiene en cuenta que en el enlace donde aparece el nombre y apellidos del afectado, se accede a un diario digital donde se publica la lista de candidatura municipal correspondiente al año 2011 de un municipio de Navarra. También se tiene en cuenta que el afectado en la actualidad es policía local en otro municipio de la misma región. Dicha información para la Sala si tiene la suficiente relevancia, que justifica que prevalezca el interés del público general.

Finalmente debe citarse la **Sentencia de 26 de marzo de 2019** recaída en el recurso nº 469/2017, en los que el afectado solicita que sus datos personales no se asocien a la publicación en unos blogs en los que se anuncia la retirada en una revista universitaria de un artículo publicado por éste, por haber plagiado texto de otros autores. El afectado alega en su favor que no se ha iniciado ninguna actividad disciplinaria por la universidad en torno a los hechos publicados, aportando un certificado al efecto. La Sala considera que esa circunstancia, en absoluto desvirtúa las propias declaraciones del reclamante que reconoció que dicha una revista de la universidad había retirado su artículo y había publicado una nota al respecto, si bien se escuda en que la nota no fue publicada en la página web de la revista sino solo en la edición impresa, por lo que considera que debe permanecer en la esfera de la relación entre autor-revista y lectores suscritos.

La Sala como elemento de cierre considera que el afectado ejerce su actividad, en la actualidad, como Investigador y Profesor de Sociología en una universidad pública, escribiendo de forma asidua artículos doctrinales y colaborando con distintos medios de comunicación. Por todo ello estima el recurso planteado por el buscador y permite que se sigan indexando los enlaces sobre los que se solicitó su eliminación.

En lo que se refiere a cuestión procedimentales o de aplicación del derecho administrativo general derivada de la actividad sancionadora de la AEPD, destaca en primer lugar la **Sentencia de 23 de abril de 2019** que anula una sanción impuesta por vulneración del deber de secreto a un buscador que al satisfacer el derecho de supresión, indicaba en el resultado de búsqueda la circunstancia de la eliminación del enlace, pero mostraba dónde podía encontrarse la información. También se sanciona en la resolución de la AEPD por la comunicación que realiza el buscador al responsable de la página web de que su enlace ya no se muestra en los resultados de la búsqueda por entender que iban aparejados datos personales. La resolución sancionadora apoya sus argumentos en criterios novedosos sentados por el Tribunal de Justicia de la Unión Europea y por el Grupo de Trabajo del Articulo 29 (actualmente Comité Europeo de Protección de Datos)

La cuestión de fondo es que la Sala considera que la AEPD ha establecido un criterio general de aplicación, con base en un procedimiento que afectaba únicamente tres denunciantes y concluye que no es el medio idóneo para fijar criterios interpretativos generales sobre una cuestión novedosa y compleja.

Es importante indicar que otras sentencias ya citadas en la presente memoria, analizan cuestiones ajenas a la protección de datos que merecen ser citadas en este apartado. Se consolida la validez de la notificación electrónica de los actos administrativos, considerándose como practicada el día de puesta a disposición en el buzón electrónico del destinatario, con independencia de que no se acceda a él transcurrido el plazo al efecto. También en relación con las notificaciones de actos administrativos, la **Sentencia de 13 de septiembre de 2017**, considera conforme a derecho la notificación practicada por una empresa de mensajería con acuse de recibo, otorgándole la misma validez que la que pudiera realizar la Sociedad Estatal de Correos y Telégrafos.

Especial mención merece la **Sentencia de 15 de octubre de 2019**, recaída en el recurso nº 521/2017, que considera que no procede discutir en sede judicial el contenido del recurso frente a una resolución sancionadora donde el investigado se ha beneficiado de las reducciones previstas en el artículo 85 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Se pone el acento en la previsión del apartado 1 del citado artículo referido al reconocimiento de la responsabilidad en la comisión de la infracción, e interpreta que no es conforme discutir en esa instancia judicial hechos respecto de los que se ha asumido su responsabilidad. Por dicha razón desestima el recurso.

Por su parte, el Tribunal Supremo dictó un total de 4 resoluciones, un Auto de inadmisión 26 de abril de 2019, derivado del recurso de casación interpuesto por un particular por carecer de legitimación activa. Las Sentencias de 5 de febrero de 2019 y de 10 de diciembre de 2019, que estiman el recurso del Abogado del Estado en representación de la AEPD. Y la Sentencia de 11 de enero de 2019, que desestima el recurso de casación interpuesto por un buscador de internet frente a la confirmación de una resolución de la AEPD.

En consecuencia, el Tribunal Supremo confirmó en los 4 asuntos que llegaron a su conocimiento el criterio que había mantenido la Agencia Española de Protección de Datos.

También el Tribunal Constitucional se ha pronunció en Sentencia de 22 de mayo de 2019, Rec. 1405/2019, que declara contrario a la Constitución y nulo el apartado 1 del artículo 58 bis, incorporado por la disposición final tercera, apartado dos, de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

En resumen, la disposición recurrida ante el Tribunal Constitucional considera que la recopilación por los partidos políticos de datos personales relativos a opiniones políticas de los ciudadanos está amparada en el interés público cuando se ofrezcan garantías adecuadas.

Sin embargo, el Alto Tribunal entiende que las opiniones políticas de las personas son datos sensibles que necesitan un nivel superior y específico de garantías que salvaguarden su tratamiento y que la norma impugnada no identifica el interés público que justifica la recopilación de datos personales que revelen opiniones políticas, sino que solo lo invoca de manera genérica e indeterminada.

También echa en falta el tribunal una regulación pormenorizada de los presupuestos y condiciones en los que procede la recopilación de datos, pues la alusión al marco de actividades electorales de los partidos políticos no proporciona reglas claras y precisas que delimiten la injerencia al derecho fundamental de protección de datos personales.

Otro aspecto importante de la sentencia es que se declara vulnerado el principio de reserva de ley orgánica, ya que las garantías adecuadas a las que se alude no están incorporadas en la propia regulación, ya sea directamente o por remisión expresa a fuentes externas con rango normativo adecuado.

Finalmente debe hacerse referencia a la jurisprudencia europea recaída en el ámbito del derecho a la protección de datos y a la privacidad.

EL Tribunal de Justicia de la Unión Europea en Sentencia de 14 de febrero de 2019, (C-345/17), analiza la publicación en internet de un vídeo grabado por el afectado de su declaración en las dependencias de una comisaría de la Policía Nacional en el marco de un expediente administrativo sancionador.

Siendo finalmente sancionado por la autoridad estatal de protección de datos de Letonia. Se indica en la conclusión que los hechos por los que es sancionado el afectado, pueden constituir un tratamiento de datos personales con fines exclusivamente periodísticos, en el sentido de dicha disposición, siempre que se deduzca de dicho vídeo que las citadas grabación y publicación tienen como única finalidad la divulgación al público de información, opiniones o ideas, cuestión que debía haber sido objeto de comprobación.

Las Sentencias de 24 de septiembre de 2019, (asunto C-136/17 y C-507/17) referidas ambas a la supresión por parte del buscador Google sobre determinados resultados de búsqueda.

Interesa destacar entre la jurisprudencia europea la **Sentencia de 29 de julio de 2019 (asunto C-40/17)**. Analiza la posición jurídica del responsable de una página de un perfil en una red social y la propia de la red social en cuestión.

En concreto se tiene en cuenta la recogida de datos a través del botón "me gusta" del que dispone la red social en relación con las publicaciones y comentarios de los usuarios y el uso del mismo en la página web de un tercero.

Se desprende que cuando un usuario accede y consulta la página web del tercero, ya sea este miembro o no de dicha red social, y sin necesidad de interactuar con botón "me gusta" que esta tiene insertado derivado de la existencia de un perfil en la red social, se transmiten a estos datos de carácter personal, como por ejemplo la dirección IP del usuario y la identificación de su explorador de internet. Estas circunstancias convierten al titular de la página web en responsable de dicho tratamiento, junto con la entidad responsable de la red social en cuestión.

El titular de la página web actuará como responsable del tratamiento consistente en la recogida y transmisión de los datos a la red social, y esta última en otras fases del tratamiento como el almacenamiento y posterior uso que se haga. De todo ello se deduce que al titular de la página web le es de aplicación la normativa de protección de datos y las obligaciones que de ella se derivan.

La sentencia reviste gran interés por lo habitual de este tipo de tratamientos y por el análisis que realiza respecto de las relaciones entre dos responsables de un mismo tratamiento en diferentes fases del mismo.

3.2 El Comité Europeo de Protección de Datos

El Comité Europeo de Protección de Datos (CEPD), nacido con la aplicación efectiva del Reglamento General de Protección de Datos (RGPD), ha avanzado en el proceso de consolidación de su nueva condición de organismo de la Unión Europea.

El año 2019 ha supuesto un incremento en la actividad del CEPD, tanto en las reuniones plenarias, que han pasado a tener carácter mensual, como en los distintos subgrupos de expertos. Los recursos asignados al Comité, tanto materiales como de personal, han aumentado de forma sostenida. Esto ha permitido afrontar el aumento de la actividad asociada al nuevo estatus del máximo organismo de coordinación de las autoridades nacionales de protección de datos.

El Comité Europeo de Protección de Datos ha sido plenamente consciente de la necesidad de hacer frente al aumento de sus funciones, que han pasado de las de tipo consultivo o de guía, recogidas en el artículo 70 del RGPD, a incluir todas las relacionadas con asegurar la coherencia en la actuación de las autoridades de supervisión.

El Comité se manifiesta a través de recomendaciones, directrices o buenas prácticas, así como de dictámenes. Las directrices tienen un carácter más general, de interpretación de cuestiones controvertidas de la legislación sobre protección de datos de la Unión. Se elaboran por los subgrupos de expertos en un trabajo intenso de colaboración durante un periodo de tiempo prolongado, seguido de una consulta pública antes de su aprobación definitiva por el Plenario del CEPD. Los temas sujetos a dictamen del Comité están especificados en el art. 64 del RGPD y se elaboran y aprueban por el Plenario en un máximo de 14 semanas.

El RGPD prevé también la adopción de decisiones vinculantes que el Comité adopta para resolver conflictos entre autoridades de supervisión. Hasta la fecha no ha habido ocasión de hacer uso de este instrumento.

Durante el año 2019 el CEPD aprobó los siguientes documentos:

Directrices 2019:

- Sobre el tratamiento de datos personales en relación con el artículo 6.1.b RGPD en el contexto de la prestación de servicios online a los interesados.
- Sobre códigos de conducta y organismos de supervisión.
- Sobre el ámbito territorial del RGPD.
- Sobre tratamientos de datos a través de dispositivos de video.
- Sobre protección de datos desde el diseño y por defecto.

Dictámenes 2019:

- Dictamen conjunto del CEPD y el SEPD sobre los tratamientos de los datos de pacientes y el rol de la Comisión Europea dentro de la infraestructura de Servicios digitales eHealth.
- Dictámenes sobre listas nacionales de tratamientos que requieren EIPD y tratamientos que no.
- Dictamen sobre la relación entre la Directiva ePrivacy y el RGPD.
- Dictamen sobre la relación entre el Reglamento de Ensayos Clínicos y el RGPD.
- Dictamen sobre el Acuerdo Administrativo para la transferencia de datos personales entre las Autoridades de Supervisión Financiera del EEE y Autoridades de Supervisión Financiera de fuera del EEE.
- Dictámenes sobre requisitos de acreditación de órganos de control de códigos de conducta.
- Dictamen sobre cláusulas contractuales tipo remitidas por la Autoridad Danesa.
- Dictamen sobre la competencia de una autoridad supervisora en caso de cambio de circunstancias relacionadas con el establecimiento principal o único.
- Dictámenes sobre las autorizaciones de BCR (Normas Corporativas Vinculantes) previstas por varias autoridades nacionales.

Varios de estos documentos tienen una especial relevancia por motivos diversos.

Es el caso de las Directrices sobre el tratamiento de datos personales en relación con el artículo 6.1.b RGPD (tratamiento necesario para la ejecución de un contrato) en el contexto de la prestación de servicios online a los interesados.

El documento concluye que los responsables podrán basarse en el artículo 6.1.b cuando establezcan tanto que el tratamiento se desarrolla en el contexto de un contrato válido con el interesado como que el tratamiento es necesario para que ese contrato en particular pueda ejecutarse. La mera referencia a un tratamiento de datos en el marco de un contrato no sirve para que ese tratamiento pueda llevarse a cabo sobre la base del art. 6.1.b. El responsable debe estar en condiciones de establecer que el tratamiento es objetivamente necesario para el desarrollo de ese contrato.

Las directrices también analizan la posible aplicación de esta base jurídica a una serie de situaciones características de los servicios on-line, como son justificar determinados tratamientos de datos en finalidades como “mejora de los servicios, “prevención del fraude”, oferta de publicidad basada en el comportamiento de los usuarios, o personalización de contenidos. El Comité concluye que en todos estos casos la base jurídica relacionada con la ejecución de un contrato no resulta adecuada, sin perjuicio de que puedan identificarse otra que permita esos tratamientos.

El RGPD establece los códigos de conducta como una nueva opción a disposición de las organizaciones que, de una manera proactiva, deseen demostrar su alineamiento con las previsiones del Reglamento. Estos instrumentos

especifican la forma de aplicar el RGPD en un sector determinado. Incluyen siempre un organismo de supervisión, que debe estar acreditado, con capacidad de vigilar la buena aplicación de este y tomar medidas correctivas en caso de incumplimiento.

Las Directrices aprobadas por el CEPD incluyen unos criterios de admisibilidad de los códigos, los criterios para su aprobación y el procedimiento que debe seguirse para su aprobación, a nivel nacional y europeo. También incluyen los requisitos generales de acreditación de los organismos de supervisión de dichos códigos. Varias autoridades, entre las que se incluye la AEPD, han presentado sus requisitos de acreditación a la consideración del CEPD, que los ha aprobado mediante los correspondientes Dictámenes.

Después de un periodo de consulta pública, el Comité aprobó las Directrices sobre el ámbito territorial del RGPD. Las Directrices sostienen que la aplicación territorial del RGPD que se deriva de su artículo 3.2 corresponde a los tratamientos que estén relacionados con la oferta de bienes y servicios a personas en la Unión o con el seguimiento de su actividad, y no a todo el responsable o encargado que desarrolla esos tratamientos.

En el mismo sentido, las Directrices aclaran que el RGPD se aplicará a encargados no establecidos en la Unión en aplicación del artículo 3.2 solo cuando el responsable que los contrata esté también establecido fuera de la Unión. Si tiene establecimientos en la Unión, la aplicación del RGPD se produce de manera indirecta a través de los contratos de encargo y de los instrumentos de transferencias internacionales.

Finalmente, el documento manifiesta que, en opinión del Comité, los representantes de responsables y encargados no pueden ser objeto de la aplicación directa de sanciones económicas, dado que el Comité entiende que el RGPD no ofrece base suficiente para hacer esta interpretación, por mucho que su Considerando 80 sí que se refiera a esa posibilidad. Sin embargo, el Comité sí admite que las multas puedan dirigirse a los representantes y no excluye la posibilidad, prevista en la legislación española, de que los representantes tengan que responder indirectamente de los incumplimientos de los responsables o encargados a los que representan.

El uso de dispositivos de captación de imágenes y su tratamiento posterior ha tenido un impacto considerable en la vida de los ciudadanos. Estas tecnologías pueden limitar las posibilidades de permanecer anónimo, incluso entre multitudes. Las implicaciones en protección de datos son masivas.

Las Directrices sobre tratamientos de datos a través de dispositivos de vídeo exploran el uso de estos dispositivos respecto a los datos personales y delimitan las excepciones derivadas de la Directiva UE 2016/680, de tratamientos con fines policiales y los tratamientos domésticos. Analizan los tratamientos amparados en el interés legítimo, el interés público y el consentimiento. También dedican una sección a la comunicación de imágenes a terceras partes y el tratamiento de datos de categoría especial, el ejercicio de derechos por parte de los ciudadanos y proponen ejemplos de carteles anunciadores para dar cumplimiento a la obligación de transparencia e información.

Las Directrices sobre protección de datos desde el diseño y por defecto se centran en la implementación por parte de los responsables de la protección de datos desde el diseño y por defecto basada en la obligación directa del Artículo 25 del Reglamento. Aunque la obligación recae en los responsables, también analiza la actuación de otros actores, como los encargados del tratamiento y los proveedores de tecnología para crear productos y servicios que cumplan con el RGPD en nombre de los responsables.

El núcleo de las Directrices se focaliza en garantizar que la protección de datos esté integrada por diseño y por defecto en los tratamientos de una manera efectiva, mediante la implantación de medidas y salvaguardas apropiadas para implementar los principios de protección de datos y los derechos y libertades de los afectados.

El primer dictamen conjunto del CEPD y el Supervisor Europeo de Protección de Datos al amparo del nuevo Reglamento UE 2018/1725,

se centró en los tratamientos de los datos de los pacientes y el rol de la Comisión Europea dentro de la Infraestructura de Servicios Digitales eHealth. En el dictamen se evalúa el papel de la Comisión en el tratamiento de los datos personales de los pacientes. También se establecen las obligaciones específicas de la Comisión como encargado de tratamiento, de conformidad con el Reglamento 2018/1725. El dictamen conjunto contiene una solicitud para que la Comisión incluya todas sus funciones como encargado en el proyecto decisión de ejecución.

La importancia de esta opinión va más allá del hecho concreto que la motiva, ya que integra un posicionamiento del Comité que puede ser extensivo a una gran variedad de situaciones en que actúan plataformas de características similares a las que presenta la plataforma desarrollada por la Comisión.

Las listas de tratamientos que requieren de la realización de una Evaluación de Impacto en la Protección de Datos (EIPD) tienen como objetivo proporcionar a los ciudadanos y las empresas de la Unión Europea unas directrices claras sobre los tratamientos que las autoridades consideran que son susceptibles de comportar un alto riesgo para los derechos y libertades de las personas físicas.

El CEPD ha continuado con su tarea de evaluación y aprobación de las mencionadas listas elaboradas por las autoridades nacionales, incluida la AEPD, al amparo del 35.4 del RGPD. Este año, como novedad, se han aprobado las listas de los tratamientos que no requieren EIPD. La elaboración de estas listas no es obligatoria para las autoridades nacionales, pero algunas, entre ellas la AEPD, las han presentado para su aprobación por el CEPD, que ha emitido dictamen favorable en todos los casos.

La Directiva ePrivacy[2] regula los tratamientos de datos personales en el marco de las comunicaciones electrónicas. Se encuentra en proceso de modificación, aunque las negociaciones entre los colegisladores europeos se han estancado. Esta norma es previa al RGPD y crea dificultades en la actividad de las Autoridades en los casos en los que Directiva y Reglamento deben aplicarse, pues algunas Autoridades, especialmente las nórdicas, no disponen de competencias en este ámbito.

El Dictamen sobre la relación entre la Directiva ePrivacy y el RGPD establece que cuando el tratamiento de datos activa la aplicación simultánea del RGPD y de la Directiva, las autoridades de protección de datos son competentes para supervisar los tratamientos de datos solo si la ley nacional les confiere esa competencia, y esa supervisión debe producirse de acuerdo con los poderes de supervisión y con las consecuencias que establezca la ley nacional de trasposición de la Directiva ePrivacy

En octubre de 2018 la Comisión Europea solicitó la opinión del CEPD sobre un Documento de Preguntas y Respuestas relativas al Reglamento de Ensayos Clínicos. El subgrupo de Cumplimiento Normativo, coordinado por la AEPD, junto con el de Disposiciones Clave, elaboraron un dictamen centrado en los puntos más conflictivos, como el uso del consentimiento como base jurídica para el tratamiento de datos en ensayos clínicos, así como los efectos de su retirada.

También se tuvo en cuenta el uso secundario de los datos fuera del protocolo del ensayo para otros propósitos científicos.

Es de destacar que el dictamen, como hace la Comisión en sus Preguntas y Respuestas, distingue claramente entre el consentimiento que se presta para participar en el ensayo clínico del que se puede prestar para el tratamiento de los datos personales, concluyendo que este segundo es una base jurídica posible pero que debe manejarse con gran cuidado. Y ello por dos motivos. El primero, que en el contexto de los ensayos clínicos pueden ser frecuentes situaciones en que el consentimiento no podría considerarse libre, como serían razones económicas que hagan del ensayo clínico la única vía para que un paciente

[2] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

acceda a un determinado medicamento, la dependencia emocional o material del paciente con el médico que va a ocuparse del ensayo, o la percepción que pueda tener el paciente de que participar en el ensayo puede ser la única vía para recuperar su salud. Por otro lado, el consentimiento debe poder ser retirado en cualquier momento, lo que llevaría aparejada la necesidad de suprimir los datos ya obtenidos o de poderlos utilizar para el análisis final del ensayo.

Por ello se sugieren las bases jurídicas del interés público, siempre que el ensayo clínico se desarrolle en unas circunstancias que de acuerdo con las normativas nacionales establezcan la existencia de ese interés público, o un interés legítimo prevalente en otros casos.

El Dictamen sobre el Acuerdo Administrativo para la transferencia de datos personales entre las Autoridades de Supervisión Financiera del EEE y Autoridades de Supervisión Financiera de fuera del EEE es el primero de este tipo que adopta el Comité. Tuvo su origen en los contactos mantenidos por la organización internacional de reguladores de los mercados financieros (IOSCO) y el extinto Grupo de Trabajo del artículo 29 con vistas a adaptar al RGPD el marco empleado por IOSCO para ofrecer garantías en las transferencias internacionales de datos que se producen entre sus miembros en el ejercicio de sus funciones de supervisión.

Debe señalarse que la intervención del Comité se ha limitado, formalmente, a emitir un dictamen sobre el acuerdo en virtud del artículo 64.1 del Reglamento, pero el acuerdo fue promovido y, en última instancia redactado y presentado por las entidades afectadas. El RGPD prevé que las transferencias internacionales a países que no ofrezcan nivel adecuado de protección podrán realizarse, entre otros supuestos, cuando se proporcionen garantías suficientes en acuerdos administrativos que habrán de ser autorizados por las autoridades de protección de datos, previo dictamen del CEPD.

En este caso concreto, los supervisores financieros presentaron el acuerdo al Comité, que dictaminó favorablemente sobre el mismo. A partir de este dictamen favorable, las distintas autoridades de la Unión han ido emitiendo sus propias autorizaciones, aunque ya sin necesidad de remitir estas al Comité para un nuevo procedimiento.

El artículo 28 del RGPD recoge que una Autoridad de Control podrá adoptar cláusulas contractuales tipo que rija los contratos entre responsable y encargado y entre encargado y subencargado. Las autoridades que quieran adoptar unas cláusulas contractuales tipo deben presentarlas al Comité para garantizar la coherencia en la aplicación del RGPD en toda la Unión.

La autoridad danesa presentó las primeras cláusulas contractuales tipo que se han sometido al Comité. Estas cláusulas, que fueron objeto de un dictamen favorable, aunque con algunas salvedades que fueron corregidas por la autoridad danesa, están orientadas a facilitar los contratos de encargo de tratamiento de datos personales entre pequeñas y medianas empresas. La intención es que sirvan como modelo para incluir en los contratos y al desarrollar las disposiciones del artículo 28 del RGPD ayuden a su cumplimiento.

La Unión Europea está reforzando sus normas sobre ciberseguridad para hacer frente a la creciente amenaza que plantean los ataques cibernéticos y aprovechar las oportunidades que presenta la nueva era digital. El 9 de abril de 2019, el Consejo adoptó el denominado Reglamento sobre la Ciberseguridad, que introduce:

- Un sistema de esquemas de certificación a escala de la UE.
- Una Agencia de la UE para la Ciberseguridad a fin de mejorar y sustituir a la actual Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA).

El propio Reglamento de ciberseguridad reconoce al CEPD su importancia en el esquema de certificación de ciberseguridad y establece que un representante participe en el Grupo de Actores Clave para la Certificación de Ciberseguridad (SCCG por sus siglas en inglés). El CEPD ha nombrado a su representante en dicho grupo a propuesta del subgrupo de expertos en Cumplimiento Normativo.

En 2019, el Comité ha emitido los primeros dictámenes sobre las decisiones de autorización de Normas Corporativas Vinculantes (BCR, por sus siglas en inglés) presentadas por diversas autoridades de supervisión. Concretamente, se adoptó dictamen favorable a las BCR de ExxonMobil, a propuesta de la autoridad belga, y de Equinix Inc., a propuesta de la autoridad del Reino Unido.

3.3 Tecnológicos

La Unidad de Evaluación y estudios Tecnológicos (UEET) se crea a finales de 2015, formando parte de la Unidad de Apoyo de la Dirección con el objeto de tener una unidad que haga frente a los nuevos retos que planteaba el nuevo enfoque hacia la Responsabilidad Proactiva del Reglamento General de Protección de Datos (RGPD) y el estado del arte de los nuevos tratamientos de datos que involucran el uso de tecnologías disruptivas.

De esta forma, la AEPD seguía el ejemplo de otras autoridades como la CNIL francesa, que dispone de una Dirección de Tecnologías e Innovación, o el ICO británico, que dispone de una Dirección Ejecutiva de Innovación y Política Tecnológica, entre otros. Desde esta Unidad se han desarrollado actividades de cooperación con asociaciones y universidades con el objetivo de promover el modelo de cumplimiento que plantea el RGPD.

Entre las actividades de la UEET durante el año 2019 cabe destacar las siguientes:

- Impulsar las medidas que garanticen la compatibilidad del desarrollo tecnológico con la privacidad asegurando los derechos de los ciudadanos según lo previsto en el artículo 57.1.i) del Reglamento (UE) 2016/679; en particular: el asesoramiento a emprendedores y desarrolladores tecnológicos, la realización de estudios de prospección tecnológica, informar y asesorar a los proyectos tecnológicos con implicaciones en el derecho a la protección de datos de las personas, participar en proyectos tecnológicos de ámbito internacional de interés público sobre la base del derecho de la Unión Europea o de los Estados Miembros y promover la colaboración con las Universidades con el fin de impulsar la protección de datos en proyectos y contenidos curriculares jurídicos y técnicos.
- Emitir informes, recomendaciones y dictámenes sobre las consultas previas relativas a la Evaluación de Impacto para Protección de Datos realizadas por los responsables conforme al artículo 36 del Reglamento (UE) 2016/679, en virtud de lo previsto en su artículo 57.1.l).
- La elaboración de una lista positiva y otra negativa de tratamientos que requieren la realización de evaluaciones de impacto según lo previsto en el artículo 57.1.k del Reglamento (UE) 2016/679.

3.3.1 Elaboración de guías y modelos

Con relación a las tareas de realización de la realización de estudios de prospección tecnológica y el impulso de medidas que garanticen la compatibilidad del desarrollo tecnológico, la UEET ha desarrollado las siguientes guías y notas técnicas durante 2019:

- Guía de Privacidad desde el Diseño
- Guía de Drones y Protección de Datos
- Modelo para realizar una Evaluación de Impacto de la Protección de Datos en AAPP

3.3.2 Elaboración de estudios y notas técnicas

- Estudio del Hash como técnica de pseudonimización, en colaboración con el Supervisor Europeo de Protección de Datos (EDPS)
- Estudio Fingerprinting o Huella digital del dispositivo
- La K-anonimidad como medida de privacidad [jun 2019]
- Nota técnica sobre Privacidad en DNS
- Nota técnica: El deber de informar y otras medidas de responsabilidad proactiva en apps para dispositivos móviles
- Nota técnica: Avance del estudio de IMDEA NETWORKS y UC3M: "Análisis del Software Pre-instalado en Dispositivos Android y sus Riesgos para la Privacidad de los Usuarios"
- Nota técnica: Acceso de aplicaciones a la pantalla en dispositivos Android
- Nota técnica: Control del usuario en la personalización de anuncios en Android
- Análisis de los flujos de información en Android. Herramientas para el cumplimiento de la responsabilidad proactiva
- Lista de tratamientos obligados a realizar una Evaluación de Impacto de la Privacidad (EIPD) de acuerdo con el artículo 35.4 del RGPD
- Lista de tratamientos exentos a realizar una Evaluación de Impacto de la Privacidad (EIPD) de acuerdo con el artículo 35.5 del RGPD
- Orientación para la aplicación provisional de la disposición adicional séptima de la LOPDGDD

Se está elaborando una Guía de Administración Digital en colaboración con la Secretaría General de Administración Digital (SGAD), una Guía de Privacidad por Defecto y una Guía sobre Inteligencia Artificial, que finalizarán en 2020.

3.3.3 Notificaciones de violaciones de seguridad (brechas de seguridad)

Con relación a la misión de gestión, análisis y evaluación de las brechas de seguridad, se han realizado las siguientes actividades:

- De las 1.459 notificaciones de brechas de seguridad, un total de 498 incluyen notificaciones a los interesados, con un total de 14 resoluciones de requerimiento de notificación a los interesados emitidas por la AEPD.
- Se ha creado una sección web sobre brechas de seguridad y se ha iniciado la publicación en la página web de la AEPD de los informes mensuales sobre brechas notificadas a la AEPD con un análisis sobre su tipología.
- Se ha establecido con el Consejo de Transparencia de Andalucía un canal para la comunicación de brechas que afecten a las AAPP de la Comunidad de Andalucía, se encuentra ya en marcha la recepción de la notificación inicial a través de la herramienta LUCIA del CCN que está conectada con la instancia de dicha herramienta en la AEPD.
- Se sigue trabajando en la integración más completa con la herramienta Lucia del CCN y con la notificación de brechas de INCIBE con el objetivo de facilitar la creación de un punto único de notificaciones de violaciones de seguridad.
- Se ha propuesto la celebración de especificaciones para el desarrollo de un sistema de gestión de brechas que facilite la comunicación con el responsable y la gestión de las brechas de seguridad.
- Además, se está trabajando en un conjunto de criterios formales para la iniciación de actuaciones de inspección en colaboración con la SGID atendiendo a niveles de riesgo para los derechos y libertades de las personas. En paralelo trabaja con el CEPD con el fin de acordar criterios comunes en la gestión de las violaciones de seguridad entre autoridades de control.

3.3.4 Evaluaciones de impacto y consultas previas

Con relación a las tareas relativas al análisis de las consultas previas relativas a la Evaluación de Impacto para Protección de Datos, las actividades han sido las siguientes:

- En 2019 se han remitido a la AEPD un total de 20 solicitudes de consulta previa de las cuales únicamente una cumplía los requisitos señalados en los artículos 36 y 36 del RGPD. Las diecinueve restantes han sido respondidas desde el Canal Informa.
- Se han realizado las especificaciones de una herramienta de gestión de solicitudes de consultas.

3.3.5 Cooperación con asociaciones y otras entidades

Con el propósito de impulsar la protección de datos como un factor de confianza y garantía de calidad en beneficio del desarrollo económico de la sociedad con el objeto de promover la sensibilización de responsables y ciudadanos, participar en proyectos tecnológicos de ámbito internacional de interés público sobre la base del derecho de la Unión Europea o de los Estados Miembros y promover la colaboración con las Universidades con el fin de impulsar la protección de datos y generar el conocimiento necesario para anticiparse a los cambios de la tecnología, se han establecido las siguientes colaboraciones con:

- Supervisor Europeo de Protección de Datos (EDPS): elaboración y difusión de informes técnicos de protección de datos
- Universidad de las Naciones Unidas: colaboración sobre blockchain en las AAPP
- Universidad Carlos III-IMDEA Networks: colaboración en la difusión de sus estudios sobre el sistema de permisos en Android, que ha resultado en la publicación de Nota técnica sobre la Gestión de Permisos en Android y la presentación del trabajo en el Subgrupo de Tecnología del Comité Europeo de Protección de Datos y se está definiendo un nuevo proyecto para ayudar a emprendedores en el ámbito de las apps.
- Universidad de Alcalá de Henares: colaboración para estudiar técnicas de gobernanza en blockchain.
- Universidad Politécnica de Madrid – Fundetel: se ha concluido el trabajo contratado, cuyo resultado ha sido la publicación dos notas técnicas.
- Universidad Nebrija: convenio con la Universidad para la realización de prácticas por parte de los alumnos de títulos propios de máster y máster oficiales.
- Fundación Éticas: contratación para el desarrollo de guías de auditorías de aplicaciones de Inteligencia Artificial
- Autoridades Autonómicas de Protección de Datos: publicación consensuada de la Orientación para la aplicación provisional de la disposición adicional séptima de la LOPDGDD, la publicación conjunta de la lista de tratamientos obligados a realizar EIPD de acuerdo al artículo 35.4 y el consenso sobre la lista de tratamientos no obligados a EIPD conforme al artículo 35.5.
- CDTI: comisión del seguimiento del Convenio de Colaboración con el CDTI.
- SGAD, Ministerio de Trabajo y Gerencia de la Seguridad Social: desarrollo de herramientas y guías para la adecuación de las AAPP al RGPD.
- Otros: Comité Técnico de Innovación Financiera, Potluckforum, Fundación Profuturo, Fundación Koplowitz, grupo de normalización CTN71, etc.

3.3.6 Desarrollo de herramientas

En el marco, también, del impulso a la protección de datos y, en particular, en el aspecto del desarrollo y mantenimiento de herramientas de ayuda para el cumplimiento por parte de los mismos, las acciones realizadas han sido:

- Publicación en una nueva versión de la herramienta para pymes, **Facilita 2.0**, adaptada a la LOPDGDD y con otras mejoras.

  Publicación de la herramienta **GESTIONA-RGPD** para el análisis de riesgos y la evaluación de impacto para pymes.

- Está en progreso una versión de Facilita Emprende, orientada a emprendedores y startups.

- En el marco de la colaboración con el Ministerio de Trabajo y con la Gerencia de Informática de la Seguridad Social para la adaptación de las herramientas ASSI y SIOM a los requisitos de del RGPD, se está trabajando para la puesta a disposición de las AAPP de herramientas de gestión RGPD.

3.3.7 Acciones de impulso a la responsabilidad proactiva

Otras acciones que impulsan el cumplimiento del principio de responsabilidad activa del RGPD, asesoran a emprendedores y desarrolladores tecnológicos e informan y asesorar a los proyectos tecnológicos con implicaciones en el derecho a la protección de datos de las personas han sido las siguientes:

- Se ha creado un espacio web en la página web de la AEPD dedicado a Innovación y Tecnología, que incluye entre otros, un apartado de herramientas para las pymes, emprendedores y desarrolladores, guías técnicas y compilación de las entradas de blog de la AEPD con carácter técnico.

- Se ha creado un espacio web para la Lucha Contra la Violencia de Género y la Violencia Digital.

- La UEET colabora con las Administraciones Autonómicas que lo solicitan con el objetivo de proporcionar formación en el contexto del análisis de riesgos, evaluaciones de impacto y consultas previas del RGPD, en este sentido, se ha participado en la formación y divulgación de dichos contenidos con la Comunidad de Madrid a la vez que se está valorando la colaboración con otras administraciones autonómicas.

- Se ha participado en la propuesta del proyecto APPRENTICE para la formación de excelencia de expertos en protección de datos dentro del campo de la ingeniería en el conjunto de acciones Marie Sklodowska Curie – H2020.

- Se han firmado cartas de colaboración con entidades para el acceso a proyectos europeas, como con IMDEA-Networks y con la Fundación Éticas.

- Se ha participado en las jornadas formativas para startups de la incubadora Lanzadera y SouthSummit.

- Se creó en la convocatoria de premios de la AEPD 2019 el nuevo Premio de emprendimiento en protección de datos personales Ángela Ruiz Robles.

De forma general, la UEET asiste a diversos grupos de trabajo con relación a proyectos e iniciativas técnicas y sobre tecnologías disruptivas que tienen impacto en protección de datos sobre temas de Big Data, Blockchain, Inteligencia Artificial, etc.

3.3.8 Acciones internacionales

En relación con la participación en iniciativas internacionales de carácter tecnológico en protección de se han realizado las siguientes actividades:

- Participación en el Subgrupo de Tecnología del Comité Europeo de Protección de Datos participando como co-revisores en las guías sobre notificación de brechas de seguridad, blockchain y privacidad por defecto y desde el diseño, y videovigilancia, así como presentación en el mismo de las acciones realizadas a nivel nacional.
- Como se ha señalado anteriormente, se ha iniciado una acción de colaboración con la Universidad de las Naciones Unidas en el campo de blockchain y con el Supervisor Europeo de Protección de Datos en temas tecnológicos.
- El espacio web de Innovación y Tecnología ha incorporado su documentación en inglés y ha creado una página completamente en inglés.

4. Al servicio de los ciudadanos

4.1 Atención al ciudadano

El área de Atención al Ciudadano de la Agencia ofrece diferentes canales de contacto a través de los cuales la ciudadanía tiene la posibilidad de plantear dudas y cuestiones relativas a la normativa en materia de protección de datos. Durante el año 2019 la actividad de los diferentes canales fue la siguiente:

- **Atención presencial.** Se atendió presencialmente a 2.443 personas, confirmándose la tendencia a la baja en el número de consultas presenciales, que se ha ido reduciendo en los últimos años (en 2016 se atendieron a 4.183 personas, 3.699 en 2017 y 3.455 en 2018).

- **Atención telefónica.** La atención telefónica se presta a través de los números de teléfono 91 266 35 17 y 901 100 099. Se atendieron 60.288 consultas telefónicas, cifra sensiblemente inferior a la del año 2018, en el que se registraron 88.302, y que se debieron en gran parte a la aplicación a partir del 25 de mayo de dicho año del RGPD, lo que dio lugar a un gran número de llamadas al servicio durante las fechas inmediatamente anteriores y posteriores.

- **Catálogo de preguntas frecuentes (FAQs).** Publicado en la Sede electrónica de la AEPD, permite la consulta de más de 200 preguntas-respuestas. Para facilitar su lectura se encuentran agrupadas en 16 áreas temáticas, como Videovigilancia, Solvencia patrimonial (Ficheros de morosos), Transparencia y protección de datos, o Tratamiento de datos en el ámbito laboral, además de una primera denominada En qué te podemos ayudar y en qué no, con la finalidad de informar a las personas sobre el ámbito de actuación de la AEPD.

  Se han registrado 562.457 accesos a las FAQs, cifra inferior a la del año anterior (651.650), cuando se experimentó un incremento exponencial de dichos accesos, debido, al igual que en la atención telefónica, al interés que suscitó la aplicación del RGPD. No obstante, el número de accesos sigue siendo muy superior al de años anteriores (147.297 en 2016 y 170.754 en 2017), confirmándose que este canal es el principal a través de la cual los ciudadanos consultan a la AEPD.

  El catálogo se actualiza permanentemente con la finalidad de dar respuesta y hacer más accesible la información que demandan los ciudadanos.

- **Consultas escritas.** Se da respuesta por escrito a las consultas recibidas a través de la Sede electrónica de la AEPD, donde se ha habilitado un trámite específico para enviar una consulta al acceder a alguna de las FAQs disponibles. A diferencia del Canal Informa_RGPD, al que se hace referencia más adelante, este canal responde a las consultas de la personas en tanto que titulares de datos personales que son objeto de tratamiento por responsables y encargados. Se ha dado respuesta a 10.872 consultas, lo que supone un incremento notable del uso de este canal con respecto a las cifras de años anteriores.

4.2 Protección de los menores

La LOPDGDD, en su artículo 83, incluyó el derecho a la educación digital para garantizar la plena inserción de los alumnos en la sociedad digital y el aprendizaje de un uso de los medios digitales que sea seguro y respetuoso, entre otros ámbitos, con la intimidad personal y familiar y la protección de datos personales. Competencia digital que las Administraciones educativas han de desarrollar en el bloque de asignaturas de libre configuración con la inclusión de los elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, en especial de las situaciones de violencia en la red.

Con el fin de fomentar y apoyar el desarrollo de la educación digital y reforzar la protección de los menores, el 17 de diciembre, el Ministerio de Educación y Formación Profesional y la AEPD

presentaron la web ASEGURATIC, desarrollada por el Instituto de Nacional de Tecnologías Educativas y Formación del Profesorado (INTEF).

La web, producto del Grupo de Trabajo creado a iniciativa de la AEPD para la aplicación efectiva de lo dispuesto en el artículo 83 de la LOPDGDD, y promovido por el Ministerio de Educación y Formación Profesional, el INCIBE, el Ministerio del Interior y la Delegación del Gobierno para la Violencia de Género, cuenta con la participación de entidades privadas (Facebook, Google, Orange, Twitter, Pantallas Amigas, Fundación ANAR, Fundación Telefónica, Fundación Cibervoluntarios, Qustodio), y tiene como objetivo contribuir a la protección de los menores en su interacción con Internet a través de más de 300 recursos aportados por las distintas entidades participantes, principalmente bajo licencias Creative Commons que facilitan su uso, adaptación y distribución de forma gratuita. Sus destinatarios principales son los miembros de la comunidad educativa: educadores, familias, alumnos, centros educativos y administraciones.

Constituye la mayor base de documentación, materiales, recursos, herramientas sobre educación digital en formato digital que existe: contenidos didácticos, guías, unidades didácticas, presentaciones, webs, tareas, juegos, cursos de formación, catalogados, organizados y fácilmente accesibles a través de un buscador que permite filtrarlos por:

- Temática (privacidad, seguridad, identidad digital, redes sociales, uso de internet, acoso en internet…)
- Público al que va dirigido (educadores, familias, menores, administración educativa)
- Etapa educativa (Primaria, Secundaria, Bachillerato, FP)
- Tipo de recurso (web, audiovisual, guía, contenido interactivo, unidad didáctica, tarea, juego, presentación, curso de formación)
- Fuente (entidad creadora)
- Licencia de uso

Así mismo, se han mantenido reuniones con la CRUE (Confederación de Rectores de las Universidades Españolas) para incidir en la necesidad de establecer en los contenidos de los currículos de los distintos grados y postgrados, preferentemente del ámbito de la educación, las competencias digitales que permitan a los futuros profesionales contar con las habilidades necesarias para ejercer su actividad profesional, en especial los docentes.

4.2.1 Canal Joven

La protección de los menores es una constante de la Agencia, recogida en su Plan Estratégico como uno de los ámbitos prioritarios de actuación, lo que ha dado lugar a iniciativas y al desarrollo de medidas, actuaciones y acciones que se han venido plasmando en las memorias de los años anteriores.

El enfoque de la actuación de la AEPD es el preventivo, mediante acciones y recursos dedicados principalmente a sensibilizar a los menores de la utilización responsable y segura de sus datos personales en internet y en particular en las redes sociales, así como a la concienciación tanto de las familias como de los profesionales de la educación sobre esta problemática ya que son los actores principales para conseguir trasladar a los menores el uso responsable de sus datos personales.

Los materiales, recursos y herramientas elaborados y recopilados por la AEPD a estos efectos están disponibles en el área dedicada a "Educación y menores" de la web de la AEPD, a los que se accede también a través del portal **Tú decides en internet**.

El Canal Joven, cuya finalidad es atender y dar respuesta a las cuestiones y dudas que se planteen a la AEPD en este ámbito, integra la dirección de correo electrónico **canaljoven@aepd.es**, un teléfono específico también para consultas sobre temas de menores (901 233 144) y una línea de WhatsApp (616 172 204). Además, el Canal Joven responde las consultas que sobre esta área se reciben a través de la Sede Electrónica de la Agencia.

Durante el año 2019 se ha dado respuesta a 1.502 consultas. 535 se plantearon por vía telefónica, lo que supone casi un 36% del total. A través de la línea de WhatsApp se registraron 421 consultas, un 28% sobre el total de las recibidas. En la dirección de correo electrónico de Canal Joven se recibieron 380, el 25%, y a través de la Sede Electrónica de la Agencia 166, el restante 11% del total de consultas recibidas.

El análisis de las consultas efectuadas por teléfono, que suponen más de un tercio del total de consultas recibidas en el Servicio de Menores, muestra que, de las 535 llamadas recibidas, 277 (52%) las han efectuado los padres preocupados por la privacidad de sus hijos.

En el ámbito educativo, los centros de educación infantil y primaria han efectuado 49 consultas, el 9%, y los centros de educación secundaria con 23 llamadas, el 4% del total.

De empresas privadas, planteando dudas sobre la protección de datos de los menores, se han recibido 70 llamadas, lo que equivale al 13% del total, y de personal destinado en Organismos Públicos se han contestado 27, el 5% del total.

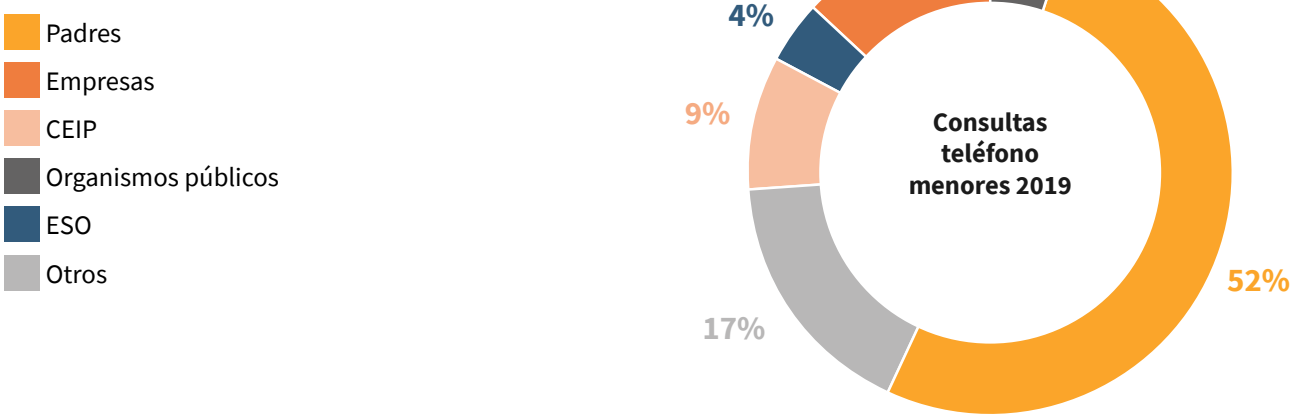
El resto, 89 consultas, el 17 % del total de las recibidas por teléfono, se han efectuado por diferentes entidades, tanto públicas como privadas, que aparecen como "otros", en el siguiente gráfico.

De las consultas más comunes que se han planteado telefónicamente en este año 2019 caben destacar las que se refieren a:

- Padres separados que no tienen un acuerdo establecido entre las partes sobre la publicación de imágenes de sus hijos menores en RRSS
- Consentimiento de los padres para la publicación de imágenes en webs, páginas de los colegios o RRSS de los centros escolares
- Videovigilancia en los colegios
- Certificados de empadronamiento solicitados por padres separados
- Grabación de imágenes en los eventos escolares por los propios centros educativos o por los padres de los alumnos
- Publicación de datos personales por profesores que mantienen blogs particulares

Premio ENISE

La AEPD ha participado, como jurado, en la tercera edición del concurso 'Mejor iniciativa escolar en materia de Ciberseguridad' en el marco de 13ENISE organizado por la S.M.E. Instituto Nacional de Ciberseguridad de España S.A., M.P., (INCIBE), dirigido a centros educativos que hayan implementado iniciativas de ciberseguridad durante el curso académico 2018 – 2019.



4.3 Comunicación

La Agencia ha desplegado a lo largo de 2019 múltiples acciones para dar visibilidad a las iniciativas realizadas. A continuación, se detallan las relacionadas con el departamento de prensa y comunicación, así como las acciones de divulgación publicadas en la página web de la Agencia y su agenda institucional.

4.3.1 Redes sociales

El 28 de enero de 2018, coincidiendo con el Día Europeo de Protección de Datos, la AEPD lanzó su cuenta oficial en Twitter, cumpliendo así con su objetivo de estar presente en el entorno de las redes sociales, una de las medidas contempladas en el Plan Estratégico de la Agencia. Al finalizar 2019, la cuenta de la AEPD contaba con más de 18.000 seguidores, con una media de 122 seguidores nuevos por semana. En este tiempo, se publicaron en el perfil más de 750 tuits, registrando más de 14.000 menciones y 5,7 millones de impresiones.

Con este canal de comunicación, la Agencia persigue varios objetivos: dar a conocer la labor que desempeña la AEPD, promoviendo la sensibilización entre los ciudadanos en relación con la protección de sus datos, y difundir las guías, materiales y herramientas de cumplimiento que la Agencia pone a disposición de los profesionales, las empresas y las administraciones públicas.

Por otra parte, esta cuenta representa un instrumento esencial para conocer cuáles son las inquietudes en esta materia por parte de los diferentes colectivos, tanto de quienes tratan datos como de aquellas personas cuyos datos son objeto de tratamiento. Desde sus inicios, la cuenta de Twitter de la Agencia ha publicado numerosos tuits destinados a fomentar el conocimiento de los derechos y obligaciones del RGPD, tanto a ciudadanos como a organizaciones, mediante la difusión de materiales elaborados por la AEPD, como guías, herramientas para facilitar el cumplimiento, infografías o la retransmisión de eventos en los que participaban representantes de la Agencia.

4.3.2 El blog de la Agencia

El **blog de la Agencia** se ha consolidado como un canal adicional a través del cual la Agencia difunde el derecho fundamental a la protección de datos. El blog de la AEPD ha seguido incrementando el número de accesos hasta superar la cifra de 188.000 en 2019. En cuanto a las publicaciones más populares, '¿Conoces las novedades de la nueva Ley Orgánica de Protección de Datos?', 'Comunidades de propietarios y administradores de fincas ante el RGPD', 'Elaborar el registro de actividades de tratamiento', 'Brechas de seguridad de datos personales: qué son y cómo actuar' y '¿Para qué puede ser útil al ciudadano el registro de Delegados de Protección de Datos? fueron los post más visitados.

4.3.3 Canal de YouTube

Tras el impulso proporcionado en 2018 a su canal de YouTube, con el que se vio incrementado el número de suscriptores hasta situarse cerca de los 1.800, la AEPD cerró 2019 superando los 2.500 suscriptores. En estos 12 meses, los vídeos publicados en el canal de la Agencia tuvieron cerca de 100.000 visualizaciones, lo que representa 4.600 horas de visualización, y fueron compartidos en casi 3.000 ocasiones.

4.3.4 Espacio “Protegemos tu privacidad” de Radio 5

Gracias al acuerdo entre la AEPD y Radio 5 el espacio ‘Protegemos tu privacidad’ ofrece a los ciudadanos recomendaciones semanales para conocer sus derechos y saber cómo ejercerlos, así como consejos para facilitar el cumplimiento de la normativa a las organizaciones. A lo largo de 2019 se han emitido 46 piezas temáticas, en las que un experto de la Agencia ofrece consejos y recomendaciones. Además de la emisión todos los domingos a las 12.05 horas, los programas se encuentran disponibles en la **página web de Radio 5**.

4.3.5 Relaciones con los medios

Los medios de comunicación han seguido jugando un papel de gran importancia en lo que a protección de datos se refiere. Por una parte, favoreciendo la concienciación de los ciudadanos en relación con su derecho a la protección de datos y las novedades que incorpora el RGPD y, por otra, incrementando la sensibilización de los responsables del tratamiento de datos acerca de los mandatos que establece el nuevo contexto normativo europeo.

A lo largo de 2019, la Agencia atendió cerca de 730 consultas de medios de comunicación relacionadas con este derecho fundamental. Pese a que el Reglamento General de Protección de Datos llevaba más de seis meses en aplicación, en 2019 continuaron recibiéndose numerosas consultas relacionadas con distintos aspectos con la nueva norma europea, como el impacto del RGPD en las microempresas y pymes; la incidencia del Reglamento en la actividad de las Administraciones Públicas; el funcionamiento del registro de Delegados de Protección de Datos (DPD); los requisitos para hacer una Evaluación de Impacto en la Protección de Datos Personales (EIPD), o la solicitud de cifras que reflejaran la evolución del primer año de aplicación del Reglamento.

En paralelo, la Agencia registró consultas referidas a notificaciones de brechas de seguridad. Asimismo, tramitó consultas relacionadas con sanciones impuestas por la AEPD en aplicación del Reglamento, difusión de imágenes tomadas por cámaras de videovigilancia o sanciones impuestas en materia de cookies. Por otra parte, la introducción en la disposición final tercera de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) del artículo 58 bis también originó consultas, vinculadas principalmente a la utilización de datos de los ciudadanos recopilados en internet para la realización de propaganda electoral; el recurso del defensor del pueblo al Tribunal Constitucional en relación con este artículo y, posteriormente, la sentencia del alto tribunal que declaró inconstitucional dicho precepto.

Otras consultas atendidas tuvieron relación con el derecho al olvido; la inclusión indebida en ficheros de solvencia; las Listas Robinson; el uso de reconocimiento facial; el fichaje en el ámbito laboral o la denominada protección de datos 'a coste cero'. En el último trimestre se recibieron múltiples consultas relacionadas con la presentación del Canal Prioritario de la AEPD para comunicar la difusión de contenido sensible en internet y solicitar su retirada.

Esta labor de atención a los medios se vio complementada con la difusión de casi 311 notas de prensa, convocatorias y notas de agenda informativa publicadas en la web. En relación con estas últimas, la Agencia publicó en 2019 un total de 236 reuniones o actos públicos en los que participaron diferentes miembros de esta institución, cumpliendo un año más con la actuación prevista en Plan estratégico 2015-2019 de fomentar la publicación de su agenda institucional y ampliar sus contenidos para reforzar la transparencia. Esta actividad se vio complementada con la participación de la Agencia en la redacción de las notas de prensa de las reuniones plenarias que periódicamente celebra el Comité Europeo de Protección de Datos (CEPD).

4.4. Agenda institucional

Para la elaboración de la presente Memoria se ha agrupado de forma sectorial la participación de la Agencia en reuniones institucionales y de trabajo, actos y jornadas. No obstante, la relación completa de la agenda institucional se encuentra disponible en la sección web de la AEPD.

Al igual que en años anteriores, 2019 estuvo caracterizado por la organización y participación en jornadas, encuentros y sesiones informativas, acciones formativas, talleres, actos y presentaciones por parte de la Agencia, orientadas a analizar las implicaciones de la normativa de protección de datos en la actividad de distintos ámbitos, así como facilitar la adecuación del sector público y privado.

Respecto a los eventos relacionados con el sector público, destacan las Jornadas de aplicación de la normativa de protección de datos en las entidades locales en distintas provincias españolas; la Jornada dirigida a los Delegados de Protección de Datos (DPD) de Universidades, organizada juntamente con la Conferencia de Rectores de las Universidades Españolas (CRUE); las Jornadas de formación de Delegados de Protección de Datos de Administración Autonómica y Local en varias provincias; la Jornada sobre Protección de Datos y Administración Local, organizada por el Instituto Nacional de la Administración Pública (INAP); la jornada dirigida a los delegados de protección de datos (DPD) de la Administración General del Estado (AGE) y órganos constitucionales y de relevancia constitucional; la jornada dirigida a los delegados de protección de datos (DPD) de las Comunidades Autónomas, y el Seminario 'A un año de la aplicación del Reglamento General de Protección de Datos' organizado por la Red Iberoamericana de Protección de Datos en colaboración con la Agencia Española de Cooperación Internacional para el Desarrollo (AECID), entre otros.

Por otra parte, la Agencia organizó y celebró encuentros informativos sobre el RGPD dirigidos a sectores específicos, como el de las telecomunicaciones; el gran consumo; el comercio electrónico; la enseñanza, la salud; la energía; los seguros; el sector financiero, las entidades bancarias; las profesiones colegiadas, o los consejos y colegios profesionales.

Asimismo, mantuvo reuniones con diversos departamentos ministeriales, organismos públicos, instituciones, direcciones generales y delegaciones, como el Consejo General de Poder Judicial; la Fiscalía General del Estado; el Instituto Nacional de Estadística, la Dirección General de los Registros y del Notariado, la Dirección General de Gobernanza Pública; la Dirección General del Trabajo Autónomo de la Economía Social y de la Responsabilidad Social de las Empresas; la Dirección General de Igualdad de Trato y Diversidad la Delegación del Gobierno para la Violencia de Género; el Ministerio de Educación y Formación Profesional; el Ministerio de Presidencia, Relaciones con las Cortes e Igualdad; el Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF), el Instituto Nacional de Ciberseguridad (INCIBE); la Oficina de Seguridad de Internauta (OSI); la Comisión Nacional de los Mercados y la Competencia; el Ministerio de Educación y Formación Profesional. También celebró reuniones de trabajo con las autoridades autonómicas de protección de datos, con las que se reúne de forma periódica.

En el ámbito del sector privado, la Agencia Española de Protección de Datos participó en numerosos actos como, entre otros, la Jornada sobre la nueva Ley de Protección de Datos organizada por Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF); el IV Encuentro sobre cumplimiento normativo, organizado por la Asociación de Profesionales de Cumplimiento Normativo (CUMPLEN); el XVI Foro de Seguridad y Protección de Datos de Salud, organizado por la Sociedad Española de Informática de la Salud (SEIS); la Jornada Novedades normativas en el sector sanitario, organizada por la Alianza de la Sanidad Privada Española (ASPE); el IV Encuentro de la DPO Community de ISMS Forum; la Jornada sobre la Ley Orgánica de Protección de Datos y garantía de los derechos digitales, organizada por la Asociación para la Autorregulación de la Comunicación Comercial (AUTOCONTROL); el Foro

de la Privacidad, organizado por el Data Privacy Institute ; la Jornada Retos y oportunidades del futuro del trabajo: Presentación de resultados de Enterprise 2020, organizado por la asociación de empresas y profesionales de la responsabilidad social empresarial y sostenibilidad Forética; el Foro Tecnológico del ICAM Abogacía 4.0; el XIII Congreso de Gestión Sanitaria, dirigido por el Instituto de Fomento Sanitario; la jornada sobre novedades de la normativa de protección de datos organizada por la Confederación Española de Organizaciones Empresariales (CEOE); la jornada 'La igualdad de género, el derecho a la desconexión digital y el registro de jornada, a examen', organizada por la Asociación de Directivos de Relaciones Laborales (ADiReLab); la World Compliance Summit 2019 'Reglamento General de Protección de Datos: Un año de la entrada en vigor', organizada por Audisec con la colaboración de la AEPD y la Universidad Complutense de Madrid; la XXI Jornada Internacional de Seguridad de la Información, organizada por ISMS Forum; el VII Congreso de la Asociación Profesional Española de Privacidad (APEP); la Jornada 'Tras el primer aniversario del RGPD: presente, futuro e impacto internacional', organizada por el Colegio de Abogados de Madrid (ICAM) en colaboración con la Asociación Internacional de Profesionales de Privacidad (IAPP); la Jornada Ciudadanía Conectada 2019 sobre educación y bienestar digital, organizada por Pantallas Amigas; el III Encuentro Justicia y Sociedad, organizado por la Fundación Mutua Madrileña y la Asociación Profesional de la Magistratura; el Día del Compliance Officer, organizada por la Asociación Española de Compliance, y la I Jornada Gestión del Tercer Sector, organizada por la Fundesplai, entre otras.

Igualmente, mantuvo reuniones con representantes de colegios, asociaciones, fundaciones y otros colectivos, como el Colegio de Procuradores de Madrid; la Asociación Española de Compliance (ASCOM); la Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF); la Agencia Española de Medicamentos y Productos Sanitarios; la Asociación de Directivos de Relaciones Laborales (ADiReLab); la Asociación para la Autorregulación de la Comunicación Comercial (AUTOCONTROL), la Asociación Española de la Economía Digital (Adigital); la Asociación Española de Anunciantes (AEA); Asociación Empresarial del Seguro (UNESPA); IAB Spain; la fundación Profuturo; la fundación ANAR; la fundación Alicia Koplowitz; la fundación Orange; la fundación Democracia y Gobierno Local; la fundación Mutua Madrileña, y los promotores de los 17 Códigos Tipo inscritos en el Registro General de Protección de Datos de la Agencia, entre otros.

Durante 2019 la AEPD celebró reuniones con distintos actores en la lucha contra la violencia de género. En este sentido, constituyó un grupo de trabajo contra la violencia en internet, compuesto por representantes de la Vicepresidencia del Gobierno; los Ministerios de Educación y Formación Profesional; Trabajo, Migraciones y Seguridad Social; Interior; Justicia; la Delegación del Gobierno para la Violencia de Género, el INCIBE, así como de las fiscalías de Criminalidad Informática y de Violencia sobre la Mujer; el CGPJ y el Consejo General de la Abogacía, con los que mantuvo una reunión de trabajo para la puesta en común y adopción de medidas dirigidas a evitar y minimizar los riesgos y los daños que la obtención y difusión de imágenes y audios a través de internet pueden provocar, especialmente a las víctimas de violencia de género y los menores de edad.

Asimismo, celebró reuniones con la secretaria de Estado de Igualdad y la delegada del Gobierno de Violencia de Género; la presidenta de Stop Violencia de Género Digital; y organizó una reunión de trabajo con representantes del Ministerio de Trabajo, Migraciones y Seguridad Social, la Confederación Española de Organizaciones Empresariales (CEOE), la Confederación Española de la Pequeña y Mediana Empresa (CEPYME), Comisiones Obreras y UGT, con el objetivo de trasladar a todos los agentes las últimas iniciativas puestas a disposición de los ciudadanos por parte de la Agencia, como el Canal Prioritario para comunicar la difusión de contenido sensible en internet y solicitar su retirada o las últimas recomendaciones para fomentar la privacidad de las víctimas de violencia de género.

En otro orden de cosas, la Agencia también celebró una jornada específica para hacer balance tras un año de aplicación de la Ley orgánica 3/2018, ley que adaptó el derecho español al RGPD. La inauguración del acto corrió a cargo de la directora de la AEPD, Mar España, y la clausura contó con la participación del secretario general técnico del Ministerio de Justicia, José Amérigo, y la presidenta del Comité Europeo de Protección de Datos, Andrea Jelinek.

Además, la Agencia celebró diversas reuniones de ámbito internacional, como la celebrada con la Delegación del Congreso de Chile, el Foro de Autoridades Iberoamericanas de Protección de Datos; el presidente de la Comisión Constitucional del Senado de Chile e impulsor del trámite sobre el proyecto de Ley de Protección de Datos de este país; el jefe de la Unidad de IT Policy del Supervisor Europeo de Protección de Datos (EDPS); el director de Fundamental Rights and Rule of Law -DG Justice- de la Comisión Europea; la Comisionada presidenta del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco, México (ITEI); el director del departamento del área internacional de la Federal Trade Commission. Asimismo, además de participar en las últimas reuniones plenarias y los Subgrupos del Comité Europeo de Protección de Datos, la Agencia intervino en el Seminario 'Training of Lawyers on the European Union´s Data Protection Reform', enmarcado en el proyecto europeo TRADATA y financiado por la Comisión Europea; la 41ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, el XVII Encuentro Iberoamericano de Protección de Datos y IV Foro Internacional de Datos Infoem.

Finalmente, el Consejo Consultivo de la Agencia de Protección de Datos -órgano colegiado de asesoramiento a la dirección de la Agencia – se reunió el 24 de enero, el 4 de julio y el 12 de diciembre de 2019 para exponer y analizar la actividad de la institución.

4.5 Infografías

La AEPD publicó en 2019 varias infografías como complemento a la información facilitada a través de sus canales. Todas ellas están disponibles en una **sección específica** la página web de la Agencia. Con motivo de la publicación de su Memoria anual, la AEPD publicó una **infografía** que ofrecía datos sobre reclamaciones, ejercicio de derechos, resoluciones, consultas más frecuentes del colectivo de menores, así como un resumen de las herramientas y recursos de la Agencia para ayudar a cumplir con el Reglamento General de Protección de Datos.

Por otra parte, coincidiendo con el primer año de aplicación del Reglamento, la Agencia publicó una **infografía** con información sobre el número de reclamaciones recibidas, resueltas, notificaciones de brechas de seguridad, casos con otras autoridades europeas, datos del número de delegados de protección de datos (DPD) designados, tanto del sector privado como público, así como cifras sobre el uso de herramientas de la AEPD para facilitar el cumplimiento, como Facilita o Informa.

Asimismo, en verano publicó '**Protección de datos en vacaciones**', con consejos de interés para la protección de datos personales en distintas situaciones, como la publicación de contenidos en internet, el uso de wifis abiertas o públicas, ordenadores compartidos, así como recomendaciones de seguridad para adelantarse al robo o pérdida de dispositivos y los datos contenidos en ellos.

Además, publicó sendas hojas de ruta con las obligaciones y aspectos a tener en cuenta para la adaptación al Reglamento General de Protección de Datos de las **Administraciones Públicas** y del **sector privado**.

La Agencia publicó también varios documentos en los que abordaba temas como la **protección de datos en la vuelta a clase**; el **Canal prioritario para comunicar la difusión de contenido sensible y solicitar su retirada**; **recomendaciones** y **consejos básicos para comprar en internet de forma segura**, y un **balance con las iniciativas y cifras más destacadas del Plan Estratégico 2015-2019** de la Agencia.

4.6 Actividades de divulgación: guías y herramientas al servicio de los Responsables

4.6.1 Actividades de divulgación

La AEPD continuó en 2019 con su compromiso de fomentar la cultura de protección de datos entre los ciudadanos y organizaciones. En este sentido, prosiguió celebrando jornadas de formación sobre las novedades del RGPD y la LOPDGDD dirigidas tanto al sector público como privado, a las que se suman las siguientes acciones de divulgación.

Reunión informativa

El 25 de enero la Agencia celebró una reunión informativa con medios de comunicación en el que la directora de la Agencia analizó el primer año de aplicación del Reglamento y la gestión de las reclamaciones recibidas, ofreciendo además otros datos de interés, como las acciones realizadas en 2018 y las iniciativas más relevantes previstas para 2019.

Presentación de las novedades de la Lista Robinson

El 8 de abril tuvo lugar la presentación de las novedades de la Lista Robinson, el servicio de exclusión publicitaria de la Asociación Española de la Economía Digital (Adigital) para proteger los datos personales de los ciudadanos y facilitar a las empresas el cumplimiento del RGPD y la LOPDGDD. La presentación fue desarrollada conjuntamente por la AEPD y Adigital.

11ª Sesión Anual Abierta de la AEPD

El 25 de junio la AEPD celebró su 11ª Sesión Anual Abierta, un encuentro que contó con la asistencia de más de más de 500 personas y pudo seguirse en directo en streaming a través de la web de la Agencia. La Sesión -que en esta edición amplió su formato tradicional, incorporando conferencias y mesas redondas paralelas en las que también intervinieron representantes de entidades públicas y privadas- se centró en efectuar un balance de los primeros 200 días de aplicación de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.

En la Sesión también tuvieron cabida otros temas, como el principio de responsabilidad activa y los mecanismos de supervisión de las autoridades de control para una actuación homogénea ante los desafíos globales; el papel del delegado de protección de datos tras el primer año de aplicación del Reglamento; los criterios respecto de las figuras del responsable, encargado y corresponsable del tratamiento; la vinculación entre el derecho a la protección de datos de carácter personal y otros derechos fundamentales y libertades que conforman la sociedad democrática, o la gestión del riesgo tecnológico en los tratamientos de datos.

Entrega de los Premios Protección de Datos 2018

La Agencia Española de Protección de Datos (AEPD) entregó durante la celebración de su 11ª Sesión Anual Abierta los 'Premios Protección de Datos 2018' en las categorías de Comunicación, Investigación, Adaptación al Reglamento y Buenas prácticas en centros escolares. Estos galardones reconocen los trabajos que promueven en mayor medida la difusión y el conocimiento del derecho fundamental a la protección de datos, así como su aplicación práctica en diferentes entornos.

El jurado –compuesto por el Consejo Consultivo de la AEPD– concedió el premio principal de comunicación a Mediaset España, por la difusión realizada en los canales del grupo de

los cambios incluidos en el Reglamento General de Protección de Datos (RGPD), tanto para ciudadanos como para responsables, que consiguió más de 155 millones de impactos, así como por el apoyo del canal Boing para difundir el uso responsable de las nuevas tecnologías entre los menores a través de los vídeos del canal Tú decides.

En la categoría de 'Buenas prácticas en privacidad y protección de datos personales sobre iniciativas para adaptarse al Reglamento europeo de Protección de Datos', en la modalidad de empresas, asociaciones y fundaciones, el jurado concedió el premio ex aequo a la Asociación Española de la Economía Digital (Adigital), por la adaptación del servicio de Lista Robinson al RGPD, y a la Asociación Multisectorial de la Información (ASEDIE), por su Código de Conducta del sector infomediario para el tratamiento de datos de carácter personal.

En el apartado de entidades del sector público, otorgó el premio a la Diputación Provincial de Valencia, por su proyecto de asistencia a las entidades locales de la provincia para el cumplimiento de la normativa de protección de datos de carácter personal. El jurado reconoció la implicación de la institución, por desarrollar el proyecto con medios y recursos propios y aportar una propuesta innovadora de formación y apoyo a los Delegados de Protección de Datos en el ámbito local, y especialmente en los municipios más pequeños.

En la categoría 'Premio a las 'Buenas prácticas educativas en privacidad y protección de datos personales para un uso seguro de internet', el jurado concedió el premio en la modalidad dirigida a centros de enseñanza públicos, concertados y privados de Educación Primaria, Educación Secundaria Obligatoria, Bachillerato y Formación Profesional, al IES Parque Goya (Zaragoza), por su programa 'Ciberayudantes', a través del cual alumnos a partir de 3º de la ESO ofrecen charlas a alumnos de cursos inferiores del propio centro, así como a distintos centros de la zona.

En la modalidad que reconoce el compromiso de personas, instituciones, organizaciones y asociaciones, públicas y privadas que hayan destacado por el impulso y difusión entre los menores de edad de buenas prácticas para un uso seguro de internet, el jurado otorgó el premio ex aequo a Pantallas Amigas, por su proyecto compuesto por varias iniciativas online dirigidas a la protección del colectivo de menores, y a Iván Carrasco Lozano (Ivangel Music), por difundir en su canal de YouTube vídeos que buscan fomentar la conciencia crítica de los jóvenes para evitar situaciones como el grooming o el ciberbullying.

Finalmente, en la categoría de 'Investigación en protección de datos personales Emilio Aced' el jurado otorgó el premio principal a José González Cabañas, Ángel Cuevas Rumín y Rubén Cuevas Rumín, por su trabajo 'Análisis y cuantificación del uso de datos sensibles por parte de Facebook', un análisis sobre las categorías especiales de datos en la red social. Asimismo, concedió el accésit a Javier Parra Arnau, Jagdish Prasa Achara y Claude Castellucia, por su trabajo 'MyAdChoices. Transparencia y control de la publicidad en línea', por diseñar una herramienta que tiene como fin permitir a los usuarios averiguar hasta qué punto se explotan sus perfiles de navegación para servirles anuncios, e investigar si los perfiles construidos por las empresas de publicidad revelan patrones de navegación únicos que puedan permitir, eventualmente, la identidad real del usuario.

Presentación Canal prioritario de la AEPD para comunicar contenidos sensibles y solicitar su retirada

El 24 de septiembre la AEPD presentó su Canal prioritario para comunicar la difusión de contenido sensible y solicitar su retirada, un sistema apoyado en un convenio y varios protocolos de colaboración suscritos por la Agencia con la Vicepresidencia del Gobierno y varios ministerios y organismos, en un acto presidido por la vicepresidenta del Gobierno y ministra de la Presidencia, Relaciones con las Cortes y Memoria Democrática, Carmen Calvo, y que contó con la presencia del ministro del Interior, Fernando Grande-Marlaska; la ministra de Educación y Formación Profesional, Isabel Celaá; ex ministra de Trabajo, Migraciones y Seguridad Social funciones, Magdalena Valerio; la ex

fiscal general del Estado, Mª José Segarra, y la presidenta del Consejo General de la Abogacía Española, Victoria Ortega.

- **Presentación de la actualización de la Guía de cookies**

  El 8 de noviembre, la AEPD y las asociaciones ADIGITAL, Anunciantes, AUTOCONTROL e IAB Spain presentaron la Guía sobre el uso de las cookies, actualización a la nueva normativa de la primera guía en Europa sobre esta materia elaborada conjuntamente por la autoridad de protección de datos y los representantes de la industria. El documento recoge las orientaciones, garantías y obligaciones que la industria debe aplicar para utilizar tanto cookies como tecnologías similares cumpliendo la legislación vigente.

- **Presentación de iniciativas para fomentar la privacidad de víctimas de violencia de género**

  El 22 de noviembre, la AEPD presentó un espacio web de ayuda a la protección de la privacidad de las víctimas de violencia de género, en un acto inaugurado por la directora de la Agencia, que también contó con la participación de la ex secretaria de Estado de Igualdad, Soledad Murillo.

  Junto a la web de ayuda, la Agencia presentó asimismo las Recomendaciones para la protección de datos en las políticas de prevención del acoso digital, un documento con el que se pretende fomentar que empresas y administraciones públicas incorporen a sus políticas de prevención del acoso digital medidas orientadas a la prevención y erradicación de este en los centros de trabajo. De este modo, la AEPD trata de abordar dos facetas de una misma problemática: por un lado, promover la ayuda a las víctimas de violencia de género en el entorno digital y, por otro, impulsar la adopción de políticas de prevención en los centros de trabajo que apliquen medidas específicas para su protección.

- **Presentación del marco de actuación de Responsabilidad Social**

  Por otra parte, el 27 de marzo, la AEPD presentó su Marco de Actuación de Responsabilidad Social 2019-2024, elaborado con la colaboración de Pacto Mundial de Naciones Unidas, y que se encuentra alineado con la Agenda 2030 y los Objetivos de Desarrollo Sostenible. Este marco de actuación es objeto de desarrollo en un epígrafe propio dentro de esta Memoria.

4.6.2 Premios recibidos por la AEPD

- XII edición de los 'Premios a la Calidad e Innovación en la Gestión Pública'. El 'Premio Ciudadanía' tiene por objeto destacar "prácticas innovadoras en la provisión de productos o servicios, así como en los sistemas de relación, con impacto externo en los ciudadanos o usuarios". La Agencia Española de Protección de Datos fue galardonada con un accésit en la categoría 'Ciudadanía' en la XII edición de los 'Premios a la Calidad e Innovación en la Gestión Pública', unos galardones del Ministerio de Política Territorial y Función Pública que reconocen a las organizaciones que se hayan distinguido por la excelencia de su rendimiento global, la innovación en la gestión de la información, el conocimiento y las tecnologías, así como por la calidad e impacto de sus iniciativas.

  El jurado distinguió con un accésit de su 'Premio Ciudadanía' la iniciativa de la Agencia al desarrollar Facilita_RGPD, una herramienta para ayudar al cumplimiento del Reglamento General de Protección de Datos (RGPD) a pymes y profesionales que traten datos personales de escaso riesgo.

- Premio de la Asociación Profesional Española de Privacidad (APEP) concedido a la Agencia Española de Protección de Datos, en la categoría de instituciones, y a Jesús Rubí, actual coordinador de la Unidad de Apoyo y Relaciones Institucionales de la AEPD, en la categoría de trayectoria profesional. La entrega tuvo lugar en el marco del VII Congreso Nacional de la APEP.

- Premio ISACA (Information Systems Audit and Control Association) concedido a la AEPD en la categoría de 'Liderazgo Inspirador'. La entrega tuvo lugar en el marco del congreso anual de ISACA, la High Level Conference of Assurance (HLCA).
- Premios otorgados en el marco de la Conferencia Internacional de Autoridades de Protección de Datos y de Privacidad. La 46ª Conferencia Internacional, celebrada en Tirana, concedió a la herramienta Facilita_RGPD de la Agencia el premio en la categoría 'People's Choice', el premio global de la Conferencia, que se concede al proyecto más votado por los miembros entre todas las candidaturas presentadas. A este galardón se sumó el premio 'Accountability', que reconoce el proyecto que mejor ha promovido de la responsabilidad proactiva, favoreciendo el cumplimiento de la normativa de forma práctica.

4.7. Transparencia

La Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno, impone a las Administraciones Públicas una serie de obligaciones en relación con los ciudadanos que se pueden agrupar en dos grandes apartados: la publicidad activa y el derecho de acceso a la información pública.

En lo que a la publicidad activa se refiere, en la página web de la Agencia se incluye una sección denominada 'Transparencia' cuyo cometido 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 cuatro grandes apartados, mostrando en cada uno de ellos, respectivamente, datos de Información institucional, organizativa y de planificación; información de relevancia jurídica; información económica, presupuestaria y estadística y otro tipo de información. En este último apartado, además de la información relativa a la agenda institucional y a la sesión anual abierta de la AEPD, se ha incluido el Inventario de Actividades de Tratamiento de la AEPD, como una nueva obligación de publicidad activa que se ha introducido para los responsables del tratamiento del sector público. Asimismo, se ha dado publicidad a las cláusulas que la AEPD utiliza para dar cumplimiento al derecho de información de los ciudadanos cuyos datos personales son tratados y a los datos de contacto del delegado de protección de datos de la AEPD. Además, también con una vocación de transparencia y de colaboración con los responsables de los tratamientos, se ofrece un modelo de cláusula para contratos con encargados del tratamiento.

Por lo que se refiere al ejercicio del derecho de acceso a la información pública, función que se lleva a cabo a través del Área de Atención al Ciudadano como Unidad de Información de Transparencia Singular (UITS) de la Agencia.

De enero a diciembre de 2019 se recibieron 82 ejercicios del derecho de acceso a la información pública, de los cuales, en 22 ocasiones en realidad se trataba de consultas sobre protección de datos u otras cuestiones, y en 4 casos se trataba de derechos de acceso a los datos personales. En los restantes casos, se concedió la información en 41 ocasiones, se inadmitió la solicitud en 6 casos y se denegó la información en 3. En 6 ocasiones se produjo el desistimiento por el solicitante.

5. Ayuda efectiva para las entidades

5.1 Acciones de difusión, concienciación y fomento del derecho a la protección de datos

La Agencia ha continuado desarrollando acciones de formación, sensibilización y comprensión de los riesgos, normas, garantías y derechos que establece el RGPD y la LOPDGDD, dirigidas a responsables, encargados, así como a los DPD con la finalidad de que puedan ejercer de manera efectiva y eficiente sus funciones.

A lo largo del año 2019 se han realizado las siguientes actuaciones:

Seguimiento y acompañamiento en la aplicación del RGPD a los diversos sectores de actividad en la que el tratamiento de datos personales constituye una actividad principal para la consecución de sus objetivos, y de aquellos otros en los que el tratamiento de datos constituye una actividad auxiliar en el marco de sus objetivos y finalidades, pero que constituyen un sector muy significativo de responsables y encargados del tratamiento.

Para la ejecución de esta tarea la AEPD organizó una serie de encuentros con los DPD para conocer de manera directa cómo estaban ejerciendo sus funciones, así como las dificultades que hubieran surgido en su desempeño, a los que se convocó a través de las organizaciones y asociaciones sectoriales más representativas de cada uno de ellos, que se concretaron en los siguientes:

	SECTOR	CONVOCADOS
20 de febrero	Universidades	DPD de las universidades parte de la CRUE
20 de marzo	Telecomunicaciones	Autocontrol, Digitales, Movistar, Vodafone, Orange Espagne, S.A.U. y Xfera Móviles, S.A.U.
4 de abril	Gran consumo y comercio electrónico	· AECOC (Asociación de Fabricantes y Distribuidores · ANGED (Asociación Nacional de Grandes Empresas de Distribución) · ASEDAS (Asociación Española de Distribuidores de Autoservicio y Supermercados) · ACES (Asociación de Cadenas Españolas de Supermercados) · CEC (Confederación Española de Comercio) · ADIGITAL (Asociación Española de Economía Digital) · Ministerio de Sanidad, Consumo y Bienestar Social · Ministerio de Industria, Comercio y Turismo · Red.es

	SECTOR	CONVOCADOS
10 de abril	Enseñanza (sector público y privado)	· Ministerio de Educación · DPD patronales de la educación: · Asociación de Centros Autónomos de Enseñanza Privada (ACADE) · Unión de Cooperativas de Enseñanza de Trabajo Asociado de Madrid (UCETAM) · Federación Española de Escuelas Católicas (FE-RE-CECA) · Confederación Española de Centros de Enseñanza (CECE) · Unión Española de Cooperativas de Enseñanza (UECOE)
24 de abril	Salud (sector público y privado)	· DPD Consejerías de Sanidad y Sistemas Públicos de Salud · Direcciones Generales de Salud/Sanidad de las CCAA · Mº de Sanidad, Consumo y Bienestar Social · Instituto Nacional de Gestión Sanitaria (INGESA) · Consejerías de Sanidad de las CCAA · Asociaciones patronales: · Alianza de la Sanidad Privada Española (ASPE) · 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) · Unión Catalana de Hospitales (UCH) · Asociación Nacional Empresarial de la Industria Farmacéutica (FARMAINDUSTRIA)
8 de mayo	Energía (eléctricas y gas)	· AELĒC (Asociación de Empresas de Energía Eléctrica) · AOP (Asociación Española de Operadores de Productos Petrolíferos) · SEDIGAS (Asociación Española del Gas)

	SECTOR	CONVOCADOS
22 de mayo	Seguros	DPD de compañías de seguros a través de UNESPA
5 de junio	Entidades financieras	· DPD de entidades financieras · AEB (Asociación Española de Banca) · CECA (Confederación Española de Cajas de Ahorros)
26 de junio	Consejos y Colegios Profesionales	· DPD de Consejos y Colegios Generales · Unión Profesional

Formación:

a) Se ha continuado impartiendo formación a través de los cursos organizados por el INAP y que tienen como finalidad dotar de los conocimientos y prácticas necesarias para el desempeño de las funciones del DPD en las AAPP. Consta de un itinerario preestablecido en 2 fases, o cursos, el primero online y el segundo semipresencial, cuyo acceso exige superar el primero.

b) Mediante las acciones derivadas de la ejecución del proyecto europeo T4DATA, en cuyo consorcio, liderado por la Fundación italiana Basso, la AEPD es parte junto con las autoridades nacionales de supervisión de protección de datos de Italia, Croacia, Bulgaria y Polonia, que se detalla posteriormente.

El objetivo del proyecto T4DATA es proporcionar apoyo para la capacitación de los Delegados de Protección de Datos (DPD) de los organismos públicos locales (autonómicos, provinciales, locales, institucionales) sobre las implicaciones prácticas y posibles interpretaciones del RGPD.

Durante el primer semestre se realizaron los siguientes seminarios dirigidos a empleados públicos fundamentalmente de las Administraciones locales (autonómicas, provincial, local, institucional), DPD o involucrados en el ámbito de la protección de datos personales:

FECHA	LUGAR	ASISTENTES	OBSERVACIONES
20.02.2019	Madrid	69	Organizado por la AEPD y dirigido a DPD de Universidades (CRUE)
12.03.2019	Badajoz	140	Organizado por la AEPD, la Diputación de Badajoz y la Fundación Democracia y Gobierno Local
13.03.2019	Sevilla	110	Organizado por la AEPD, la Diputación de Sevilla y la Fundación Democracia y Gobierno Local

FECHA	LUGAR	ASISTENTES	OBSERVACIONES
27.03.2019	Málaga	118	Organizado por la AEPD, el Consejo de Transparencia y Protección de Datos de Andalucía y la Diputación de Málaga
28.03.2019	Sevilla	108	Organizado por la AEPD, el Consejo de Transparencia y Protección de Datos de Andalucía y el Parlamento de Andalucía
03.04.2019	Cáceres	186	Organizado por la AEPD, la Diputación de Cáceres y la Fundación Democracia y Gobierno Local
11.04.2019	Lugo	163	Organizado por la AEPD, la Diputación de Lugo y la Fundación Democracia y Gobierno Local
11.04.2019	Madrid	80	Organizado por la AEPD y la Comunidad de Madrid
10.05.2019	Jaén	140	Organizado por la AEPD, la Diputación de Jaén y la Fundación Democracia y Gobierno Local

Dentro del proyecto T4DATA, la Agencia Española de Protección de Datos ofreció, a través de la plataforma del INAP, un curso online masivo y gratuito (MOOC) de formación sobre protección de datos dirigido a empleados públicos de las Administraciones autonómicas universitarias e institucionales que sean DPD de las AAPP y a las personas de sus equipos, así como a aquellas que aspiren a serlo o que entre sus funciones y tareas el tratamiento de datos personales tenga una especial incidencia.

MOOC de formación para Delegados de Protección de Datos de Administraciones Públicas

El curso ha contemplado la celebración de varios webinarios en los que se han abordado todas las cuestiones derivadas de la aplicación de las funciones del DPD. Comenzó el 23 de septiembre de 2019 y finalizó a primeros de enero de 2020.

c) Otras acciones formativas:

- Ministerios: Hacienda, Presidencia, Fomento, Educación y Formación Profesional, Sanidad, Consumo y Bienestar Social, Justicia, Interior, Agencia Española del Medicamento y Agencia Española de Cooperación Internacional
- Jornada directores de Institutos de Medicina Legal y Ciencias Forenses en Logroño (29.03.19)
- Jornada para responsables de actividades de tratamiento dirigida a los DPD de los Ministerios.
- Jornada en la Dirección General de Consumo de la Comunidad Autónoma de Madrid (12.06.19)
- Curso del Instituto Asturiano de Administración Pública (IAAP) dirigido a operadores de la Consejería de Educación (20.06.19)
- Jornada para DPD en la Universidad de Sevilla (19.09.19)

- Jornada para DPD en la Diputación de Valencia (25.09.19)
- Congreso Nacional de Registradores en Sevilla (04.10.19)
- Jornada organizada por el Ministerio Fiscal en A Coruña (15.10.19)
- Jornada para DPD Administración General de Estado y Órganos Constitucionales (23.10.19)
- Jornada para DPD de las Administraciones Autonómicas. En esta Jornada se realizó la presentación del Canal Prioritario de la AEPD, por lo que también se invitó a los/as responsables de los Institutos de la Mujer y/o Direcciones Generales de la Mujer (30.10.19)
- Curso Transparencia y Administración - Ayuntamiento de Pontevedra (15.11.19)
- Jornada para Asociaciones y Fundaciones-Fundació Catalana de l'Esplai -Fundesplai- (21.11.19)
- Encuentro de DPD en el ámbito de la Administración Local en Valencia (26.11.19)
- 11ª Conferencia Internacional sobre la Reutilización de la Información del Sector Público organizada por ASEDIE (28.11.19)
- Curso Ley de Transparencia y Ley de Protección de Datos - Diputación de Guadalajara (12.12.19)

d) Participación en Webinarios

Organizado por el Instituto de Nacional de Tecnologías Educativas y Formación del Profesorado (INTEF), en el que se trataron cuestiones relacionadas con las líneas de actuación de la AEPD y la protección de datos en los centros educativos (28.11.19)

'Cómo adaptarse a la normativa sobre protección de datos siendo autónomo o pyme', organizado por Infoautónomos (29.11.19)

Subcomunidad para Delegados de Protección de Datos

Desde enero se encuentra disponible la Subcomunidad para Delegados de Protección de Datos de las AAPP, que mantiene la Red Social del INAP y de la que la AEPD es la administradora.

El objetivo de esta subcomunidad es el establecimiento de un espacio para compartir y discutir experiencias y dudas relacionadas con las funciones asignadas a las personas y equipos que ejerzan la función de delegados de protección de datos en el ámbito de las administraciones públicas. En ella también se publican las referencias que la AEPD entiende que pueden interesar a la comunidad de DPD de las AAPP.

La subcomunidad de delegados de protección de datos de las Administraciones Públicas está dirigida a las personas y equipos que ejerzan las funciones de delegados de protección de datos señaladas en el RGPD y la LOPDGDD. El acceso está restringido a las personas que formen parte de los equipos que ejerzan la función de delegados de protección de datos.

5.2 El Registro de Delegados de Protección de Datos

El RGPD establece, en su artículo 37.7, la obligación del responsable o encargado de tratamiento de comunicar los datos de contacto de su delegado de protección de datos (DPD) a la autoridad de control. Obligación que reproduce el artículo 34.3 de la LOPDGDD que, en su apartado 4, establece la obligación de la AEPD de mantener una lista actualizada de DPD accesible por medios electrónicos.

A 31 de diciembre de 2019, un total de 50.356 entidades habían comunicado el DPD con sus datos de contacto, de los cuales 134 corresponden a responsables del tratamiento de la Administración General del Estado; 378 a las Administraciones Autonómicas; 2.593 a las Entidades Locales; 3.182 a Órganos Constitucionales, Colegios Profesionales, Cámaras de Comercio, Notarios, Registradores de la Propiedad, Federaciones Deportivas. En el sector privado el número de DPD comunicados alcanzó un total de 44.069.

Los datos de contacto de los DPD comunicados a la AEPD se pueden consultar a través de la Sede electrónica.

El RGPD contempla que el DPD forme parte de la plantilla del responsable o encargado del tratamiento (interno), o desempeñar sus funciones en el marco de un contrato de servicios (externo). Aproximadamente el 80% de los responsables y encargados que procedieron a comunicar su DPD manifestaron disponer de un DPD externo, que no pertenecía a la organización.

5.2.1 Canales de actuación con los DPD de la Administración

El artículo 37.1.a) del RGPD estipula que toda autoridad u organismo público debe contar con un delegado de protección de datos. En este contexto la AEPD mantiene una línea de contacto específica con los DPD de los órganos constitucionales y de todas las administraciones públicas con el objeto de conocer la problemática específica que pueda surgir en el ejercicio de sus funciones y facilitar la comunicación con la autoridad de control. En este sentido se han mantenido encuentros específicos con los delegados de los órganos constitucionales y la administración general del estado, el 23 de octubre, y con los delegados de las comunidades autónomas, 30 de octubre. Así mismo se mantiene una línea de contacto permanente a través del correo electrónico y el teléfono que permita responder de forma ágil e inmediata a cualquier problemática imprevista.

En este mismo sentido, y con objeto de poner a disposición de las administraciones locales esquemas que respondan a actividades de tratamiento y cláusulas informativas comunes en los tratamientos que las corporaciones realizan, la AEPD ha formado parte de un grupo de trabajo liderado por la Fundación Democracia y Gobierno Local y cuyos resultados se publicarán durante este año 2020.

5.3 Certificación

El artículo 35 de la LOPDGDD prevé que el cumplimiento de los requisitos exigibles a los delegados de protección de datos (DPD) podrá demostrarse, entre otros medios, a través de mecanismos voluntarios de certificación.

El papel fundamental de los DPD en el actual sistema de gestión de datos personales determinó que la Agencia Española de Protección de Datos, con el objetivo de ofrecer seguridad y fiabilidad tanto a los profesionales de la privacidad como a las empresas y entidades que van a incorporar esta figura a sus organizaciones, o que necesitan contratar los servicios de un profesional cualificado y capacitado, promoviera un Esquema de Certificación para que los responsables y encargados puedan seleccionar profesionales cuyas competencias como DPD hayan sido certificadas por entidades previamente acreditadas por la Entidad Nacional de Acreditación (ENAC).

El Esquema de Certificación de DPD, cuya primera versión se publicó el 14 de julio de 2017, dispone que la Agencia Española de la Protección de Datos es la responsable de su desarrollo, revisión y validación cuando las condiciones lo aconsejan, involucrando a las diferentes partes interesadas reunidas en el Comité Técnico creado en el propio Esquema.

La aplicación práctica del Esquema desde su puesta en marcha ha puesto de manifiesto aspectos susceptibles de mejora que, junto con la necesidad de adecuarlo a la existencia de entidades de certificación ya acreditadas por ENAC, han justificado la necesidad de su revisión y actualización.

En consecuencia, la Agencia Española de Protección de Datos, de conformidad con las funciones que le atribuyen los artículos 57.1 y 47 del RGPD y la LOPDGDD, respectivamente, y previa información al Comité Técnico convocado al efecto el 20 de diciembre de 2019, procedió a modificar el Esquema de Certificación adoptando una nueva versión, la 1.4, el 23 de diciembre que fue aprobada por resolución ya de 10 de enero de 2020.

Las principales novedades que presenta la nueva versión del Esquema de Certificación hacen referencia a la inclusión de un código ético para las entidades de certificación y para las entidades de formación, cuyo incumplimiento puede dar lugar a la resolución del contrato de uso de la marca del Esquema, lo que impediría operar en el Esquema que, en su caso, implicaría la extinción de la acreditación al no poder operar en el esquema sin la marca.

Se actualizó y adecuó el contrato de uso de la marca a la obligación de las entidades de certificación y de formación de respetar el código ético.

A la vez, se ha dado un nuevo diseño a la marca del Esquema que proporciona información de utilidad, al incluir las fechas de acreditación, o de certificación según se utilice por una entidad de certificación o por un DPD.

Así mismo se adecuó el Esquema a la situación actual, en la que ha dejado de ser necesaria la acreditación provisional al contar el mercado con varias entidades de certificación acreditadas plenamente operativas.

También se mejoraron algunos aspectos, como la elaboración de preguntas por las entidades en proceso de acreditación, o la realización de pruebas durante dicho proceso.

A fecha 31 de diciembre habían sido acreditadas las seis entidades de certificación de DPD.

Así mismo, a 31 de diciembre habían sido certificados como DPD 418 profesionales, y se habían reconocido 72 programas de formación.

5.4 Códigos de Conducta

Los códigos de conducta constituyen una muestra de lo que se denomina autorregulación, es decir, la capacidad de las entidades, instituciones y organizaciones para regularse a sí mismas a partir de la normativa establecida. Son mecanismos de cumplimiento voluntario en los que se establecen reglas específicas de protección de datos para categorías de responsables o encargados del tratamiento.

El desarrollo de los códigos de conducta durante 2019 se ha visto afectado por la adopción, e4 de junio, por el Comité Europeo de Protección de Datos (CEPD) de las Directrices 1/2019 sobre los códigos de conducta y los organismos de su supervisión que fueron sometidas a consulta pública entre el 19 de febrero y el 2 de abril; así como por el transcurso del plazo de un año establecido en la Disposición adicional segunda de la LOPDGDD para adecuar los códigos tipo que, con arreglo a la normativa anterior, fueron inscritos en el Registro General de Protección de Datos.

El 1 de abril, con la finalidad de informar sobre las Directrices del CEPD, que en ese momento se encontraban en consulta pública, e impulsar la adecuación la educación de los códigos tipo a la regulación del RGPD, se celebró una sesión informativa en la sede de la AEPD a la que se convocaron todos los promotores de códigos tipo (17). Así mismo, se ha dado respuesta a 16 consultas relativas a los códigos de conducta que se han formulado a través de la sede electrónica de la AEPD.

De los 17 códigos tipo se han recibido 5 proyectos para su actualización y adecuación a la regulación de los códigos de conducta.

Conforme a lo dispuesto en el artículo 41.4 del RGPD, la AEPD elaboró y sometió a dictamen del CEPD los criterios para la acreditación de los organismos de supervisión de los códigos de conducta, cuya publicación se ha realizado ya en 2020.

A 31 de diciembre la situación de los códigos de conducta era la siguiente:

a) En estudio:

- Código de conducta del sector infomediario protección de datos promovido por la Asociación Multisectorial de la Información (ASEDIE).
- Código de conducta para el tratamiento de datos en la actividad publicitaria promovido por la Asociación para la Autorregulación de la Comunicación Comercial (AUTOCONTROL).

b) En estudio la adecuación de los códigos tipo a la regulación del CEPD (Disposición transitoria segunda de la LOPDGDD, promovidos por:

- La UNED
- La Universidad de Castilla-La Mancha
- Farmaindustria
- La Asociación Española de Micropréstamos
- Unión Española de Entidades Aseguradoras y Reaseguradoras (UNESPA)
- Unión Catalana de Hospitales
- Confianza Online
- Asociación Nacional de Entidades de Gestión de Cobro (ANGECO)
- Asociación Catalana de Recursos Asistenciales (ACRA)
- Establecimientos sanitarios privados de la provincia de Sevilla
- Asociación nacional de Empresas de Investigación de Mercados y Opinión Pública (ANEIMO)

También durante 2019 se ha procedido a la inadmisión de tres proyectos de códigos de conducta.

Asimismo, con otros 14 promotores de códigos de conducta se han mantenido reuniones y contactos previos a la presentación formal para su aprobación:

- Código de conducta sobre atención y mediación de derechos en protección de datos, promovido por Adigital.
- Código de conducta del Servicio de Lista Robinson, promovido por Adigital.
- Código de conducta de protección de datos personales Kumon, promovido por Kumon Instituto de Educación de España.
- Código de conducta para la protección de datos de carácter personal de la Unión de Federaciones Deportivas Madrileñas (UFEDEMA).
- Código de conducta agencias de viajes, promovido por la Unión de Agencias de Viajes.
- Código de conducta del Colegio de Ingenieros de Telecomunicaciones.
- Código de conducta de Orange.
- Código conducta contact centers, promovido por asociación CEX.
- Código de conducta de oficinas de farmacia provincia de Alicante.
- Código de conducta de ANF, entidad de certificación.
- Código de conducta del Consejo Andaluz de Colegios de Médicos.
- Código de conducta Registros de la Propiedad, Mercantiles y de Bienes Muebles.
- Código de conducta sector turístico/hotelero.
- Código de conducta para regular el servicio de intercambio de información para la prevención del fraude.

5.5 Recursos para facilitar el cumplimiento del RGPD

5.5.1 Canal INFORMA_RGPD

El canal INFORMA_RGPD se puso en marcha en marzo del año 2018 con el objetivo de ayudar en la aplicación del RGPD y de resolver las cuestiones y dudas que pudieran derivarse en la práctica.
Los destinatarios de este recurso de ayuda son los sujetos obligados, tanto responsables y encargados del tratamiento como delegados de protección de datos, ya sean de designación obligatoria o facultativa y procedentes tanto del sector público como del sector privado, así como las organizaciones y asociaciones de categorías de responsables y encargados.
De 1 de enero al 31 de diciembre de 2019 se han atendido un total de 2.758 consultas, que han planteado cuestiones con un grado de complejidad que han exigido un mayor grado de análisis para poder dar una respuesta.

Los temas más demandados han sido aquellos relacionados con la necesidad de nombrar un Delegado de Protección de Datos; con las figuras del encargado, responsable y corresponsable; con el tratamiento de datos en el ámbito laboral, debido a los cambios legislativos que se han realizado (registro de jornada laboral y tratamiento de datos biométricos); con la videovigilancia; la salud; y el ejercicio de derechos.

5.5.2 Guías

Además de las guías, modelos y notas técnicas de carácter tecnológico que figuran en el apartado relativo a la Unidad de Evaluación y Estudios Tecnológicos, en el año 2019 se han adoptado las siguientes iniciativas para facilitar el conocimiento y cumplimiento de la normativa de protección de datos.

Actualización de la Guía sobre el uso de las cookies

La Agencia Española de Protección de Datos (AEPD) y las asociaciones ADIGITAL, Anunciantes, AUTOCONTROL e IAB Spain participaron en la actualización de la Guía sobre el uso de las cookies, para actualizarla adaptándola al RGPD.

La Guía recoge las orientaciones, garantías y obligaciones que la industria debe aplicar para utilizar tanto cookies como tecnologías similares (fingerprinting y otras) cumpliendo la legislación vigente.

El documento analiza la necesidad de obtener el consentimiento informado de usuario antes de instalar las cookies, recogiendo tanto la obligación de transparencia en la información como el consentimiento en sí mismo, teniendo en cuenta que la nueva normativa de protección de datos establece unos requisitos más estrictos. Además, la Guía se complementa con ejemplos prácticos de fórmulas válidas para facilitar información y recabar el consentimiento de los usuarios; así como para rechazarlas, configurarlas o revocar los consentimientos prestados, de forma que resulte tan sencillo obtenerlo como revocarlo.

Guía del paciente

Se ha elaborado y publicado en la página web de la Agencia una Guía en la que se recogen los derechos de los pacientes relacionados con la protección de sus datos personales. Se ha indicado la información que tienen derecho a recibir los pacientes cuando se utilizan sus datos por parte de profesionales sanitarios y los derechos que les asisten, entre otros puntos. Además, al final de la Guía, se incluye un apartado de preguntas frecuentes y sus respuestas.

Guía de profesionales sanitarios

De manera paralela a la guía del paciente, se ha trabajado en una Guía dirigida a los profesionales del sector sanitario, donde se abordan diferentes cuestiones relativas al cumplimiento de la normativa de protección de datos en dicho ámbito; guía que será presentada en 2020.

Guía de relaciones laborales

Durante el año 2019 se ha trabajado en una nueva Guía de Protección de datos en la Relación Laboral, que se está ultimando y se presentará a lo largo del año 2020. Como punto de partida, se ha tomado el índice de la anterior Guía “La protección de datos en las relaciones laborales”, del año 2009, actualizando y ampliando de manera considerable la información proporcionada.

5.6 Transferencias internacionales

Con arreglo a la regulación de las transferencias internacionales de datos que establece el RGPD, en su Capítulo V, y la LOPDGDD, en sus Título VI, la AEPD, con fecha 14 de mayo de 2019, ha autorizado la transferencia internacional de datos personales a la entidad Comisión Nacional del Mercado de Valores (CNMV) con destino a autoridades de supervisión financiera ubicadas en países que no pertenecen al Espacio Económico Europeo.

Las garantías adecuadas, que incluían derechos efectivos y exigibles para los interesados, se aportaron a través de un acuerdo administrativo, previsto en el artículo 46.3.b) del RGPD, entre la Autoridad Europea de Valores y Mercados (ESMA) y la Organización Internacional de Comisiones de Valores (IOSCO), que fue informado favorablemente por el Comité Europeo de Protección de Datos (CEPD) conforme al mecanismo de coherencia como dispone el artículo 46.4 del RGPD y 42.2 de la LOPDGDD.

A finales de 2019, se ha presentado una solicitud de autorización para realizar transferencias internacionales de datos entre encargados del tratamiento, en el que las garantías se han aportado a través de cláusulas contractuales, cuya resolución va a requerir el dictamen del CEPD.

Así mismo, durante 2019, la Agencia Española de Protección de Datos ha tramitado, como autoridad líder, las solicitudes de aprobación de Normas Corporativas Vinculante (BCR por sus siglas en inglés) correspondientes a dos grupos empresariales que tienen su sede principal en España, y cuyo procedimiento se espera concluir en 2020, teniendo en cuenta que sobre una de ellas ya se cuenta con la opinión favorable del Comité Europeo de Protección de Datos, conforme a lo que establecen los artículos 47.1 y 41.2 del RGPD y de la LOPDGDD, respectivamente.

Hay que añadir la tramitación de una solicitud de modificación de las BCR de un grupo empresarial derivada del cambio de autoridad líder como consecuencia del BREXIT. Además durante 2019, la AEPD ha participado en la correvisión de 6 BCR lideradas por otras autoridades de control.

6. La potestad de supervisión

6.1 Resultados

El análisis de los resultados sobre la potestad de supervisión de la Agencia en 2019 está condicionado por la concurrencia de un conjunto de circunstancias que se describen a continuación.

El trámite de traslados, que tiene como objetivo facilitar la resolución amistosa de reclamaciones, promovido por el RGPD y articulado en la LOPDGDD, implica una ampliación de los días de tramitación de las reclamaciones asociada a la necesidad de remitirlas, con el fin de solicitar información al responsable o a su DPD, esperar respuesta y evaluarla.

Este trámite se ha aplicado en 2019 durante todo el año frente a 2018 en el que sólo se aplicó durante la mitad del ejercicio.

En este nuevo escenario, como se comentará más adelante, puede decirse que las reclamaciones pueden resolverse más rápidamente, y es menor el número de ellas que acaba ocasionando la iniciación de un procedimiento por infracción de la normativa de protección de datos. Ya en el ejercicio 2018 se observó un descenso en la cifra de resoluciones de la potestad sancionadora, descenso que se ha intensificado de forma notoria en 2019.

En la aplicación del RGPD para las reclamaciones presentadas, a diferencia de años pasados, ya no diferencian las denuncias y las reclamaciones de tutela de derechos, denominándose a todas ellas bajo el epígrafe de reclamaciones.

Otra de las novedades del escenario creado por el RGPD es el relativo a los casos transfronterizos. Con la aplicación efectiva del RGPD los ciudadanos pueden presentar reclamaciones ante cualquier autoridad del Espacio Económico Europeo, y las autoridades intercambiarán las reclamaciones recibidas para que sean atendidas adecuadamente. El sistema de información que soporta este intercambio es el IMI.

En la tramitación de casos transfronterizos ha concurrido un condicionamiento similar al antes mencionado, ya que en 2018 sólo se tramitaron en el segundo semestre, mientras que en 2019 se tramitaron durante el año completo.

Por otra parte, el RGPD extiende la obligación de notificar las brechas de seguridad sufridas por las distintas entidades. Estas notificaciones, son inicialmente recibidas por la Unidad de Estudios y Evaluación Tecnológicos. Tras un primer análisis, sólo algunas dan lugar a actuaciones previas de investigación.

En lo relativo al procedimiento sancionador, el RGPD y la LOPDGDD incorporaron otra novedad, que es la unificación del procedimiento sancionador, independientemente de la naturaleza pública o privada del infractor. En caso de que el infractor tenga naturaleza privada, se podrá resolver con una sanción económica o con un apercibimiento. En caso de que el infractor tenga naturaleza pública, siempre se resolverá, en el caso de que se compruebe la actuación infractora, con apercibimiento. Tanto la multa administrativa como el apercibimiento pueden ir acompañados de medidas correctoras de las infracciones.

Asimismo, se han remitido reclamaciones a las autoridades autonómicas de protección de datos o al Consejo General del Poder Judicial por referirse a materias de su competencia.

El detalle del conjunto de reclamaciones tramitadas por la Subdirección General de Inspección de Datos y su valoración se ha incluido en el apartado correspondiente de la “Memoria en cifras”.

6.2 Procedimientos más relevantes

Ámbito nacional

Entre los procedimientos más relevantes del ejercicio 2019 podemos destacar los expedientes abiertos a dos entidades bancarias españolas por incumplimientos del RGPD en la política de privacidad que se ofrece a los clientes. Estos expedientes han dado lugar a dos procedimientos sancionadores cuya tramitación no ha concluido en el periodo que abarca esta memoria.

Se han abierto varios expedientes de investigación aplicando el enfoque del RGPD para investigar incumplimientos de la normativa, no asociados a una reclamación concreta sino a la no adecuación a la normativa de determinados procesos de tratamiento de responsables y/o encargados de diferentes sectores.

También se han abierto varias actuaciones de investigación consecuencia de la recepción de notificaciones de brechas de seguridad. La mayoría de ellas finalizaron con el archivo de las actuaciones.

Igualmente, cabe mencionar la tramitación de un procedimiento sancionador **PS/00326/2018** a la Liga Nacional de Fútbol Profesional por publicar una app para dispositivos móviles con capacidad de recoger sonidos de ambiente. Se impuso una sanción de 250.000 euros. La entidad ha interpuesto recurso contencioso-administrativo.

El expediente de investigación abierto a la Dirección General de la Policía en el año 2018 en relación con la información difundida en medios de comunicación sobre posibles accesos a datos de ficheros policiales del Ministerio del Interior culminó en el 2019 con un procedimiento (AAPP/00001/2019), a raíz del cual se han llevado a cabo diversas actuaciones para el seguimiento de la ejecución de las medidas a implementar.

Puede mencionarse, asimismo, que, tras la finalización del proceso judicial instruido, se reanudó la tramitación del **PS/00258/2016**. En la resolución que pone fin al citado procedimiento, se sanciona por incumplimiento de la LOPD y de la LSSI con una multa de 1.450.000 euros a dos personas que, para cometer la estafa millonaria por la que fueron condenados en la vía penal, sometieron a tratamiento sin habilitación legal datos especialmente protegidos: de salud, de orientación sexual, de origen étnico, de ideología, de menores de edad, sin las medidas de seguridad pertinentes y que utilizaban para captar a las victimas comunicaciones comerciales por medios electrónicos sin autorización ni la concurrencia de los requisitos legalmente establecidos.

Cuantitativamente, el mayor número de expedientes resueltos son consecuencia de reclamaciones de videovigilancia, en la que los particulares denuncian a vecinos que han instalado cámaras que graban de forma desproporcionada y sin cartel informativo. Las sanciones que se imponen son de apercibimiento, en el caso de que los responsables sean personas físicas, requiriendo que la grabación sea la mínima imprescindible para cumplir la finalidad de seguridad para la que se instala y que se informe, si es preciso, de su instalación.

También resultan significativos, por su número, los procedimientos sancionadores que son consecuencia de que en las páginas web, en las que se recogen datos, o bien no existe información de la política de privacidad, conforme establece el artículo 13 RGPD, o la información es deficiente. Asimismo, se denuncia y sanciona, el incumplimiento de las obligaciones de obtener un consentimiento informado para la utilización de cookies u otros dispositivos análogos.

Asimismo, son relevantes los procedimientos relacionados con el tratamiento de datos en el sector sanitario, como es el caso del expediente **TD/00291/2019**, que se tramitó al solicitar el reclamante la rectificación de un informe sobre su persona relativo a su salud mental y el ejercicio del derecho de acceso. “Se solicitaba el acceso a datos personales, concretado en la siguiente información: información sobre el origen de dichos datos, es decir, la identificación con nombre

y apellidos, puestos y domicilio de trabajo de los otros profesionales que manifestaron datos sobre la salud mental del padre, según la frase que Don (…) recoge en el Informe "la información recogida de otros profesionales sobre la salud mental del padre"

Solicita que se "eliminen los datos referidos a maltrato, por ser igual dato inexacto, y a posibilidad de enfermedad mental del padre, por no haber sido evaluado para tal fin".

En la reclamación presentada en esta Agencia, el reclamante solicitaba, además de la rectificación, el acceso a los datos de los profesionales que llevaron a emitir un informe respecto a su salud mental, así como el origen de esos datos. La información está incluida en un peritaje que solicitó la madre separada sobre los problemas de su hijo menor. Se rectificó lo referente al maltrato, pero no se facilitó quiénes eran los profesionales que le habían visitado para determinar su salud mental. No obstante, se estimó la tutela para que contestaran al reclamante.

En el marco de la prestación de servicios sanitarios cabe destacar, también, el **PS/00366/2018** La reclamación se dirige contra una Consejería de Sanidad como responsable última de que un Centro de Salud y un Hospital, ambos de titularidad pública, hayan facilitado sin su consentimiento informes médicos de los reclamantes a su hija. Dichos informes clínicos fueron utilizados por su hija ante un juzgado de Primera instancia, solicitando ser nombrada administradora provisional de su patrimonio, hasta que se dicte resolución judicial declarando la incapacidad de sus padres.

Respecto al Hospital, manifiestan que una vez que se aporta el correspondiente informe clínico, el protocolo médico de asistencia para pacientes con patologías neurológicas, aconseja que estos pacientes, por razones obvias, vayan acompañados de manera habitual a las consultas médicas por una tercera persona (en el presente caso, su hija, con el objeto de que pueda orientar mejor a los pacientes en relación con las informaciones recibidas por parte del personal sanitario.

Respecto al Centro de Salud, la Consejería de Sanidad manifestó que no se había podido emitir ningún informe clínico, puesto que las peticiones realizadas no cumplían los requisitos mínimos de validez para garantizar la representación, debido a que, a diferencia de lo que ocurrió en el Hospital, el representante se negó a cumplimentar el modelo oficial de ejercicio de derechos ARCO, y no pudo acreditar la representación de los reclamantes.

Se sancionó al Hospital por vulneración del deber de secreto, al no haber acreditado la hija la representación ni la incapacitación de los padres o su autorización.

La reclamación del **PS/00424/2018** viene motivada porque datos de salud de un tercero fueron incorporados a su historia clínica tras ser atendido en varias ocasiones en un Hospital, e identificarse con datos correspondientes al hijo del reclamante.

Según el reclamante, dicho tercero acudió identificándose como el reclamante al Servicio de Urgencias de dicho Centro una noche de 2016 de madrugada, otro día posterior, e ingresó un tercer día para una intervención quirúrgica, dándose a la fuga finalmente, pero sin documentación alguna que acreditará la identificación facilitada, a pesar de lo cual por parte del Centro Hospitalario no se efectuó ninguna constatación al respecto.

Al pedir el acceso a la historia clínica, no sólo le dieron los datos del suplantador sino también de un tercero con su mismo nombre y apellidos, pero distinta edad y patología. Se apercibió al ser un Hospital público, y a lo largo de la tramitación del procedimiento, corrigieron el error.

Finalmente, en el **PS/00238/2019** la reclamante denuncia a una clínica ya que la cláusula de envío de información comercial por parte de dicha clínica establece que para no recibir publicidad hay que marcar una casilla, lo cual considera contrario a la normativa de protección de datos que establece que para la remisión de publicidad se necesita un acto afirmativo, y no uno negativo. Lo modificaron de forma inmediata.

En cuanto a expedientes transfronterizos, destacan varios casos abiertos por la Autoridad de Control Española, que están siendo liderados por la Autoridad Irlandesa, y en los que la AEPD participa como autoridad interesada (art. 60 del RGPD). Es el caso que se tramita contra Facebook por no comunicar las solicitudes de supresión de datos a los terceros cesionarios de los mismos y no suprimirlos de forma efectiva en sus propios sistemas. También destaca el caso que se sigue contra WhatsApp por no facilitar la portabilidad de los datos personales de forma completa ni en un formato de uso común.

La Autoridad de Control Española participa también como interesada en otros casos relevantes para nuestros ciudadanos como el que se sigue en Luxemburgo contra Amazon por procesamiento ilegal y cesión de datos a terceros, o el caso seguido contra la misma compañía por el tratamiento de datos personales realizado mediante sus altavoces inteligentes y por el almacenamiento de datos bancarios en su plataforma de comercio electrónico sin informar ni recabar el consentimiento de sus clientes, y los que se siguen en Irlanda contra algunas redes sociales como LinkedIn, Whatsapp, Twitter e Instagram. Entre estos procedimientos merecen especial consideración los seguidos contra Linkedin por el envío de correos electrónicos invitando a los destinatarios a unirse a la red profesional de un miembro de la red social; contra Whatsapp por no atender el ejercicio de los derechos de acceso y oposición relacionados con la comunicación de datos de dicha red social a Facebook; contra Twitter por el fallo de la funcionalidad "Borrar toda información de localización" en una cuenta y contra Instagram por hacer públicas las fotografías almacenas en las cuentas de menores de 16 años, así como uno de sus datos de contacto, al convertirse sus cuentas en cuentas "de negocio".

Asimismo merece ser destacado el caso que se sigue en Bélgica contra IAB por su sistema de Apuestas en Tiempo Real o RTB (Real Time Bidding), o en Irlanda contra Google por el procesamiento manual de mensajes de voz recibidos de los usuarios.

También es oportuno señalar que la Autoridad de Control española ha mantenido contactos con la Autoridad de Control de Irlanda para participar en una operación conjunta en el seno de una investigación liderada por Irlanda.

Por otra parte, España lidera 33 casos transfronterizos con el apoyo de otras autoridades interesadas y participa periódicamente en los grupos de trabajo internacionales para la mejora del sistema de intercambio de reclamaciones IMI y la homogenización de las multas.

Tras la investigación de estas reclamaciones, se ha procedido a iniciar cuatro expedientes sancionadores por los motivos siguientes: quiebra de seguridad, falta de legitimación para el tratamiento de datos, y política de privacidad que no cumple lo establecido en el artículo 13 del RGPD.

El resto de reclamaciones se han fundamentado en: falta de legitimación para el tratamiento de datos; recepción de correos electrónicos publicitarios sin consentimiento previo; no atención a los derechos de acceso y supresión; falta de medidas de seguridad; y directorios con datos personales cuyo origen se desconoce. La mayoría de estas reclamaciones se han archivado porque se ha atendido el derecho o porque no se han acreditado los hechos denunciados. En algún supuesto no ha sido posible identificar y encontrar a la entidad reclamada.

6.3 Planes sectoriales o de auditoría

La plena aplicación del RGPD y las novedades en los procedimientos han hecho necesario modificar la estructura interna de la Subdirección General de Inspección para implantar una organización que permitiera realizar un análisis en profundidad del nuevo modelo de cumplimiento basado en la responsabilidad proactiva centrado no solo en reclamaciones concretas si no también y, particularmente, en las políticas de privacidad y protocolos desarrollados por los responsables y encargados del tratamiento para cumplir con el principio antes mencionado. Por ello se ha creado un área especializada en estas investigaciones: el Área de Auditorías.

De su análisis resultará, dependiendo de si se encuentran indicios de vulneración de la normativa, bien una serie de recomendaciones o medidas orientadas a implantar buenas prácticas en estas organizaciones, o bien el criterio de que debe incoarse un procedimiento sancionador.

Por otro lado, el área de auditorías se ocupa de realizar investigaciones de amplio alcance sobre el cumplimiento de la normativa en sectores concretos de actividad y en ámbitos específicos de responsables o encargados de tratamientos. Son los Planes de Auditoría sobre determinados sectores, también conocidos como Planes de Investigación Sectorial de Oficio, que se contemplan en el art. 54 de la LOPDGDD. A resultas de esos planes, la Presidencia de la Agencia Española de Protección de Datos puede dictar las directrices generales o específicas para un concreto responsable o encargado de los tratamientos precisas para asegurar la plena adaptación del sector o responsable a la normativa.

Además, esta área tiene encomendada la investigación de las brechas de seguridad trasladadas por la UEET.

Las Operaciones Conjuntas previstas en el artículo 62 del RGPD han sido, también, con las autoridades de Irlanda y Luxemburgo también ha sido una de las labores del área de auditorías, que ha realizado cuatro y dos investigaciones, respectivamente con cada país.

También en un entorno internacional, el área colabora en otra investigación a una empresa del sector de logística y reparto con el Garante italiano como autoridad interesada, donde la Agencia es autoridad principal.

Esta área ejecuta las evaluaciones Schengen a los sistemas SIS II y VIS para los que la Agencia es autoridad de control de protección de datos y de su seguimiento en los grupos internacionales.
Finalmente, también tiene encomendada la participación en grupos de trabajo y proyectos internacionales de supervisión.

Plan de Inspección sectorial de oficio de contratación a distancia

La comercialización de productos por medios electrónicos ha experimentado en los últimos años un crecimiento exponencial, junto con la utilización de nuevas tecnologías en sectores de servicios fundamentales que ha permitido la realización de contrataciones utilizando la Red y sin presencia simultánea de los implicados en la contratación. Ello ha puesto de manifiesto la necesidad de acreditar el contrato efectuado y la identificación del contratante con objeto de evitar, en lo posible, la suplantación de identidad y las consecuencias negativas para los ciudadanos.

Con este objetivo, la Agencia incluyó en el Plan Estratégico 2015-2019 un Plan de Auditoria Preventiva para analizar los tratamientos de datos que se realizan, su adecuación al RGPD y a la LOPDGDD.

El Plan, compuesto de cinco fases, finalizó en el año 2019. Sus conclusiones y recomendaciones se harán públicas en 2020.

Plan de inspección sectorial de oficio del sector sociosanitario

Su objetivo principal ha sido analizar los tratamientos que se llevan a cabo en este ámbito e investigar su adecuación a la normativa de protección de datos.

Durante el año 2019 han culminado las actuaciones del Plan cuyas conclusiones y recomendaciones se harán públicas en 2020.

Evaluación Schengen de España. Plan SIS/VIS del acervo Schengen

Las actividades desarrolladas en 2019, siguiendo el Plan de Auditoría continuo de cuatro años en estrecha colaboración con los responsables del Sistema de Información Schengen (SIS II) y del Sistema de Información de Visados (VIS), han sido la realización de dos reuniones de seguimiento de la AEPD con la Oficina SIRENE, la Secretaría de Estado de Seguridad y el Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, para el establecimiento de un calendario de inspecciones

y la anotación de las mejoras introducidas en los Sistemas para su posterior validación en visitas presenciales.

Dentro del seguimiento del Sistema de Información Schengen (SIS II), se han realizado inspecciones presenciales a la Policía Vasca (Ertzaintza), a Vigilancia Aduanera y a la Dirección General de Tráfico completándose con los informes correspondientes a estas actuaciones presenciales incluyendo el Informe de la Policía Foral de Navarra, cuya inspección presencial finalizó a comienzos de 2019.

Por otra parte, se ha colaborado en la elaboración del cuestionario para el estudio de calidad de determinados señalamientos anotados en el SIS II que finalmente ha sido aprobado por el Grupo de coordinación de supervisores del SIS y ha sido incluido en la planificación 2019-2021. También se ha colaborado para la preparación de diversas contestaciones de la Agencia para el Supervisor Europeo.

Las actividades de supervisión sobre el sistema VIS, tras las ya ejecutadas en 2018, fueron la inspección al Consulado de España en La Habana (Cuba) y Bucarest (Rumanía). Tales actuaciones dieron lugar en 2019 a la realización de informes parciales sobre su adecuación. Las recomendaciones fueron puestas en conocimiento de los responsables, y continúa en curso el seguimiento de las actuaciones de adecuación.

7. Una estructura en permanente evolución

7.1 Avance en digitalización

Siguiendo la hoja de ruta de la digitalización de la Agencia, y conforme a las directrices de la Secretaría General de Administración Digital, se han impulsado relevantes actuaciones que han visto la luz en este año 2019.

Así, se ha dado el primer paso en la transformación de la oficina de registro general en una oficina de asistencia en materia de registro de las previstas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, cambiando, el procedimiento de recepción de escritos para devolver los originales al interesado, **eliminando así la entrada del papel** en la Agencia por completo, a excepción de los envíos postales.

En este año se ha conseguido automatizar un canal electrónico de **remisión de expedientes a la Audiencia Nacional por vía telemática**, conforme al Esquema Nacional de Interoperabilidad, y con entrada directa en el sistema de gestión de la Administración de Justicia.

Desde el lado del ciudadano, una de las principales demandas del sector de los profesionales de protección de datos era la mejora del acceso a la información publicada en la web. Este año se ha renovado toda la plataforma tecnológica de **la página web de la Agencia** www.aepd.es, ofreciendo un potente motor de búsqueda que eleva enormemente la calidad de los resultados, así como una nueva interfaz que ofrece la posibilidad de hacer filtros por tipos de contenidos en décimas de segundo.

Internamente, la Agencia también necesitaba reformar sus procesos de gestión y modernizar sus herramientas de trabajo. De esta manera, en 2019 se ha formalizado un proceso de gestión de incidencias y peticiones de servicio en el ámbito de las Tecnologías de la Información y de las Comunicaciones mediante una reorganización interna y un servicio que permite registrar la demanda, hacer seguimiento pormenorizado y sacar indicadores de rendimiento para su mejora continua. Esta iniciativa tiene vocación de ser extendida a otros ámbitos de la Secretaría General y procesos de gestión interna y también al servicio de Atención al ciudadano.

Finalmente, como herramienta transversal y fundamental para el día a día de los trabajadores de la Agencia, se ha creado una nueva intranet, basada en la última tecnología de espacios colaborativos, que moderniza el acceso a la información para el empleado, la compartición de documentos y facilita la gestión de trámites internos como las solicitudes de teletrabajo y la autorización de actividades externas con representación de la Agencia, que eran procesos manuales muy voluminosos y que implicaban un importante consumo de recursos.

7.2 Consolidación del programa de teletrabajo

El teletrabajo es ya la principal herramienta de conciliación de la vida familiar y laboral de la que dispone la AEPD, siendo la forma de trabajo -durante dos días de la semana- de todos los empleados públicos con funciones compatibles que han solicitado acogerse a ella.

Esta medida, prevista en el eje 5 del Plan Estratégico, «una Agencia más ágil y eficiente», juntamente con otras iniciativas orientadas a la optimización de los recursos, ha ayudado decididamente a la Agencia a adaptar su estructura y sistema de trabajo, para poder afrontar en las mejores condiciones los nuevos retos, y, en especial, la conocida reforma del marco normativo europeo ya plenamente en vigor.

Desde que en 2017 se puso en marcha el programa, con 17 plazas (10 %), se ha ampliado a las 87 plazas en 2019, lo que supone un 57 % de la plantilla activa.

Después de estos tres años de vida del programa, la Agencia cuenta con datos que permiten extraer conclusiones sobre su buen funcionamiento.

Las encuestas entre los interesados demuestran que esta capacidad de conciliación de la vida laboral, personal y familiar redunda inequívocamente en una mayor **satisfacción del trabajador** y, por ende, en otros beneficios para la Agencia que se mencionan a continuación.

a) Retención, fidelización y atracción del talento

Desde que el programa de teletrabajo se aprobó con carácter sistemático en el año 2018, la Agencia no ha sufrido apenas bajas de personal que se encontrase disfrutando del teletrabajo. Es más, en estos años de crecimiento sistemático importante de la RPT de la Agencia (en torno al 10 % anual), los responsables de seleccionar personal valoran el teletrabajo como el factor principal para atraer a nuevos trabajadores a la organización, por encima de las condiciones económicas del puesto. El teletrabajo es pues una oportunidad de retención, fidelización y atracción de talento, aspecto que se convierte en una ventaja competitiva para la Agencia en un contexto en que la AGE ha disminuido notablemente su plantilla y resulta difícil cubrir las vacantes.

b) Mejora de la productividad

La ejecución del Plan Estratégico sobre el objetivo establecido ha sido prácticamente igual en las últimas anualidades, estando muy cerca del 100%, incluso en un momento de cambio y necesidad de transformación interna ante la entrada en vigor del RGPD. El mismo resultado arrojan los principales indicadores de actividad como son la resolución de reclamaciones en materia de protección de datos, que se han incrementado en un 2% adicional, o la respuesta de un 20% más de consultas ciudadanas recibidas en el último año.

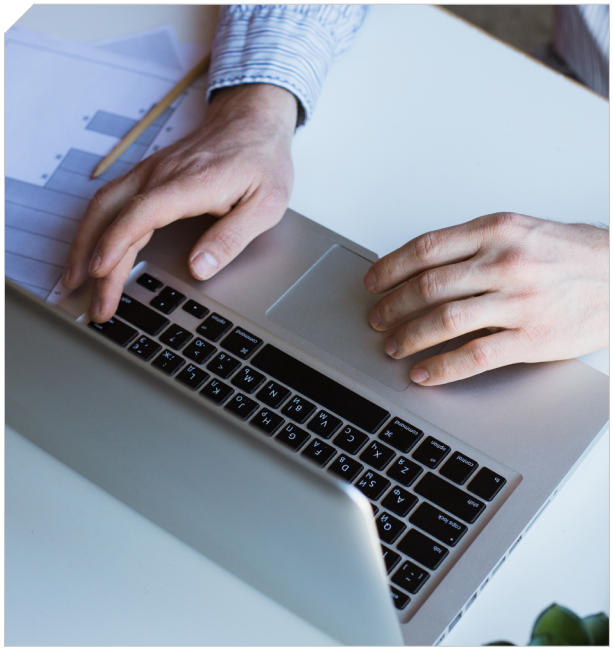
Los empleados públicos han sido capaces de absorber un considerable incremento de su trabajo (un tercio adicional) a la vez que han disminuido los tiempos medios de resolución. Creemos que, con una plantilla estable en volumen como mostraba anteriormente, este fenómeno no habría podido tener lugar sin una gran motivación del personal y un cambio en la organización del trabajo.

Bajando el foco al día a día de la actividad, gracias a las tecnologías de la información se ha podido comprobar empíricamente que la actividad durante los días donde se concentra el teletrabajo ofrece indicadores de participación y actividad de los trabajadores similares a aquellos días de mayor carácter presencial, lo que hace suponer que el trabajador cumple fielmente con los compromisos del teletrabajo.

Se puede decir que el sistema ha alcanzado un **grado elevado de confianza** entre los diferentes colectivos implicados.

El programa de teletrabajo desplegado en la Agencia ha despertado interés. Así, en este año, se ha presentado el programa de teletrabajo al Tribunal de Cuentas y al Instituto de la Mujer.

Los beneficios contrastados son tan contundentes, que el teletrabajo ha sido formalizado en el Plan de Responsabilidad Social, con el compromiso de mejorar el porcentaje de la plantilla en teletrabajo siempre que los resultados de evaluación sean positivos, como han sido hasta la fecha.



7.3 Adaptación de la RPT a las nuevas necesidades

Los esfuerzos en gestión de recursos humanos se han dirigido a dar cobertura a las necesidades de la principal actuación de la Agencia en este año 2019, el canal prioritario de retirada urgente de contenidos sensibles.

Como ya se señalaba en la memoria anterior, la Ley Orgánica de Protección de Datos y garantía de los derechos digitales 3/2018, publicada el 6 de diciembre, habilita a la Agencia para elaborar y aprobar su relación de puestos de trabajo, en el marco de los criterios establecidos por el Ministerio de Hacienda, respetando el límite de gasto de personal establecido en el presupuesto.

En este momento, se ha conseguido incrementar, desde 2018, la RPT en un 7,49% hasta los 201 puestos y habiendo conseguido mantener el nivel de ocupación tras dicho incremento en el 85 % de años anteriores.

Para ello, ha sido necesario incrementar el número de puestos de la RPT y realizar las convocatorias de méritos, concursos de libre designación y otras gestiones para su cobertura en el menor tiempo posible.

Se han realizado también actuaciones para la formación y especialización del personal, así como para su fidelización mediante principalmente la extensión del programa de teletrabajo como se desarrolla en el apartado anterior.

7.4 Ejecución presupuestaria

La gestión presupuestaria en el ejercicio 2019, con un presupuesto prorrogado de 2018, presenta un incremento de su crédito disponible en 959.000,23 euros, un 6,87% más sobre el crédito inicial, obtenido mediante la tramitación de distintas modificaciones presupuestarias de generaciones de crédito por ingresos. Ello ha posibilitado, por un lado, con el incremento del 7,99% del capítulo 1, la cobertura de la incorporación de 15 nuevos puestos a la RPT de la Agencia, y por otro, con el incremento del 2,54% en capítulo 2, hacer frente a las nuevas cuotas a abonar tras la firma de la renovación del contrato de arrendamiento de la finca sede de este ente.

En cuanto al nivel de ejecución, tanto el capítulo 2 de gastos corrientes como el capítulo 6 de gastos en inversión, han incrementado su ejecución en un 4,25% y un 6,05% más respectivamente respecto de 2018, siendo la ejecución total en 2019 del 87,98% del crédito definitivo para este año.

El presupuesto aprobado para la Agencia para 2019 se cubre mayoritariamente, como en años anteriores, con unas previsiones de ingresos por recargos, sanciones e intereses de demora de 9.127.610 euros y con remanente de tesorería por total de 5.051.270 euros. En cuanto a la ejecución de los ingresos, en 2019, los derechos reconocidos netos por recargos, sanciones e intereses de demora ha seguido siendo una de las principales fuentes de financiación de la Agencia, que han alcanzado los 5.370.619,40 euros.

Asimismo, en este ejercicio se ha finalizado la participación de la Agencia en los tres proyectos europeos en los que se participaba: Proyecto SMOOTH (97.500 euros para el desarrollo de herramientas de ayuda al cumplimiento del Reglamento General de Protección de Datos de las pymes y micropymes europeas), Proyecto PANELFIT (107.062 euros para uso ético de las Tecnologías de información y comunicación) y Proyecto T4D4-BASSO (58.196,17 euros para la formación de delegados de protección de datos en la Administración Local), que se ha citado anteriormente.

8. La necesaria cooperación institucional

8.1 Autoridades autonómicas

La relevancia de las novedades del Reglamento y de la LOPDGDD, especialmente a partir del momento de la aplicación efectiva de ambas normas, ha propiciado la celebración de reuniones de coordinación entre las autoridades de protección de datos.

Así, en marzo y noviembre de 2019 se celebraron reuniones del Grupo de Coordinación de Asesorías Jurídicas de las Agencias de Protección de Datos.

Por su parte, el Grupo de Coordinación de Inspección celebró por videoconferencia una reunión en el mes de mayo.

Las iniciativas de coordinación culminaron con la celebración el 27 de noviembre de 2019 de una reunión en Sevilla con participación de delegaciones de la Agencia Española de Protección de Datos, 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.

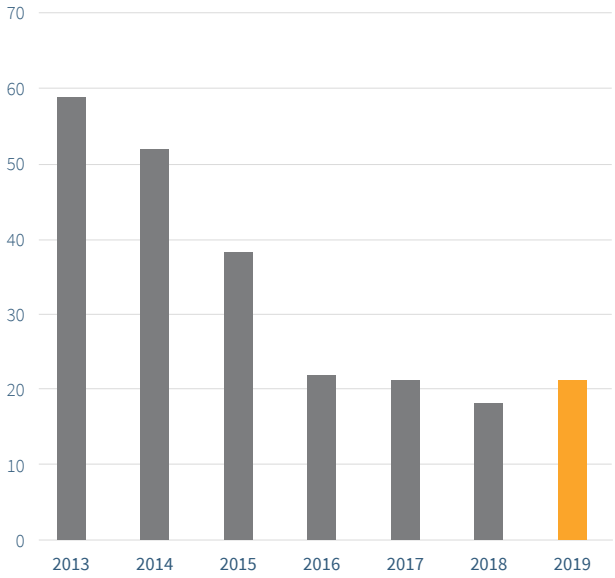
La reunión se inició con la felicitación al Director del Consejo de Transparencia y Protección de Datos de Andalucía por parte de las Directoras de las restantes autoridades por la asunción efectiva de las plenas competencias del Consejo en materia de protección de datos personales.

En ella se intercambiaron criterios sobre los diversos aspectos jurídicos, metodológicos y procedimentales recogidos en el orden del día, así como sobre las iniciativas para impulsar la coordinación entre las autoridades. La AEPD realizó una presentación de las Guías de privacidad desde el diseño y del paciente.

8.2 Relaciones con el Defensor del Pueblo

Asuntos o materias objeto de queja

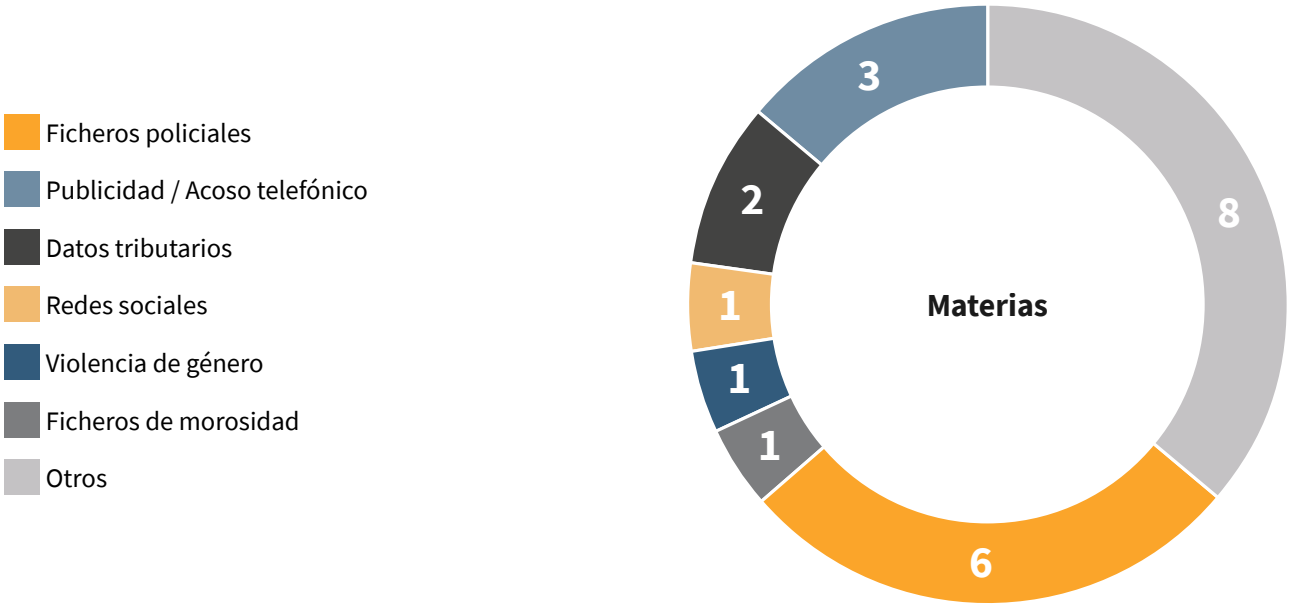
Se ha producido en 2019 un incremento de los casos planteados por el Defensor del Pueblo, concretamente seis, pasando de 17 en 2018 a 22 en 2019. Cinco de ellos corresponden a asuntos promovidos por Defensores del Pueblo autonómicos (Canarias, Cataluña, Galicia y Navarra).



Entre las principales materias o cuestiones que han sido objeto de la atención del Defensor del Pueblo están las quejas relativas al acceso a ficheros policiales (6), sobre tratamiento de datos en el ámbito de la publicidad (cookies, Lista Robinson, acoso telefónico, etc.) (3) y en el ámbito tributario (2). Otras cuestiones que han sido objeto de queja han sido las referidas a comentarios en redes sociales, la inclusión indebida en ficheros de morosos o no contemplar la Tesorería General de la Seguridad Social la circunstancia de violencia de género en los informes de vida laboral, con un asunto cada una de ellas.

De entre todas ellas, hay que destacar el escrito del Defensor del Pueblo solicitando información a esta Agencia en relación con el estado de la tramitación e instrucción de los cuatro expedientes abiertos por los servicios de inspección de la AEPD en relación con el llamado "caso de La Manada". En respuesta a esa petición, se informó al Defensor del Pueblo sobre la tramitación de cuatro expedientes (Acuerdos de inicio), dos de los cuales, incoados a miembros de ese colectivo, que fueron objeto de suspensión en tanto el asunto se está sustanciando en la vía judicial. Los otros dos procedimientos abiertos al diario 'La Tribuna de Cartagena', uno por publicar imágenes y otro por no atender los requerimientos de la Agencia, han sido resueltos por la Agencia con una sanción de 50.000 euros y con un archivo, respectivamente.

Otro asunto de interés ha sido la queja presentada por el Defensor del Pueblo de Navarra y diversas asociaciones en materia de extranjería en relación con una actuación del Ayuntamiento de Ribaforada (Navarra), en la que agentes de la Brigada de Extranjería solicitaron verbalmente al consistorio colaboración para investigar y esclarecer los delitos en los que posiblemente estaba implicado el interesado, un ciudadano senegalés, para proceder a su expulsión del territorio nacional cuando acudió a dependencias municipales tras ser citado por el mencionado ayuntamiento para realizar gestiones relacionadas con su empadronamiento.



Motivos de queja

Respecto a los principales motivos que han llevado a los ciudadanos a dirigirse a la AEPD mediante este cauce, prácticamente la mitad de ellos lo han sido para solicitar información sobre el estado de tramitación de su denuncia o recurso ante la falta de respuesta de la Agencia (10). Mediante los restantes escritos del Defensor del Pueblo se solicita a la AEPD que inicie actuaciones sobre los hechos objeto de queja; que profundice en su estudio, o bien que fije criterio en relación con algunos de los asuntos planteados. En tres de ellos solicita información sobre las medidas correctoras adoptadas en otras tantas resoluciones sancionadoras a organismos públicos.

9. Una autoridad activa en el panorama internacional

9.1 Unión Europea

El Comité Europeo de Protección de Datos (CEPD) se configura como un organismo de la Unión, con personalidad jurídica propia, y con funciones que incluyen la de adoptar decisiones jurídicamente vinculantes para las autoridades de supervisión a fin de resolver los conflictos que puedan surgir entre ellas en determinadas actuaciones de aplicación del RGPD.

Son miembros del Comité los directores o presidentes de las autoridades de supervisión en materia de protección de datos de los Estados Miembro. Cuando en un Estado exista más de una autoridad, será designada una de ellas como representante común de las demás ante el Comité. En el caso español, es la Agencia Española de Protección de Datos la que asume esa representación común a las demás autoridades del Estado.

El Supervisor Europeo de Protección de Datos es también miembro del Comité, como lo son las autoridades de supervisión de los estados del Espacio Económico Europeo, aunque estas últimas, pese a su condición de miembros de pleno derecho, no tienen derecho a voto. La Comisión participa en las reuniones del Comité y debe ser informada de su actividad.

La naturaleza de organismo de la Unión con personalidad jurídica propia del CEPD tiene importantes consecuencias, entre las que pueden destacarse que está plenamente sometido a la normativa europea aplicable al funcionamiento de instituciones, agencias y organismos de la Unión, o el que sus decisiones vinculantes pueden ser objeto de recurso ante el Tribunal de Justicia de la Unión Europea.

Como se ha indicado ya en otra sección de esta Memoria, el Comité puede adoptar recomendaciones, directrices o buenas prácticas, así como dictámenes que vinculan material, aunque no formalmente, a sus miembros, y decisiones jurídicamente vinculantes.

El denominador común de todas estas funciones, tengan o no como resultado textos de carácter vinculante, es que persiguen dotar al Comité de los instrumentos para conseguir que actúe como el máximo órgano de coordinación y cooperación entre las autoridades de supervisión de la Unión a fin de garantizar conseguir una aplicación uniforme y coherente de la normativa de protección de datos.

Durante 2019, el Comité ha continuado en la consolidación de ese nuevo papel como organismo de la Unión, tanto en términos materiales como en funcionales.

El Comité ha seguido desarrollando su sistema interno de comunicación, pieza clave no solo para el funcionamiento del propio Comité sino también para la aplicación del mecanismo de cooperación ("ventanilla única") entre autoridades.

Como se ha expuesto en anteriores Memorias, el sistema de información del Comité es una adaptación del Sistema de Información del Mercado Interior (IMI) configurada para atender a las necesidades del Comité y de sus autoridades.

El Sistema de Información del Comité ha seguido revisándose y refinando su funcionamiento durante 2019. Se han incorporado nuevas herramientas informáticas para la coordinación de los trabajos de los Subgrupos de Expertos y una aplicación de videoconferencia que permite mantener reuniones virtuales. Asimismo, se han incluido nuevos procesos para responder mejor a las necesidades de las autoridades de supervisión.

El Comité ha aumentado la dotación de personal de su Secretariado y también ha mejorado la dotación de locales para celebración de reuniones,

estando previsto que en 2020 esté operativa una nueva sala de reuniones que permitirá albergar las sesiones plenarias del Comité.

La Agencia Española de Protección de Datos ha sido consciente de la importancia del papel que el CEPD está desempeñando. Por ello se ha involucrado de forma muy activa en su funcionamiento desde sus primeros pasos.

Dentro ya del marco de funcionamiento del Comité, es preciso hacer mención del que es el elemento central en la organización de sus trabajos: los subgrupos de expertos.

Estos subgrupos están integrados por representantes de las autoridades de supervisión y su principal misión es la de preparar las decisiones del Comité. Dicho en términos muy esquemáticos, prácticamente ningún documento o decisión es adoptado por el Comité sin que antes haya mediado el estudio y preparación de propuestas por parte de un subgrupo.

En 2019 se cerró la actual estructura de subgrupos, estableciéndose un total de 13 subgrupos de expertos, aunque algunos de ellos tienen un ámbito material de actuación muy restringido, como sucede con el "Subgrupo Multas", cuya tarea es la identificar criterios comunes para la fijación de sanciones económicas en los Estados Miembro, o el "Subgrupo de Usuarios IT", dedicado fundamentalmente a velar por el correcto funcionamiento y evolución del Sistema de Información del CEPD.

La AEPD participa en todos los subgrupos de expertos y es coordinadora de dos de esos subgrupos.

El primero de ellos es el denominado Subgrupo de Supervisión del Cumplimiento (enforcement), en el que actúa como co-coordinador junto con la autoridad holandesa. Este subgrupo tiene como misión la de actuar como foro de intercambio de información, coordinación y preparación de decisiones en materia de actuaciones llevadas a cabo por las autoridades nacionales en el ámbito de la inspección y sanción de infracciones.

Como ejemplo del modo en que se concreta esa misión, durante el año 2019 el subgrupo ha realizado, entre otras, las siguientes actuaciones: desarrollar una estrategia de enforcement para el CEPD; preparar un manual de comunicación en materia de inspección y sanción de infracciones; analizar los problemas asociados con la inspección y sanción de responsables no establecidos en la Unión Europea pero a los que se aplica el RGPD, identificando posibles soluciones; y establecer "grupos de contacto" para el seguimiento de procedimientos desarrollados en varios Estados Miembro en relación con una misma organización o con un mismo tipo de infracción al RGPD.

El segundo subgrupo de expertos en el que la AEPD actúa como coordinador es el denominado "Cumplimiento, Salud y Gobierno Electrónico". Este subgrupo, cuyo ámbito material es, sin duda, heterogéneo, es el resultante de integrar en un solo foro, que originariamente se dedicaba tan solo a cuestiones de gobierno electrónico, materias de relevancia para el Comité pero que no encontraban acomodo en otros subgrupos.

El trabajo de este subgrupo del año 2019 ha incluido, entre otras cuestiones, finalizar la adopción de unas directrices del Comité sobre códigos de conducta en el marco del RGPD; preparar la respuesta a varias consultas formuladas por la Comisión al CEPD en materias como ensayos clínicos o la relación entre el Reglamento de libre circulación de datos no personales en la UE y el RGPD; preparar los dictámenes del CEPD en relación con las cláusulas estándar de encargo de tratamiento que deseen adoptar las autoridades nacionales de supervisión y preparar un los dictámenes del Comité sobre las propuestas de criterios de acreditación de los organismos de supervisión de códigos de conducta y de acreditación de entidades de certificación propuestos por las autoridades nacionales.

El papel del coordinador es clave para el funcionamiento del subgrupo y para sus resultados. El coordinador preside las reuniones de los subgrupos, actúa como punto de contacto de los miembros del subgrupo, prepara el orden del día de las reuniones, distribuye los documentos, vela por que el desarrollo de las reuniones se adecúe a lo establecido en las Reglas

de Procedimiento y reporta al Plenario del Comité sobre la actividad del subgrupo.

Parte importante de su papel consiste, también, en que los coordinadores de todos los subgrupos forman parte, a su vez, de otro subgrupo, el de "Coordinadores", una de cuyas principales tareas es la de establecer los programas de trabajo de los diferentes subgrupos para cada año.

La AEPD participa también en el subgrupo de redacción de las Reglas de Procedimiento (RdP) del Comité. Este subgrupo, como su nombre ya denota, se encargó de preparar las RdP que fueron aprobadas en su primera reunión, en mayo de 2018.

Sin embargo, el subgrupo no se disolvió al finalizar su tarea, sino que se ha mantenido para atender a los necesarios ajustes que se están llevando a cabo en las RdP como consecuencia de la experiencia adquirida en el funcionamiento práctico del Comité. El subgrupo ha preparado durante 2019 varias modificaciones de las RdP, entre ellas las relativas a los criterios de admisión de observadores o las que se han introducido en el procedimiento de tramitación de los dictámenes del artículo 64 RGPD.

9.2 Supervisión de los Sistemas IT de Cooperación Policial y Judicial del Espacio de Libertad, Seguridad y Justicia– nuevo Comité de Supervisión Coordinada.

Las modificaciones en el marco normativo de la protección de datos en la Unión Europea han afectado también a otro ámbito material que, aunque relacionado con la actividad de la Unión, se había abordado hasta fechas recientes desde la perspectiva de la cooperación entre los Estados Miembro. Se trata de la supervisión de la aplicación de la normativa de protección de datos en materia de cooperación policial y judicial penal en del denominado Espacio de Libertad, Seguridad y Justicia que es la Unión Europea.

En la Unión Europea se han desarrollado históricamente agencias o grandes sistemas de información orientados a promover y facilitar la cooperación entre los Estados Miembro en materia policial y judicial. Entre las agencias puede mencionarse Europol o Eurojust y entre los grandes sistemas el Sistema de Información Schengen o el Sistema VIS. En el marco del control de la Inmigración en el área Schengen se estableció un sistema IT específico para la aplicación del Convenio de Dublín y un Órgano de Supervisión también específico, el Grupo de Coordinación de la Supervisión de Eurodac.

Esas agencias o grandes sistemas integran intercambios de datos personales entre las autoridades nacionales participantes, usando una infraestructura europea, o de esas autoridades entre sí y con una instancia central europea, que es el caso de las agencias europeas.

La supervisión de esos intercambios desde la perspectiva de la protección de datos se ha realizado a partir de un modelo tradicional, el de las "autoridades conjuntas de control", que ha ido evolucionando paulatinamente a la figura de los "grupos de supervisión coordinada". Estos grupos, que son los que actualmente están implantados en la mayoría de agencias o grandes sistemas de información, se basan en una supervisión coordinada sobre los diferentes niveles de utilización de los datos. En el marco de sus competencias específicas, las autoridades nacionales se ocupan de los tratamientos a nivel nacional, mientras que el Supervisor Europeo de Protección de Datos hace un seguimiento de la actividad del sistema de información como tal o de la agencia europea afectada. Los grupos de coordinación sirven para asegurar la cooperación y la coherencia de la supervisión en esos diferentes niveles.

En 2018 se aprobó el Reglamento UE/2018/1725, que es el que regula la protección de datos en el ámbito de las instituciones, agencias y organismos de la Unión, reemplazando al anterior Reglamento UE/45/2001.

En este nuevo Reglamento se reitera el modelo de "grupos de coordinación", en la medida que se prevé que el Supervisor y las autoridades

nacionales ejercerán las labores de supervisión actuando cada uno en el marco de sus respectivas responsabilidades y competencias, debiendo intercambiar información y cooperar entre sí.

La diferencia, no obstante, estriba en que el Reglamento se aleja de la pluralidad de instancias de coordinación existentes para establecer que esa cooperación y coordinación deberá realizarse en el marco del Comité Europeo de Protección de Datos, donde el Supervisor y las autoridades nacionales deberán reunirse, al menos, dos veces al año.

Tras la aprobación del Reglamento UE/2018/1725, el Comité ha iniciado los trabajos para desarrollar las estructuras y métodos de trabajo adecuados para dar cabida a esta nueva función. Por el momento, la principal dificultad de esta tarea radica en la ya citada diversidad de tareas y funciones asumidos por las anteriores instancias de coordinación, que derivan de las previsiones que contienen las normas que regulan cada agencia o gran sistema de información. En tanto no se modifiquen esas normas, el Comité deberá respetar esa diversidad de funciones.

El primer paso para la evolución y desarrollo del nuevo sistema de supervisión ha tenido lugar en Eurojust, donde el pasado diciembre de 2019 se produjo del traspaso de poderes de la supervisión del sistema por parte del Grupo de Supervisión Conjunta de Eurojust al Supervisor Europeo de Protección de Datos.

En el pasado mes de diciembre, fueron aprobadas las normas de procedimiento del nuevo Comité de Supervisión que habrá de sustituir a los diferentes grupos de supervisión de la coordinación de los sistemas IT del SIS de visados, del SIS II (Sistema Schengen II) y JIS y CIS de Aduanas (Sistemas de Información Conjunta y Sistema de Información de Aduanas) y del extinto Órgano de Supervisión Conjunta de Eurojust y del Comité de Supervisión de Europol. Asimismo, el Comité se ocupa de la supervisión del Sistema de Información del Mercado Interior (IMI).

Queda por definir el modelo de participación del Comité en la futura supervisión conjunta de los sistemas, lo que probablemente suponga la reforma de los actuales Reglamentos sectoriales que gobiernan cada uno de los sistemas de información de cooperación policial y judicial por el Colegislador Europeo.

Por otra parte, se encuentra en desarrollo en este momento el nuevo modelo de interoperabilidad de los sistemas que supone la implantación del nuevo Portal de Búsquedas Europeo. Este conjunto de instrumentos informáticos integrados en una nueva plataforma de tres capas integra un identificador de identidades múltiples, un sistema de emparejamiento biométrico y un repositorio común de identidades. Este sistema que incorpora datos biométricos alfanúmericos permitirá la detección e identificación de las personas que se presentan varias identidades bajo unos mismos datos biométricos, por ejemplo, huellas dactilares.

Además, se encuentra en desarrollo el Sistema de Entrada Salida Europeo (EES) y el sistema ETIAS para los viajeros exentos de visado con destino a la UE, que se prevé sean integrados también en el nuevo sistema de interoperabilidad.

Se pretende que el conjunto del sistema permite encontrar el equilibrio entre el derecho a la intimidad de las personas y la protección de sus datos personales y el aseguramiento de la vida e integridad de los ciudadanos y la prevención de delitos como el terrorismo.

9.3 Participación de la AEPD en otros foros internacionales

9.3.1 Convenio 108+ del Consejo de Europa

El Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal fue el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos. Tiene como fin garantizar a cualquier persona física «el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con

respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona». Con el Protocolo que ha modificado el Convenio, conocido como 108 +, se pretende ampliar su ámbito de aplicación, aumentar el nivel de protección de los datos y mejorar su eficacia. En su honor, desde 2006 se celebra en dicha fecha el día de la Protección de Datos Personales.

La AEPD asiste a las reuniones del Comité Consultivo de la Convención 108+, formando parte del tanto del Comité Consultivo como de su Mesa, y este mismo año la Secretaría de la Convención 108+ del Consejo solicitó de la delegación española su participación como miembro del Mecanismo de Seguimiento de la Convención 108+, ofrecimiento que ha sido aceptado por la Agencia española.

9.3.2 Conferencia OCTOPUS, convención de Budapest

La AEPD participó en la Conferencia OCTOPUS del Consejo de Europa sobre la lucha contra la cibercriminalidad.

La Delegación Española presentó las posiciones de la AEPD en el marco de la Conferencia. A solicitud del EDPS y en su condición de miembro permanente del Comité Europeo de Protección de Datos la Delegación sostuvo y apoya también la posición del propio CEPD.

También se comentó el canal prioritario para comunicar la difusión de contenido sensible en internet y solicitar su retirada que recientemente ha puesto en marcha la AEPD, en el marco del taller “explotación y abuso sexual en línea”.

9.3.3 41ª Conferencia Internacional de Protección de Datos y Privacidad

Del 21 al 24 de octubre se celebró en la capital de Albania, Tirana, la 41ª Conferencia Internacional de Comisionados de Protección de Datos y Privacidad (ICDPPC).

La Conferencia reunió a más de 120 autoridades independientes de más de 80 países, donde bajo el lema “Convergencia y Conectividad”, acordó continuar con el fortalecimiento de la Conferencia como un foro internacional efectivo, ensanchando la cooperación en cuanto a la observancia de la ley.

Las autoridades de protección de datos reunidas destacaron la importancia de trabajar hacia un entorno regulatorio global, así como fortalecer las relaciones con otros organismos y redes internacionales. Para ello, se hace preciso avanzar en el intercambio de información y en los instrumentos que permitan dichos intercambios como los memorandos de entendimiento.

La Conferencia aprobó un cambio en su denominación al objeto de simplificarla, pasando a denominarse Asamblea Global de Privacidad, o GPA por sus siglas en inglés. También se aprobó que la autoridad del Reino Unido (ICO) continuará ostentando la presidencia de la Conferencia durante los próximos dos años.

Desde hace tres años, la Conferencia otorga varios premios a proyectos o actuaciones desarrollados por sus miembros en el tiempo transcurrido entre dos conferencias. En 2019, la AEPD obtuvo dos de los galardones. Uno, en la categoría, de accountability, destinada a reconocer directrices o herramientas orientadas a facilitar el cumplimiento por parte de responsables y encargados. El premio, que se decide por los votos de los miembros de la conferencia entre los proyectos seleccionados de entre todos los candidatos por el Comité Ejecutivo de la Conferencia, fue concedido a la herramienta Facilita, como se ha señalado anteriormente.

Facilita_RGPD obtuvo también el premio por votación popular, que se otorga al proyecto más votado por los miembros de entre todos los que son seleccionados para las cuatro categorías en que se concede premio.

9.3.4 Grupo de Berlín

En octubre se celebró en Bruselas la 66ª reunión del Grupo de Protección de Datos en Telecomunicaciones, o también denominado Grupo de Berlín. La AEPD participa activamente en este grupo y en la redacción de los documentos de trabajo.

Este año, el Grupo de Berlín ha aprobado dos documentos de trabajo relativos al tratamiento de datos de menores, uno sobre los servicios en línea y otro sobre dispositivos inteligentes.

Los menores pasan una cantidad significativa de tiempo usando servicios en línea, aplicaciones y dispositivos inteligentes, siendo particularmente vulnerables con respecto a la protección de sus datos, ya que los menores carecen de conciencia sobre los riesgos asociados con la recogida y el tratamiento de sus datos personales. Por ello, los productos y servicios ofrecidos a menores deben cumplir con elevados estándares en cuanto a transparencia, validez del consentimiento, así como con respecto a la protección de datos desde el diseño y por defecto.

En el documento de trabajo sobre la protección de la privacidad de los menores en los servicios en línea se destacan los riesgos y desafíos asociados con los servicios en línea utilizados por los menores. Desde el documento, se hace un llamamiento a los proveedores de servicios a fin de garantizar la transparencia y obtener el consentimiento válido de los padres para el tratamiento de los datos de los menores. También se proporcionan recomendaciones para los encargados del tratamiento, los desarrolladores de servicios en línea y los reguladores, a la hora de establecer políticas de protección de datos para los servicios en línea destinados a menores.

En el documento de trabajo sobre riesgos para la privacidad en los dispositivos inteligentes destinados a menores se analizan, en particular, los problemas asociados con los juguetes inteligentes: falta de transparencia, fallos de seguridad, tratamientos de datos contrarios a la ley y posible abuso en el uso de juguetes inteligentes por parte de adultos con fines de vigilancia. El documento de trabajo proporciona recomendaciones para hacer frente a estos problemas y dirigidas a todas las partes interesadas: fabricantes, usuarios, escuelas y autoridades.

10. La cooperación con Iberoamérica

Especial referencia a la Red Iberoamericana de Protección de Datos (RIPD)

Las principales actividades desarrolladas por la AEPD en relación con Iberoamérica, especialmente a través de la Red Iberoamericana de Protección de Datos (RIPD), en su condición de Secretaría Permanente, han sido las siguientes:

Participación de la AEPD en eventos de la RIPD

- 15 a 17 de mayo. I Foro de Autoridades Iberoamericanas de Protección de Datos. Cartagena de Indias (Colombia)

Se constituyó por primera vez el Foro de Autoridades Iberoamericanas de Protección de Datos, integrado exclusivamente por las entidades de la RIPD que tienen el estatuto de Miembros (Autoridades), para abordar cuestiones que, como Autoridades, les conciernen más directamente, en especial aquellas orientadas a la cooperación efectiva (enforcement) en su gestión ordinaria.

En concreto, participaron en el Foro representantes de la Agencia de Acceso a la Información Pública de Argentina (AAIP), la Agencia de Protección de Datos de los Habitantes de Costa Rica (PRODHAB), la Agencia Española de Protección de Datos (AEPD), la Autoridad Nacional de Protección de Datos Personales de Perú (APDP), el Consejo para la Transparencia de Chile (CpT), el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales de México (INAI), el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal (INFODF), el Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios (INFOEM), la Superintendencia Delegada de Protección de Datos Personales de Colombia (SIC) y la Unidad Reguladora y de Control de Datos Personales de Uruguay (URCDP/AGESIC).

En dicho foro se abordaron cuestiones como las estrategias de cooperación de las Autoridades de Control en relación con los prestadores de servicios de internet; la aprobación de la Guía sobre tratamiento de datos e inteligencia artificial (IA); la eventual fijación de criterios u orientaciones sobre la computación en la nube (cloud computing) en Iberoamérica; los instrumentos de cooperación en los flujos internacionales de datos entre Europa e Iberoamérica; la convergencia entre la RIPD y la OEA, y la propia definición del papel del Foro como herramienta de cooperación efectiva entre las Autoridades.

Por parte de la AEPD, asistieron el Subdirector General de Inspección de Datos y el Abogado del Estado-Jefe del Gabinete Jurídico, quienes participaron activamente en sendas ponencias sobre los citados asuntos.

- 19-21 junio. XVII Encuentro Iberoamericano de Protección de Datos. Naucalpan (México)

Los dos primeros días tuvo lugar la Sesión Abierta del Encuentro, en la que se incluyeron ocho paneles con diferentes temas de actualidad en el ámbito internacional de la protección de datos, tanto desde el punto de vista normativo, tecnológico, judicial, etc. El evento, organizado por el Instituto de Transparencia y Protección de Datos del Estado de México (INFOEM) contó con una asistencia masiva durante todas las sesiones con más de 300 participantes.

El día 21 de junio tuvo lugar la Sesión Cerrada del Encuentro, en el que participan únicamente los Miembros y los Observadores de la RIPD, en la que se abordaron diversos asuntos de gran interés para la RIPD, como la aprobación de unas recomendaciones generales y unas orientaciones específicas sobre protección de datos e inteligencia artificial; el estado de situación de los trabajos entre la RIPD y el Comité Jurídico Interamericano de la OEA; el examen del estado actual de los nuevos desarrollos legislativos en la materia (Chile, El Salvador, Brasil….); información sobre el estado actual y principales novedades

del Convenio 108+; el papel de la RIPD en las Conferencias Internacionales de Autoridades de Privacidad; información sobre la iniciativa de Educación digital y menores postulada por algunas Autoridades iberoamericanas de protección de datos en el marco del programa europeo EUROsociAL+; el estado de situación actual de las Autoridades iberoamericanas de protección de datos en relación con su autonomía y estabilidad, que dio lugar a la aprobación de una declaración final específica sobre esta cuestión; información sobre la reforma de la Web de la RIPD y las nuevas altas. En concreto, se acreditaron como nuevos Observadores el Comité Consultivo del Convenio 108 (Consejo de Europa); la Agencia Nacional de Protección de Datos Personales de Santo Tomé y Príncipe; el Instituto de Acceso a la Información Pública del Estado de Chiapas; el Instituto Veracruzano de Acceso a la Información y Protección de Datos Personales y la Comisión de Transparencia y Acceso a la Información del Estado de Nuevo León. Se acordó designar al INAI como organizador del XVIII Encuentro, en el marco del programa de actividades de la Conferencia Internacional de Autoridades de Privacidad que tendrá lugar en octubre de 2020, en Ciudad de México, para lo que se establecerá la debida coordinación entre el INAI y la RIPD.

Por parte de la AEPD, asistieron al XVII Encuentro la Directora, el Coordinador de la Unidad de Apoyo y Relaciones Institucionales y el Vocal Asesor de la Unidad de Apoyo encargado de la Secretaría Permanente de la RIPD.

- 13-15 noviembre. Seminario "A un año de la aplicación del Reglamento General de Protección de Datos". Montevideo (Uruguay).

El Seminario pretendía hacer balance de la ejecución del nuevo Reglamento General de Protección de Datos por parte de los países que cuentan con normativa propia en protección de datos, basada en el "modelo europeo", una vez transcurrido casi un año y medio de su entrada en vigor efectiva, el 25 de mayo de 2018. Especialmente, se examinaron los procesos de adaptación legislativa emprendida por los países afectados, tanto en lo que se refiere a la revisión de sus procesos de adecuación a la normativa europea (caso de Argentina y Uruguay), como en la reforma de sus respectivas legislaciones, o nuevas leyes, en los restantes casos (Chile, Colombia, Costa Rica, España, México, Perú y Portugal).

El evento estuvo centrado en el debate sobre las principales cuestiones que, en relación con la aplicación del Reglamento General de Protección de Datos, se les han ido suscitando a las Autoridades de Protección de Datos en su gestión ordinaria, pero también a otros actores procedentes tanto del sector público, como empresarial y profesional, poniendo en común los problemas planteados y las posibles soluciones acordadas entre todos.

Como novedad, respecto a otros seminarios anteriores, se incorporaron por primera vez paneles específicos de las organizaciones sociales que integran el Foro de la Sociedad Civil de la RIPD; de las empresas, con la participación de las principales empresas tecnológicas (Facebook, Google, Amazon y Microsoft), y de los profesionales de la privacidad, a través de las organizaciones de ámbito iberoamericano (IAPP, ALP, AIPYC). Se pretendía que todos estas asociaciones, organizaciones y empresas aportaran su propia visión, desde cada uno de sus ámbitos respectivos, sobre cómo ven la aplicación del nuevo marco europeo de protección de datos en la región.

Los asistentes y ponentes son representantes de alto nivel de las instituciones que integran la RIPD, así como del resto de los organismos públicos invitados al mismo. Asimismo, participaron en el evento expertos y especialistas en la materia procedentes del ámbito académico, empresarial y profesional. Igualmente, representantes de organizaciones internacionales, como la Organización de Estados Americanos y la Unión Europea, y de la Federal Trade Commission de Estados Unidos.

Por parte de la AEPD, asistieron la Directora y el Coordinador de la Unidad de Apoyo y de Relaciones Institucionales, quienes participaron en sendas ponencias relativas, respectivamente, a la estrategia de las Autoridades de control ante el nuevo escenario: la eficacia extraterritorial de la legislación de protección de datos y la cooperación en relación con la investigación,

inspección y sanción de los grandes prestadores de internet, y a las bases de legitimación para el tratamiento de los datos personales.

Visitas a la AEPD de delegaciones iberoamericanas

- 28 de enero. Visita a la AEPD de una delegación de parlamentarios chilenos

Participaron en dicha reunión cuatro parlamentarios de la Cámara de Diputados de Chile, en que se trataron, entre otros asuntos, la aplicación del derecho al olvido, el impacto del Reglamento europeo en las empresas y el estado de situación del proyecto de ley de protección de datos personales.

- 10 de junio. Visita a la AEPD del senador Felipe Harboe, presidente de la Comisión Constitucional del Senado Chileno

En la reunión se abordó especialmente el estado de tramitación del proyecto de ley de protección de datos de Chile, que está siendo objeto de debate en la Comisión de Asuntos Constitucionales del Senado chileno, que preside el senador Harboe.

- 26 septiembre. Visita a la AEPD de la Comisionada Presidenta del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco (México)

En dicha reunión se abordaron con el ITEI asuntos de interés común en su condición de Observadores de la Red Iberoamericana de Protección de Datos y, en especial, la iniciativa que están desarrollando en el Estado de Jalisco, en coordinación con la autoridad educativa, para implantar un proyecto de educación digital para los alumnos de educación básica.

- 14 de noviembre. Visita de asesor en Ciberseguridad de la Presidencia de la República de Chile.

En esta reunión con el asesor presidencial en Ciberseguridad, Mario Farren Risopatrón, estuvieron presentes el Coordinador de la Unidad de Evaluación y Estudios Tecnológicos de la AEPD y el Director de Operaciones del INCIBE, abordándose diversos temas relacionados con las competencias en materia de seguridad y privacidad en España.

- 22 de noviembre. Visita a la AEPD de consejero del Consejo para la Transparencia de Chile.

En la reunión con el Consejero Francisco Leturía se abordó el estado de situación del proyecto de ley de protección de datos y la eventual asunción de competencias en materia de protección de datos por parte del Consejo para la Transparencia, una vez que se apruebe finalmente la ley en tramitación, ofreciendo la AEPD toda su colaboración en la aplicación de la ley, especialmente en lo que se refiere a la capacitación de los empleados del Consejo que se vayan a hacer cargo de esta materia.

Comité Ejecutivo de la RIPD

Se celebraron dos reuniones virtuales del Comité Ejecutivo de la RIPD los días 9 de abril y 11 de junio, y una reunión presencial el 19 de junio con ocasión del XVII Encuentro Iberoamericano de Protección de Datos, en Naucalpan (México).

Otras actuaciones de la AEPD en relación con Iberoamérica

- 12 a 14 de marzo. Asistencia técnica de apoyo a la reunión de la Comisión de Seguimiento del Convenio de Buenos Aires (AMERIPOL). Quito (Ecuador)

En el marco de la colaboración con la FIIAPP, la Agencia participó en la I reunión de la Comisión de Seguimiento del Convenio de Buenos Aires, sobre intercambio de datos policiales entre los cuerpos policiales de América Latina (en siglas, AMERIPOL), asesorando en la redacción del citado convenio internacional en la parte relativa a la protección de los datos personales (Anexo sobre clausulado de privacidad).

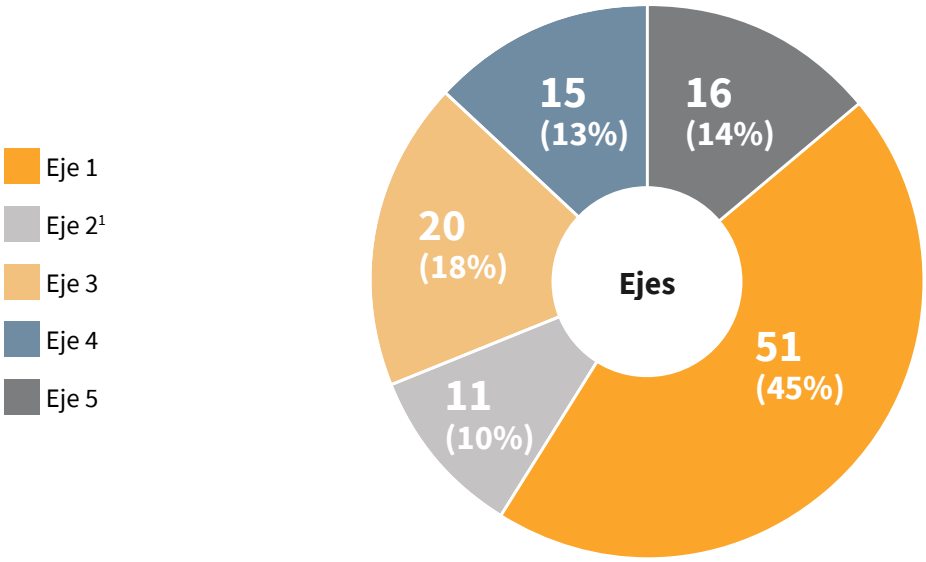
ANEXO

LA AGENCIA EN CIFRAS

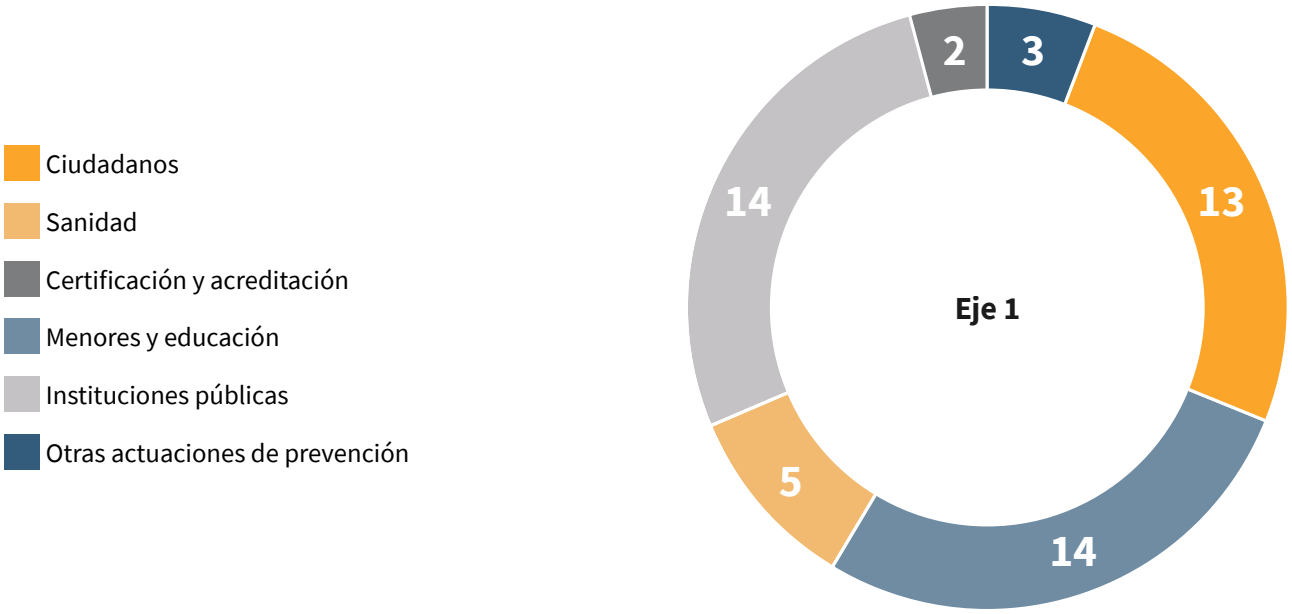
agencia española protección datos

1. Plan estratégico

Distribución inicial de las 113 acciones del Plan estratégico



Distribución inicial de las acciones del Plan estratégico por programas



[1] El Eje 2 no tiene programas.

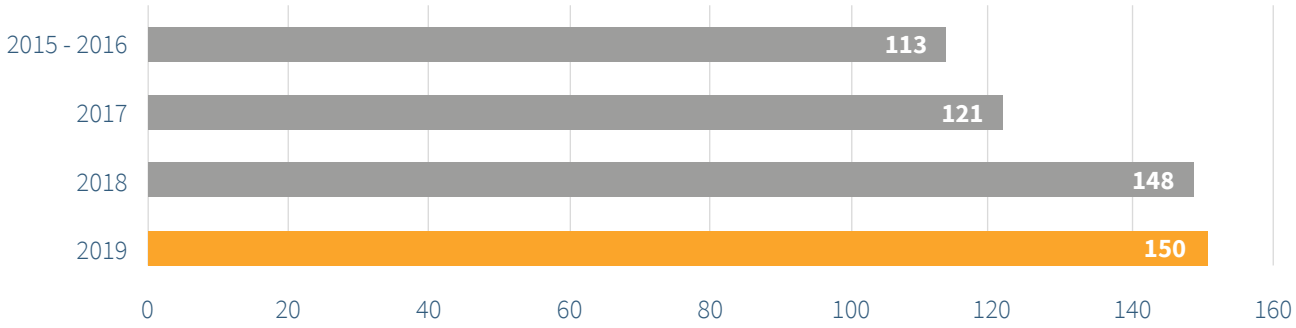
Distribución inicial de las acciones del Plan estratégico por programas

- Herramientas de comunicación
- Cultura de protección de datos
- Divulgación
- Página web

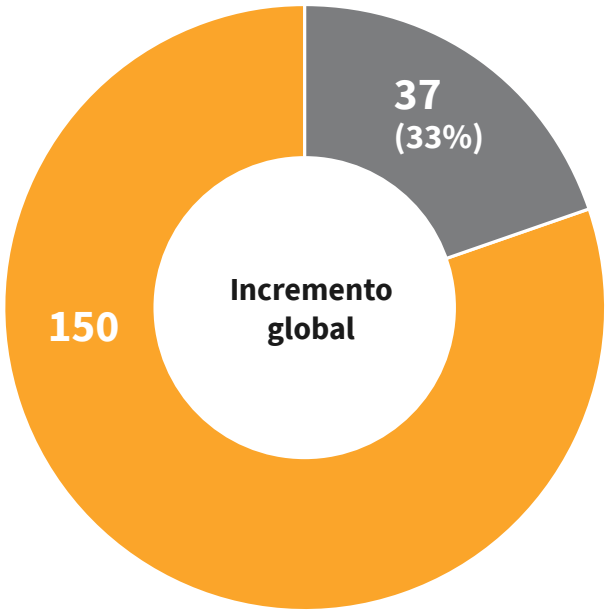
- Relaciones con los responsables
- PYME
- Profesionales y DPD

- AEPD Digital
- Retos interncionales
- Simplificación y mejora de la gestión

Evolución de las iniciativas del Plan estratégico (2015 - 2019)



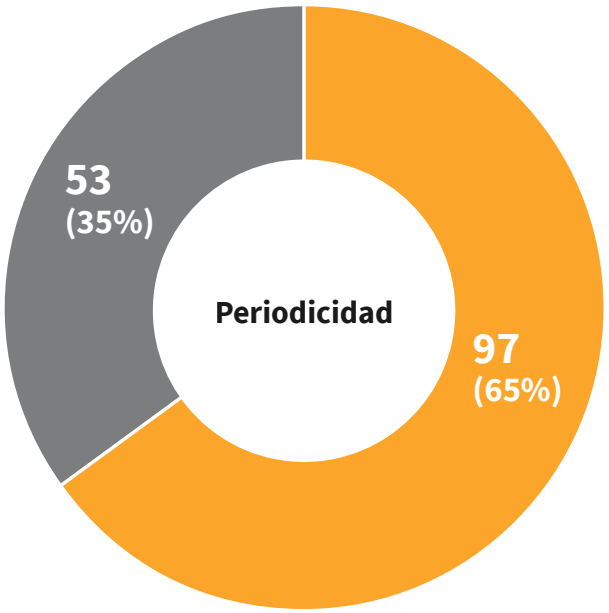
Incremento global de las acciones del Plan



Cifra final

Incremento sobre la previsión inicial

Periodicidad de las accciones del Plan



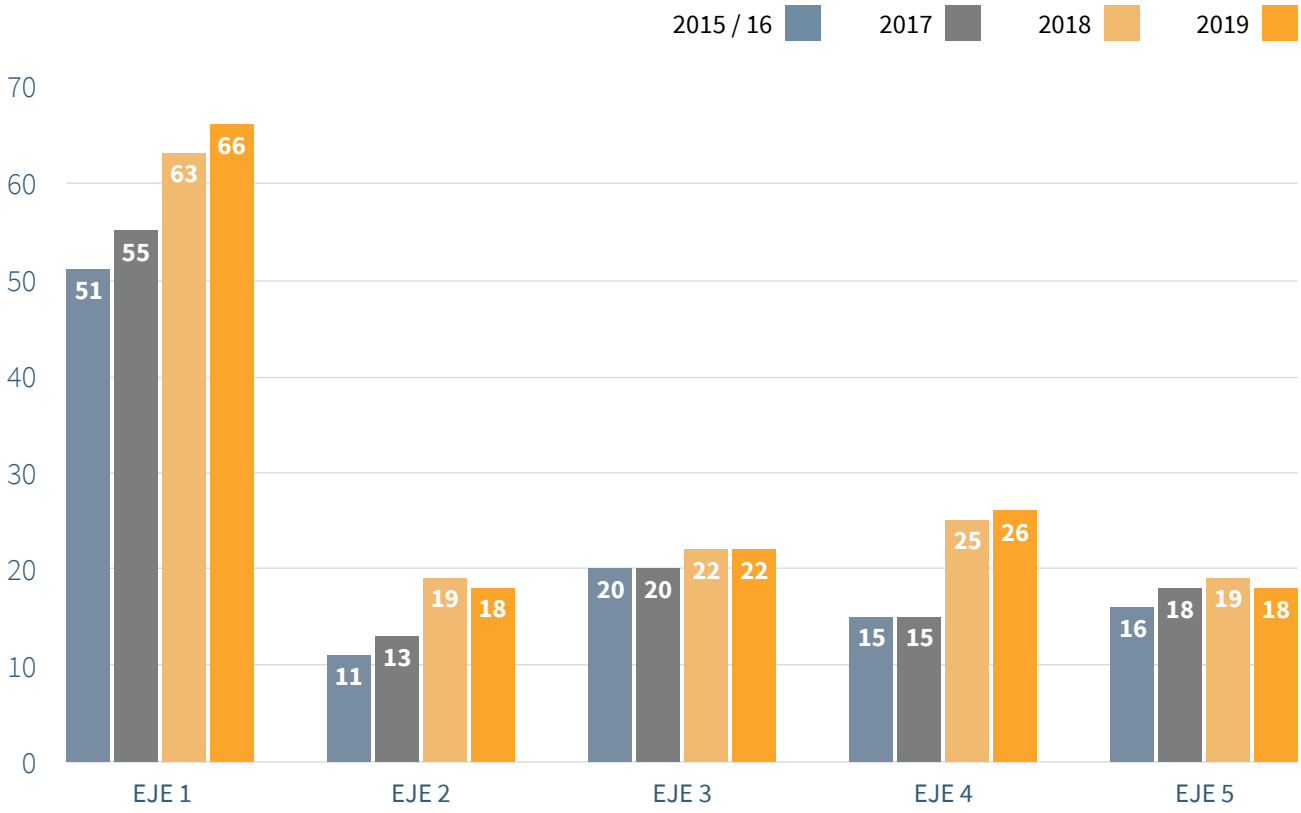
Acciones de ejecución continua o plurianual

Acciones de ejecución no continua o anual / bianual

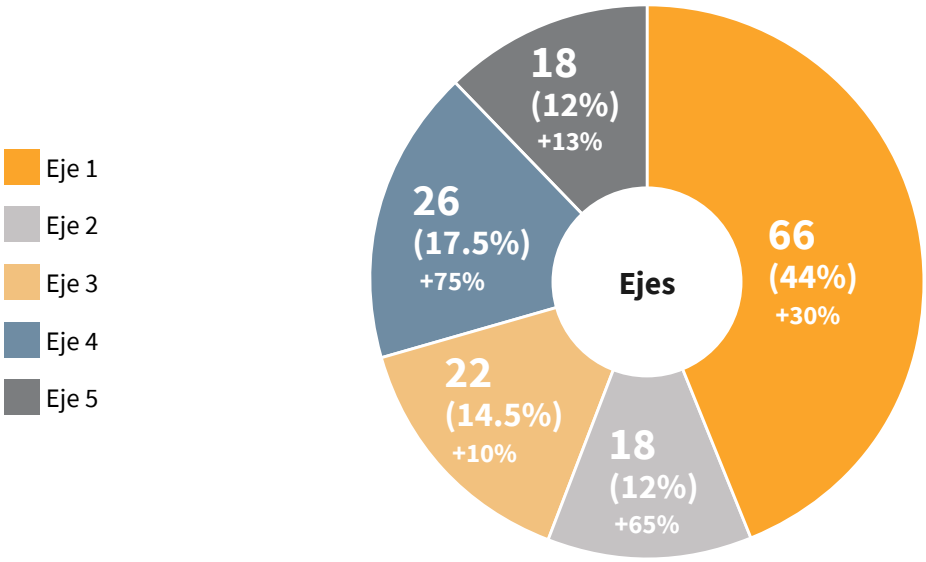
Evolución de las acciones del Plan por ejes y años

Ejes	Cronograma inicial	2017		2018		2019	
		Increm.	Total	Increm.	Total	Increm.	Total
Eje 1	51	+4 (6/2)	55	+8 (11/3)	63	+3 (4/1)	66 (+15)
Eje 2	11	+2 (2/0)	13	+6 (7/1)	19	-1 (2/3)	18 (+7)
Eje 3	20	-	20	+2 (2/0)	22	0	22 (+2)
Eje 4	15	-	15	+10 (11/1)	25	+1 (2/1)	26 (+11)
Eje 5	16	+2 (2/0)	18	+1 (3/2)	19	-1 (0/2)	18 (+2)
TOTAL	**113**		**121**		**148**		**150 (+37)**

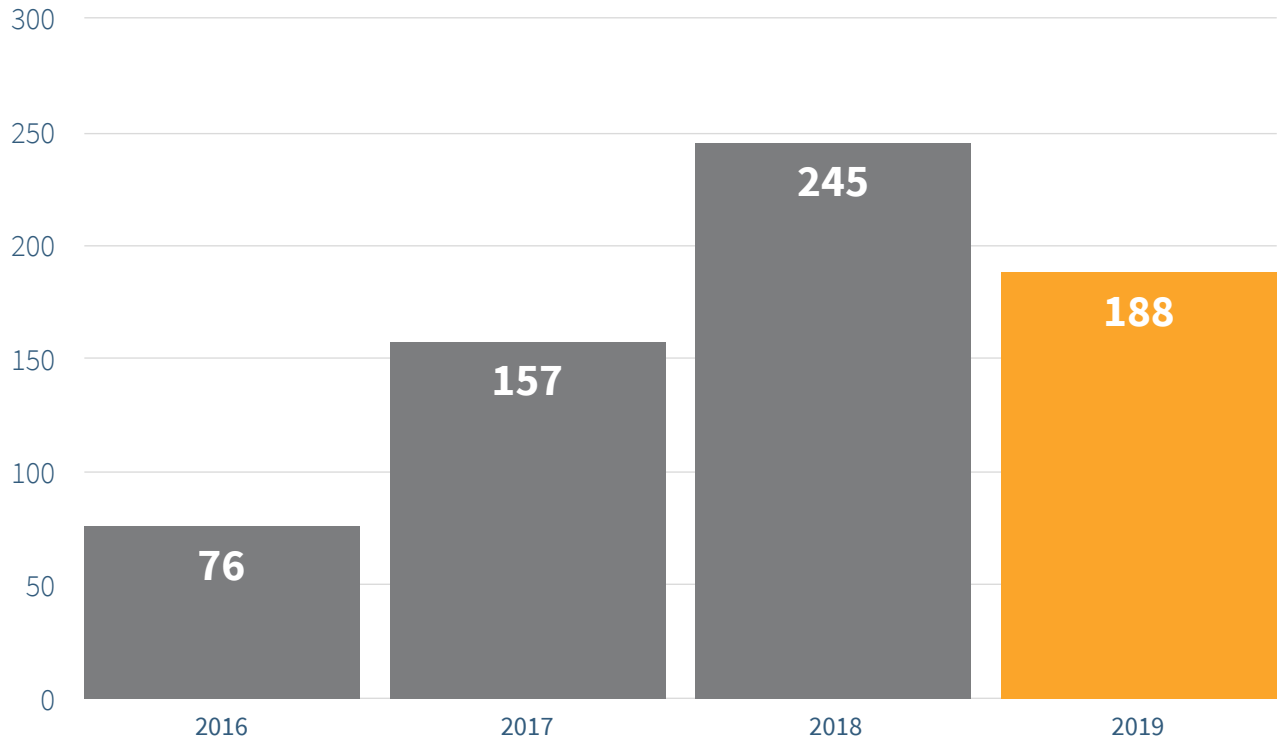
Evolución de las iniciativas del Plan por ejes y años



Distribución final de las acciones del Plan/Incremento sobre la previsión inicial



Actividades públicas de la AEPD 2016 - 2019



Grado de cumplimiento del Plan estratégico

Ejes	Cronograma inicial	Nuevas altas	Bajas	Cronograma final	Crecimiento	Grado de cumplimiento
Eje 1	51	15	-	66	+ 30%	**100%**
Eje 2	11	8	1	18	+ 65%	**95%**
Eje 3	20	2	-	22	+ 10%	**100%**
Eje 4	15	11	-	26	+ 75%	**100%**
Eje 5	16	3	1	18	+ 13%	**95%**
TOTAL	**113**	**39**	**2**	**150**	**+ 38,6%**	**98%**

Grado de cumplimiento global

2. Inspección de datos

1. Reclamaciones y actuaciones por iniciativa propia

La Subdirección General de Inspección de Datos, SGID, es la unidad dentro de la Agencia que se centra en verificar el cumplimiento de la normativa en materia de protección de datos a través de determinados análisis. Estas investigaciones se realizan a partir de las reclamaciones que llegan a la Agencia, directamente o a través de alguna Autoridad de Control de algún Estado miembro del Espacio Económico Europeo (EEE), y por propia iniciativa, en determinados casos.

En relación a las reclamaciones que llegan directamente a la AEPD hay que decir que desde el 25 de mayo de 2018, las denuncias y las reclamaciones de tutela pasaron a denominarse reclamaciones siguiendo la nomenclatura del Reglamento General de Protección de Datos (RGPD), eliminándose la distinción entre unas y otras. Esto ha supuesto un cambio a la hora de organizar el trabajo y, además, mejoras en los tiempos de respuesta que se están ofreciendo.

Las reclamaciones que tienen carácter transfronterizo presentadas en un Estado miembro del EEE o aquellas en las que es la Autoridad de Control de un Estado miembro decide iniciar una actuación por propia iniciativa, en las que la AEPD está afectada, las remiten las autoridades de control (AC) para que se inicie un procedimiento de cooperación, teniendo en cuenta el mecanismo de ventanilla única, establecido en el artículo 60 del RGPD. Por ello, la SGID también evalúa su participación en la iniciación de procedimientos de cooperación de casos transfronterizos en los que otras AC nos comunican una reclamación.

Por otro lado, como consecuencia de determinadas reclamaciones, la AEPD también determina la apertura de otras actuaciones por propia iniciativa derivadas del conocimiento directo o indirecto de circunstancias, conductas o hechos que puedan infringir la normativa de protección de datos. A todo ello hay que sumar la realización de planes sectoriales y auditorías preventivas, previstas en la normativa.

Dentro de los casos en los que se actúa iniciativa propia hay que destacar las que se realizan, cuando procede, a raíz de las notificaciones de brechas de seguridad en materia de protección de datos. Las notificaciones se efectúan de acuerdo con el artículo 33 del RGPD. Estas brechas se reciben en primera instancia en la Unidad de Evaluación y Estudios Tecnológicos (UEET) de la AEPD y tras un primer análisis propone a la Directora que sean trasladadas a la Subdirección General de Inspección de Datos, donde se valora el inicio de una posible investigación.

Dada la importancia que tienen, se analizan de manera independiente bajo el epígrafe de notificaciones de brechas de seguridad. Se contabilizan únicamente aquellas en las que se la UEET determina que procede su evaluación y posible investigación por parte de la Subdirección General de Inspección de Datos.

La siguiente tabla muestra estos datos y su comparación con los del ejercicio anterior.

Tipo de entrada	2018	2019	% relativo	Δ% anual
Reclamaciones presentadas en la AEPD	13.005	11.590	93%	-11%
Casos transfronterizos procedentes de otras AC del EEE	594	709	6%	33%
Propia iniciativa de la AEPD (excl. brechas)	29	15	0%	-48%
Notificaciones de brechas de seguridad trasladadas a la SGID	16	79	1%	394%
TOTAL	**13.644**	**12.474**	**100%**	**-9%**

2. Resoluciones

Uno de los indicadores que muestran la actividad que se realiza desde la Subdirección General de Inspección de Datos es el número de resoluciones que se emiten. Los diferentes conceptos en los que se clasifican las entradas, detallados en el apartado anterior, pueden dar lugar a diferentes procedimientos que finalizan en resoluciones. El número de entradas tramitadas no tiene que coincidir necesariamente con el número de resoluciones firmadas: varias reclamaciones referidas a un mismo reclamado pueden agruparse y, paralelamente, en una reclamación pueden aparecer múltiples reclamados dando origen a múltiples procedimientos y, por lo tanto, a diferentes resoluciones.

Resoluciones en fase de Análisis de la Reclamación

La primera fase que se lleva a cabo en la tramitación de las reclamaciones es el análisis inicial de cada una de ellas. Comprende su clasificación, la verificación formal de su contenido y el análisis de competencia y de otras causas que afectan a su fundamento y admisibilidad. Es lo que se denomina la fase de Análisis de la reclamación.

Esta fase, previa a la tramitación de cualquier procedimiento, finaliza con la inadmisión de la reclamación presentada en torno al 50% de los casos, ligeramente menor que la del año anterior, como muestra la siguiente tabla:

Número de Resoluciones finalizadas en fase de Análisis según el tipo de resultado	2018	2019	% relativo	Δ% anual
Resoluciones tras la fase de Análisis de la reclamación**	**6.190**	**5.820**	**52%**	**-6%**
Inadmisiones a trámite*	6.165	5.743	52%	-7%
Competencia de otras AC nacionales (CGPJ, AC autonómicas)*	25	77	1%	208%
Resoluciones en otras fases	**4.389**	**5.300**	**48%**	**21%**
TOTAL***	**10.579**	**11.120**	**152%**	**5%**

** Incluye reclamaciones relacionadas con el ejercicio de derechos.*

*** No se incluyen en las inadmisiones a trámite aquellas brechas de seguridad analizadas por la UEET que no se han trasladado a la SGID, por no ser técnicamente inadmisiones a trámite. Por ello, con respecto a los datos de la memoria del año pasado, el número total de inadmisiones de 2018 se ve decrementado en 531.*

**** Con respecto a años anteriores, se deduce de la cifra total de resoluciones, la contabilización de las admisiones a trámite, por ser acuerdos que prosiguen con el procedimiento y posteriormente dan pie formalmente a una resolución. Por ese motivo, el número total de 2018 aparece decrementado en 531 con respecto a la memoria del año pasado (número coincidente con el anterior, pero sin relación con él).*

Resoluciones en otras fases

Desde la entrada en vigor del RGPD y fundamentalmente de la LOPDGDD, se ha introducido una fase de traslado de la reclamación con la pretensión de resolver con mayor rapidez las reclamaciones, contando con la intervención de los responsables y de los DPD que hayan designado, en su caso. Estos traslados pueden conducir al archivo de la reclamación tras la participación del responsable o encargado del tratamiento: adoptando las medidas correctivas para solventar el posible incumplimiento y prevenir que no se produzca en el futuro, o aportando información que contribuya a clarificar la situación, de manera que se pueda determinar que no existe infracción de la normativa de protección de datos. Estos archivos no impiden que la AEPD inicie actuaciones de investigación posteriores para analizar los procedimientos implantados de acuerdo con las competencias que tiene atribuidas.

La inclusión de esta nueva fase ha supuesto una gran mejora con relación a los procedimientos de trabajo anteriores. Así, casi el 80% de las resoluciones finalizan tras la fase de traslado, dando solución a los reclamantes de manera más rápida que la que se establecía con la normativa anterior.

Debe tenerse en cuenta que, con la entrada en vigor de la LOPDGDD y la derogación de las normas anteriormente vigentes, han desaparecido de la regulación de los procedimientos administrativos los procedimientos específicos de tutela de derechos y, por lo tanto, también las resoluciones relacionadas con ellos. La nueva normativa contempla en su lugar reclamaciones de ejercicio de derechos, lo cual conlleva una tramitación que puede resultar parecida, pero dista mucho de ser idéntica desde el punto

de vista administrativo. Así, por ejemplo, las reclamaciones se ven beneficiadas por la fase de traslados, con lo que se mejoran los tiempos de resolución si se comparan con los de los antiguos procedimientos de tutelas. Por citar algunas cifras, en el 2019 aproximadamente el 75% de los procedimientos relacionados con ejercicios de derechos que pasaron la fase de Análisis se resolvieron en la de traslados y, por lo tanto, no fue necesario iniciar una actuación posterior para resolver ese ejercicio de derechos. Esto hace que el número de resoluciones emitidas tras el procedimiento de ejercicio de derechos sea menor que el número de procedimientos de tutela de derechos de ejercicios anteriores. Todo esto supone una gran ventaja para el reclamante.

Dado que ya no se realizan procedimientos específicos de apercibimiento o infracción de las AAPP, se han eliminado las referencias a los mismos, incluyéndose de forma global como procedimientos sancionadores. También se eliminan las referencias a los archivos por subsanación por haberse dejado de realizar, quedando los realizados en los primeros meses de 2018 encuadrados bajo el título de archivo por otros motivos.

Número de resoluciones finalizadas en otras fases del procedimiento según el tipo de resultado	2018	2019	% relativo	Δ% anual
Resoluciones tras traslado*	**1.897**	**4.197**	**79%**	**121%**
Respuesta satisfactoria tras traslado al responsable o encargado	863	2.598	49%	201%
Archivo por ser plena competencia de otra AC del EEE	147	384	7%	161%
Archivo provisional actuando como AC interesada en el EEE	237	571	11%	141%
Archivo por otros motivos tras traslado**	650	644	12%	-1%
Resoluciones tras Actuaciones previas de Investigación	**658**	**428**	**8%**	**-35%**
Archivo de actuaciones previas de investigación	658	428	8%	-35%
Resoluciones en procedimiento de Ejercicio de derechos* **	**0**	**337**	**6%**	**-**
Resuelto en el procedimiento de ejercicio de los derechos	0	337	6%	-
Resoluciones en procedimiento de Tutela de derechos** **	**927**	**0**	**0%**	**-**
Resuelto en procedimiento de tutela de derechos	927	0	0%	-

Número de resoluciones finalizadas en otras fases del procedimiento según el tipo de resultado	2018	2019	% relativo	Δ% anual
Resoluciones en procedimiento Sancionador	**907**	**338**	**6%**	**-63%**
Resuelto en procedimiento sancionador – Multa	369	112	2%	-70%
Resuelto en procedimiento sancionador – Apercibimiento	235	139	3%	-41%
Resuelto en procedimiento sancionador – Archivo	303	87	2%	-71%
TOTAL	**4.389**	**5.300**	**100%**	**21%**

** En 2019 se incluyen reclamaciones relacionadas con el ejercicio de derechos.*

*** En 2018, el número de archivos incluye requerimientos de subsanación no respondidos, requerimientos que dejaron de realizarse coincidiendo con la plena aplicación del RGPD.*

Esta cifra incluye también los traslados originados por denuncias de videovigilancia de FF y CC de Seguridad del Estado recibidas.

**** La entrada en vigor de la Ley Orgánica 3/2018 ha ocasionado un nuevo procedimiento referido al ejercicio de los derechos establecidos en Reglamento (UE) 2016/679.*

***** Los procedimientos de tutelas dejaron de tramitarse con la entrada en vigor de la Ley Orgánica 3/2018.*

Tiempos medios de resolución

Se reflejan a continuación los tiempos medios, en días, hasta que se dicta una resolución.

En fase de **Análisis de la reclamación**, el tiempo medio responde al tiempo desde que tiene entrada la reclamación hasta que se resuelve su inadmisión. Debe tenerse en cuenta que el artículo 65.5 de la LOPDGDD establece un tiempo 3 para este concepto inferior a tres meses, lo que significa que durante el año 2019 se ha reducido ese tiempo de un 74%.

Tiempos medios de resolución en fase de Análisis (en días)	2018	2019	Δ% anual
Resoluciones tras el Análisis de la reclamación*	20	25	25%
TOTAL	**20**	**25**	**25%**

** Incluye reclamaciones relacionadas con el ejercicio de derechos.*

En la fase de traslado, el tiempo medio responde al tiempo desde que tiene entrada la reclamación hasta que se firma su resolución.

Por su parte, con la inclusión de la fase adicional de traslado y los plazos marcados para ésta en la LOPDGDD, en 2019 los tiempos de resolución en actuaciones previas de investigación, en procedimientos de ejercicio de derechos y en procedimientos sancionadores, se contabilizan desde la fecha de admisión a trámite de la reclamación hasta que se firma la resolución.

Se puede observar cómo disminuyen de manera significativa los tiempos medios de las resoluciones de actuaciones previas de investigación y de las del procedimiento sancionador con relación al año anterior y, aunque aumentan los de las resoluciones tras el traslado, debido al aumento significativo de carga de trabajo, suponen una importante reducción de tiempo de cara a los reclamantes.

Tiempos medios de resolución según la fase del procedimiento (en días)	2018	2019	Δ% anual
Resoluciones tras traslado*	76	126	66%
Resoluciones tras actuaciones previas de Investigación	177	138	-22%
Resoluciones tras procedimiento de Ejercicio de derechos**	0	109	-
Resoluciones tras procedimiento de Tutela de derechos***	86	0	-
Resoluciones tras procedimiento Sancionador	297	212	-29%
TIEMPO MEDIO	**139**	**132**	**-5%**

** En 2019, se incluyen reclamaciones relacionadas con el ejercicio de derechos.*

*** La entrada en vigor de la Ley Orgánica 3/2018 ha ocasionado un nuevo procedimiento referido al ejercicio de los derechos establecidos en Reglamento (UE) 2016/679.*

**** Los procedimientos de tutelas dejaron de tramitarse con la entrada en vigor de la Ley Orgánica 3/2018.*

3. Actuaciones realizadas

Las cifras que se muestran a continuación dan una perspectiva del total de las actuaciones realizadas en la Subdirección General de Inspección de Datos que finalizan una fase del procedimiento administrativo, pero que no lo concluyen y, por lo tanto, no dan lugar a resoluciones. Un ejemplo de ello sería una actuación previa de investigación que da lugar a un procedimiento sancionador; esta actuación no genera una resolución y, por lo tanto, no aparece detallada en el apartado anterior, pero, sin embargo, sí implica un trabajo que es el que se indica en este epígrafe. En el caso de procedimientos de ejercicio de derechos, sancionadores o recursos de reposición, que siempre ponen fin al procedimiento administrativo y producen, por tanto, una resolución, las cifras son coincidentes con las dadas en el capítulo anterior.

Al observar la tabla se puede apreciar la importancia que tiene la fase de traslados por el aumento que muestra respecto del ejercicio anterior, en el que la aplicación de la nueva normativa solo se aplicó desde mediados de 2018 y como disminuyen las actuaciones de investigación y los procedimientos sancionadores al quedar solucionadas las reclamaciones en la fase de traslados.

Número de actuaciones finalizadas según la fase del procedimiento	2018	2019	Δ% anual
Reclamaciones analizadas*	12.708	11.553	-9%
Traslados*	2.300	5.691	147%
Actuaciones previas de investigación	1.006	526	-48%
Ejercicio de derechos**	0	337	-
Tutelas de derechos***	927	0	-
Procedimientos sancionadores	907	338	-63%
Recursos de reposición	926	698	-25%
TOTAL	**18.774**	**19.143**	**2%**

** Incluye reclamaciones relacionadas con el ejercicio de derechos.*

*** La entrada en vigor de la Ley Orgánica 3/2018 ha ocasionado un nuevo procedimiento referido al ejercicio de los derechos establecidos en Reglamento (UE) 2016/679.*

**** Los procedimientos de tutelas dejaron de tramitarse con la entrada en vigor de la Ley Orgánica 3/2018.*

Tiempos medios de tramitación

Los tiempos que aparecen en este apartado se refieren a los tiempos medios de actuaciones de cada una de las fases individuales relacionadas con la gestión de la reclamación. Estos tiempos medios se miden en días desde el inicio de cada fase hasta su finalización. **Se puede observar una gran disminución, del 55%, en los tiempos medios.**

Tiempos medios de actuaciones realizadas en la gestión de la reclamación según la fase del procedimiento (en días)	2018	2019	Δ% anual
Actuaciones previas de investigación	136	110	-19%
Ejercicio de derechos*	0	89	-
Tutelas de derechos**	83	0	-
Procedimientos sancionadores	128	115	-10%
Recursos de reposición	60	72	19%
TOTAL	**21**	**9**	**-55%**

** La entrada en vigor de la Ley Orgánica 3/2018 ha ocasionado un nuevo procedimiento referido al ejercicio de los derechos establecidos en Reglamento (UE) 2016/679.*

*** Los procedimientos de tutelas dejaron de tramitarse con la entrada en vigor de la Ley Orgánica 3/2018.*

4. Recursos

Los recursos interpuestos frente a resoluciones de los procedimientos de Inspección se muestran a continuación, según hayan sido de reposición, extraordinarios de revisión, o contencioso-administrativos.

Tipo de recurso	2018	2019	Δ% anual
Recursos de reposición	758	797	5%
Recursos extraordinarios de revisión	11	14	27%
Recursos contencioso-administrativos	140	109	-22%
TOTAL	**909**	**920**	**1%**

Los recursos de reposición y revisión resueltos anualmente por la AEPD se muestran en la siguiente tabla.

Tipo de recurso	2018	2019	Δ% anual
Recursos de reposición	926	698	-25%
Recursos extraordinarios de revisión	14	11	-21%
TOTAL	**940**	**709**	**-25%**

5. Clasificaciones

Reclamaciones planteadas con mayor frecuencia

Se muestran las 10 áreas de actividad con mayor número de reclamaciones recibidas en 2019.

Reclamaciones planteadas con mayor frecuencia	2018	2019	% relativo	Δ% anual
TOP 10	**10.273**	**8.826**	**76%**	**-14%**
Servicios de Internet	1.353	1.529	13%	13%
Videovigilancia	1.396	1.415	12%	1%
Ficheros de Morosidad	2.127	1.407	12%	-34%
Reclamación de Deudas	1.261	1.059	9%	-16%
Publicidad (excepto spam)	644	784	7%	22%
Administración pública	957	776	7%	-19%
Comercios, transporte y hostelería	606	508	4%	-16%
Entidades financieras/acreedoras	576	464	4%	-19%
Sanidad	901	460	4%	-49%
Telecomunicaciones	451	424	4%	-6%
Otros	**2.733**	**2.764**	**24%**	**1%**
TOTAL	**13.005**	**11.590**	**100%**	**-11%**

Áreas más frecuentes en procedimientos sancionadores

Se muestran las 10 áreas de actividad con mayor número de procedimientos sancionadores finalizados en 2019.

Grupo de actividad	2018	2019	% relativo	Δ% anual
TOP 10	**674**	**287**	**85%**	**-59%**
Videovigilancia	260	106	31%	-61%
Servicios de Internet	55	58	17%	-9%
Publicidad a través de e-mail o teléfono móvil	52	32	9%	-38%
Telecomunicaciones	12	21	6%	75%
Administración Pública	51	15	4%	-71%
Asociaciones, Federaciones y Clubes	8	13	4%	63%
Contratación fraudulenta	107	13	4%	-88%
Ficheros de Morosidad	105	11	3%	-90%
Comercios, transporte y hostelería	16	10	3%	-38%
Suministros de gas, electricidad y agua	8	8	2%	0%
Otros	**233**	**51**	**15%**	**-76%**
TOTAL	**907**	**338**	**100%**	**-63%**

6. Ámbito transfronterizo (EEE)

La aplicación del RGPD desarrolla en su capítulo VII los mecanismos de cooperación entre autoridades de control del Espacio Económico Europeo, donde es de plena aplicación el Reglamento.

Casos transfronterizos con participación de la AEPD

En los casos con componentes transfronterizos que afectan a ciudadanos o a establecimientos de responsables en España, la AEPD colabora en su resolución. Según se encuentre el establecimiento principal del responsable en España o en otro Estado miembro, en atención al mecanismo de ventanilla única, la participación será como autoridad principal o interesada.

Papel de la AEPD	2018	2019	Δ% anual
Nuevos casos liderados como autoridad principal	15	21	40%
Nuevos casos en cooperación como autoridad interesada	229	565	147%
TOTAL	**244**	**586**	**140%**

Entradas recibidas relacionadas con el procedimiento de Cooperación

Además del mecanismo de ventanilla única desarrollado en el artículo 60, el RGPD también regula otros mecanismos de cooperación en el capítulo VII. Los procedimientos de los artículos 61 y 62 pueden solicitarse incluso para casos locales.

La siguiente información recopila tanto los nuevos casos procedentes de otras AC, como otras solicitudes de asistencia y consulta recibidos por la AEPD, así como los proyectos de decisión analizados y participados por la AEPD.

Tipo de entrada	2018	2019	Δ% anual
Casos transfronterizos procedentes de otras AC	594	790	33%
Solicitudes de asistencia de otras AC	18	93	417%
Consultas de otras AC en procedimientos transfronterizos	6	119	1883%
Proyectos de decisión de casos en los que la AEPD participa	9	50	456%
TOTAL	**627**	**1.052**	**68%**

Peticiones enviadas relacionadas con el procedimiento de Cooperación			

Finalmente, se muestra la misma tabla que en el apartado anterior, con la visión opuesta: los casos, solicitudes, consultas y proyectos de decisión emitidos por la AEPD.

Tipo de notificación	2018	2019	Δ% anual
Casos transfronterizos compartidos con otras AC	56	86	54%
Solicitudes de asistencia a otras AC	14	61	336%
Consultas a otras AC en procedimientos transfronterizos	0	46	-
Proyectos de decisión de casos liderados por la AEPD	0	21	-
TOTAL	**70**	**214**	**206%**

7. Multas

Las siguientes cifras hacen referencia a las sanciones impuestas en resolución firme, con independencia de su estado de ejecución y recaudación.

Evolución de las multas impuestas			
Evolución de las multas impuestas	**2018**	**2019**	**Δ% anual**
Número de multas	371	112	-70%
Importe total en euros	13.180.655	6.295.923	-52%

Puede observarse que se ha producido un notable descenso tanto en el número de multas como en el importe total de las sanciones. Ello se debe a varios motivos.

En primer lugar, como se ha indicado anteriormente, el RGPD establece un nuevo enfoque que propicia la proactividad de los responsables y los DPD, de tal modo que hay muchas reclamaciones que pueden solucionarse en las fases anteriores, particularmente en el traslado.

En segundo lugar, el RGPD también dispone que en caso de infracción leve o cuando la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento.

Por último, es necesario recordar que, puesto que en muchas ocasiones el origen de las vulneraciones se encuentra en los procesos de gestión de datos, desde el 25 de mayo de 2018 se está tendiendo a ir más allá de las reclamaciones concretas para realizar grandes análisis de los sistemas de tratamiento de datos de los responsables.

Estas investigaciones son muy complejas y conllevan una duración superior a la de una reclamación ordinaria. En consecuencia, a medida que se vayan finalizando ese tipo de actuaciones de investigación, se irán instruyendo los correspondientes procedimientos sancionadores en los que los importes de las sanciones que se propongan serán acordes a la naturaleza de la infracción que se detecte.

Áreas con mayor importe global de multas

La siguiente información desglosa las 6 áreas de actividad con mayor importe en sanciones en 2019.

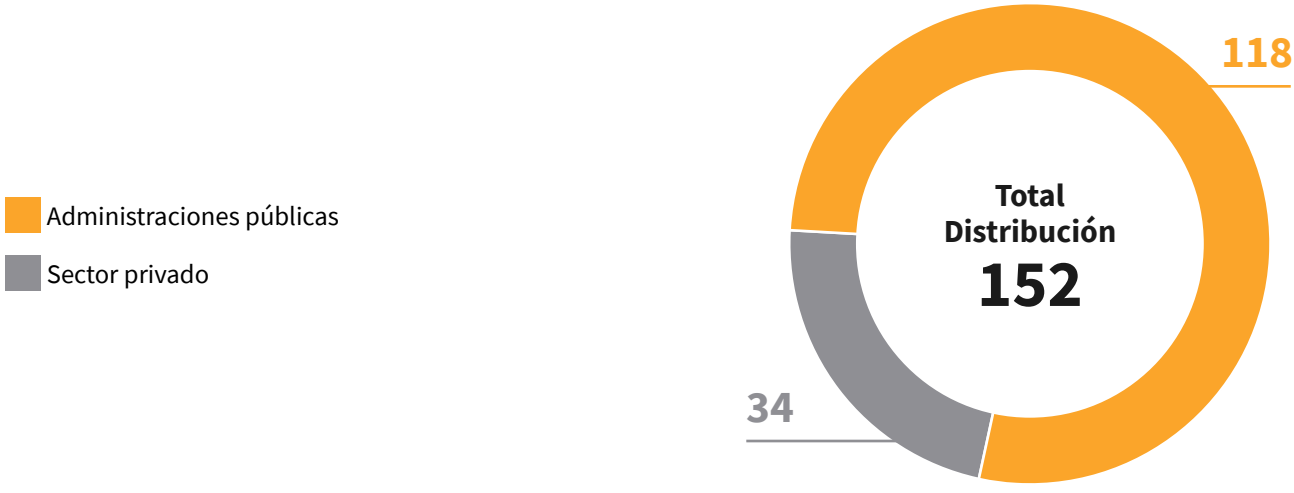
Importe de multas en euros según el sector de actividad	2018	2019	% relativo	Δ% anual
Seis sectores con mayor de actividad	**10.340.209**	**5.264.122**	**84%**	**-49%**
Directorios	1.074.002	2.900.000	46%	170%
Telecomunicaciones	230.001	641.000	10%	179%
Contratación fraudulenta	5.003.200	620.620	10%	-88%
Quiebras de seguridad	60.200	460.000	7%	664%
Energía/Agua	130.002	356.001	6%	174%
Ficheros de Morosidad	3.842.804	286.501	5%	-93%
Otros sectores	**2.840.446**	**1.031.801**	**16%**	**-64%**
TOTAL	**13.180.655**	**6.295.923**	**100%**	**-52%**

3. Gabinete jurídico

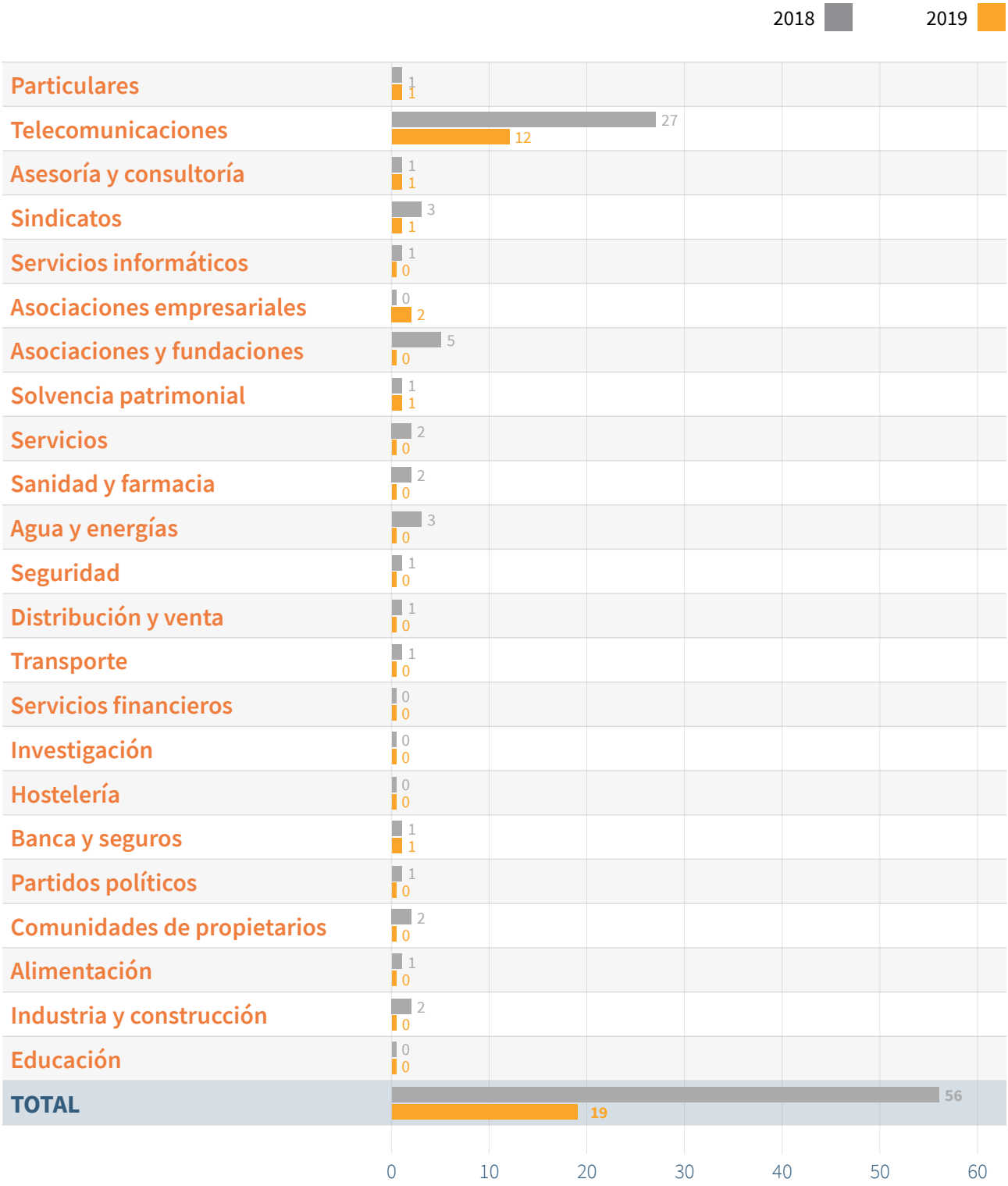
Consultas

Administraciones públicas	
Administración General del Estado	85
Comunidades Autónomas	14
Entidades locales	6
Otros Organismos	13
TOTAL	**118**
Consultas privadas	
Asociaciones y Fundaciones	4
Empresas	20
Particulares	1
Sindicatos	3
Otros	6
TOTAL	**34**
TOTAL	**152**

Distribución 2019 de consultas públicas / privadas

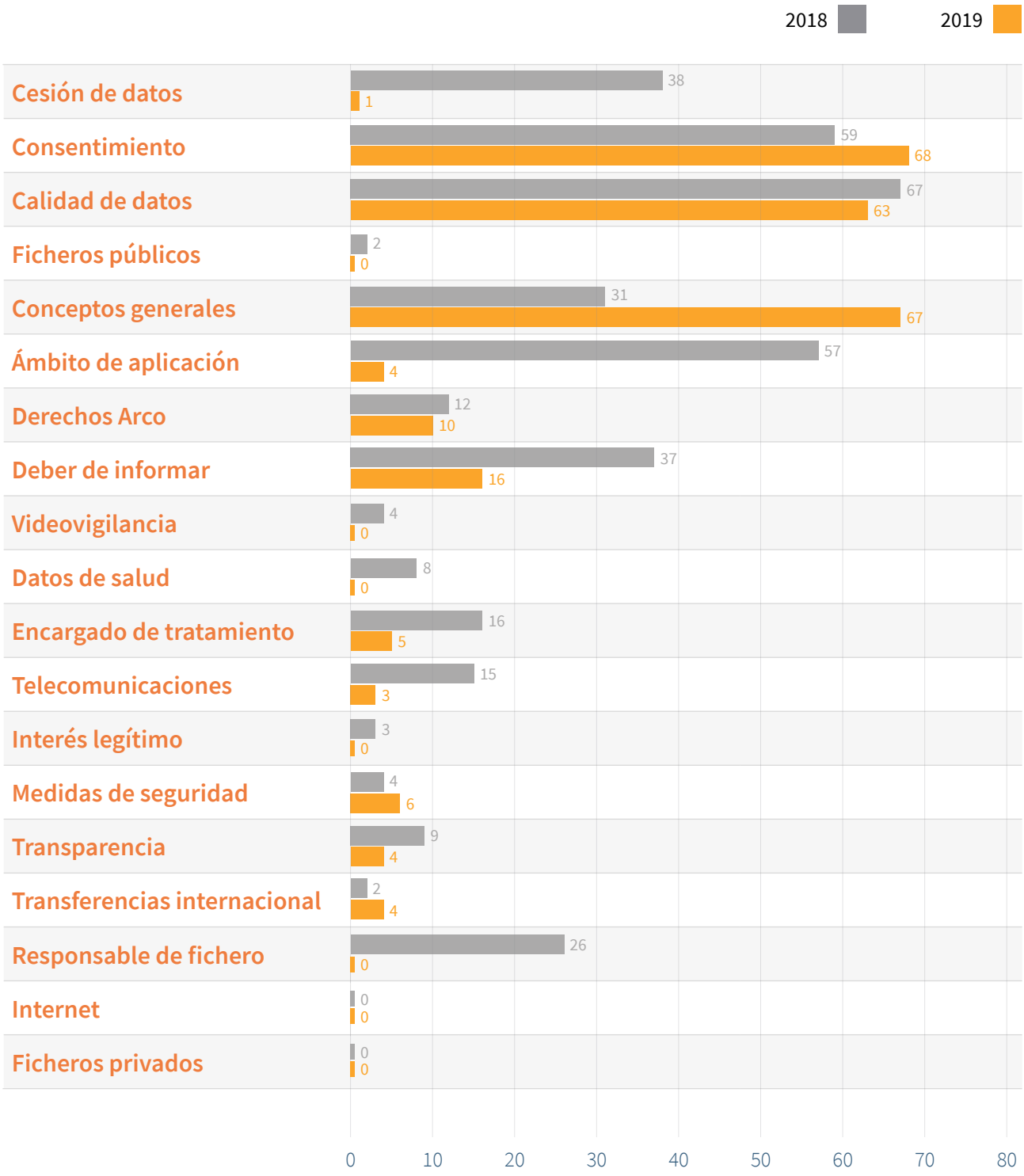


Evolución de las consultas por sectores



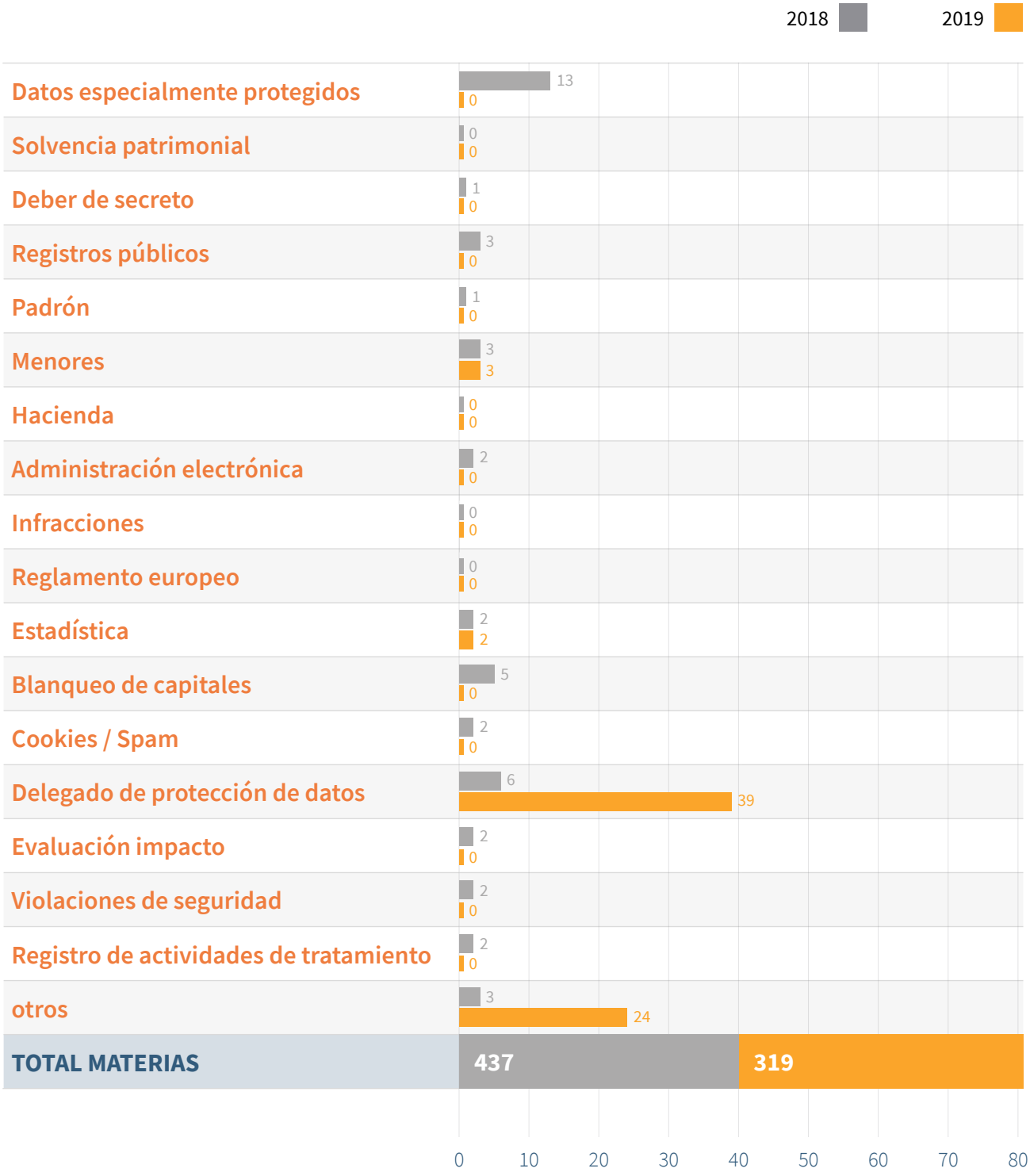
Nota: Existen consultas que versan sobre más de un sector y son clasificadas en el que mas relevancia tengan. Asimismo otras categorias estan en desuso y tienden a desaparecer por la evolucion normativa actual, se mantienen en términos comparativos con el ejercicio anterior.

Evolución de las consultas por materias



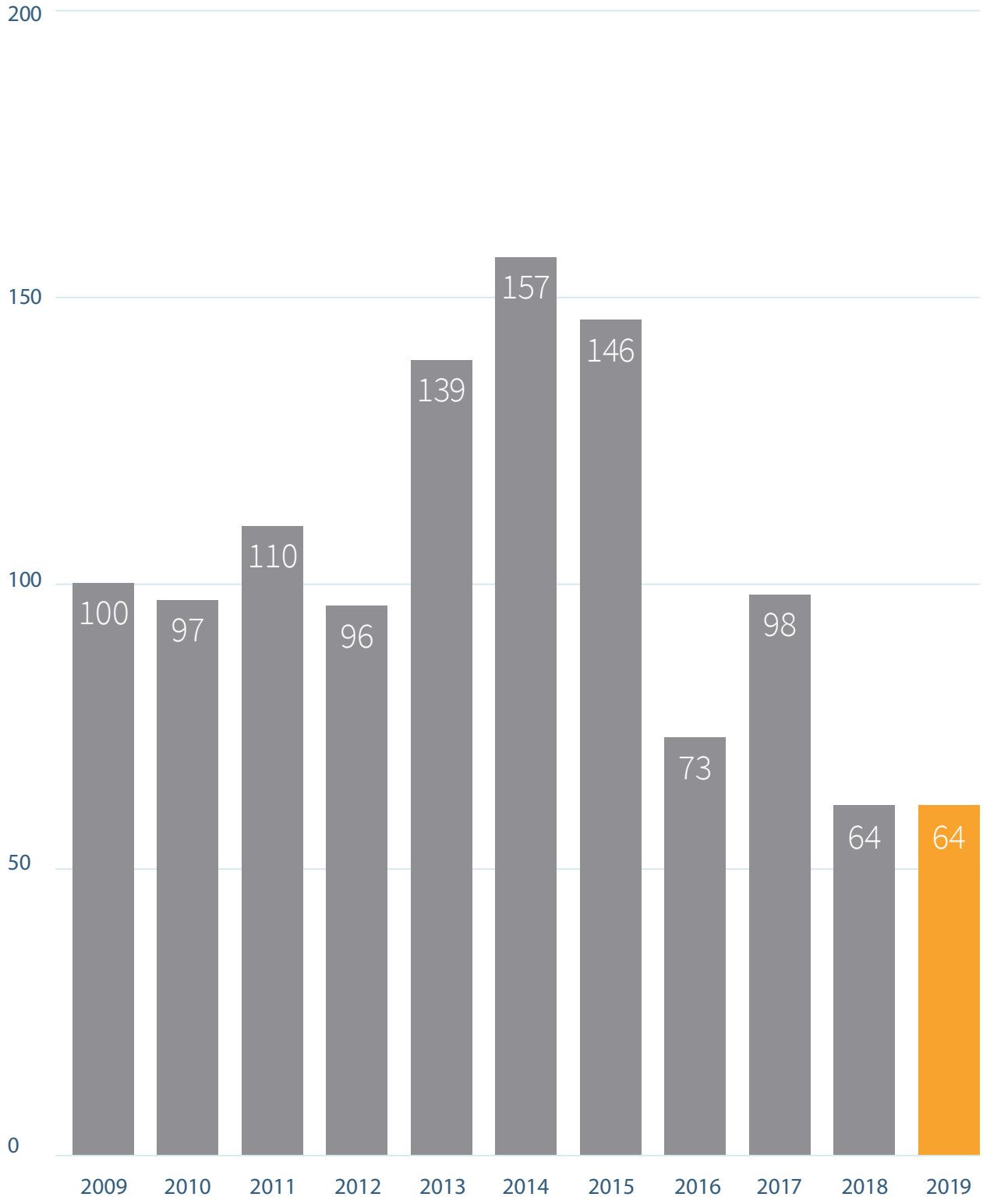
Nota: Existen consultas que versan sobre más de una materia y son clasificadas en el que mas relevancia tengan. Asimismo otras categorias, si bien estarían en desuso y tienden a desaparecer, se mantienen por razones comparativas con otros ejercicios.

Evolución de las consultas por materias

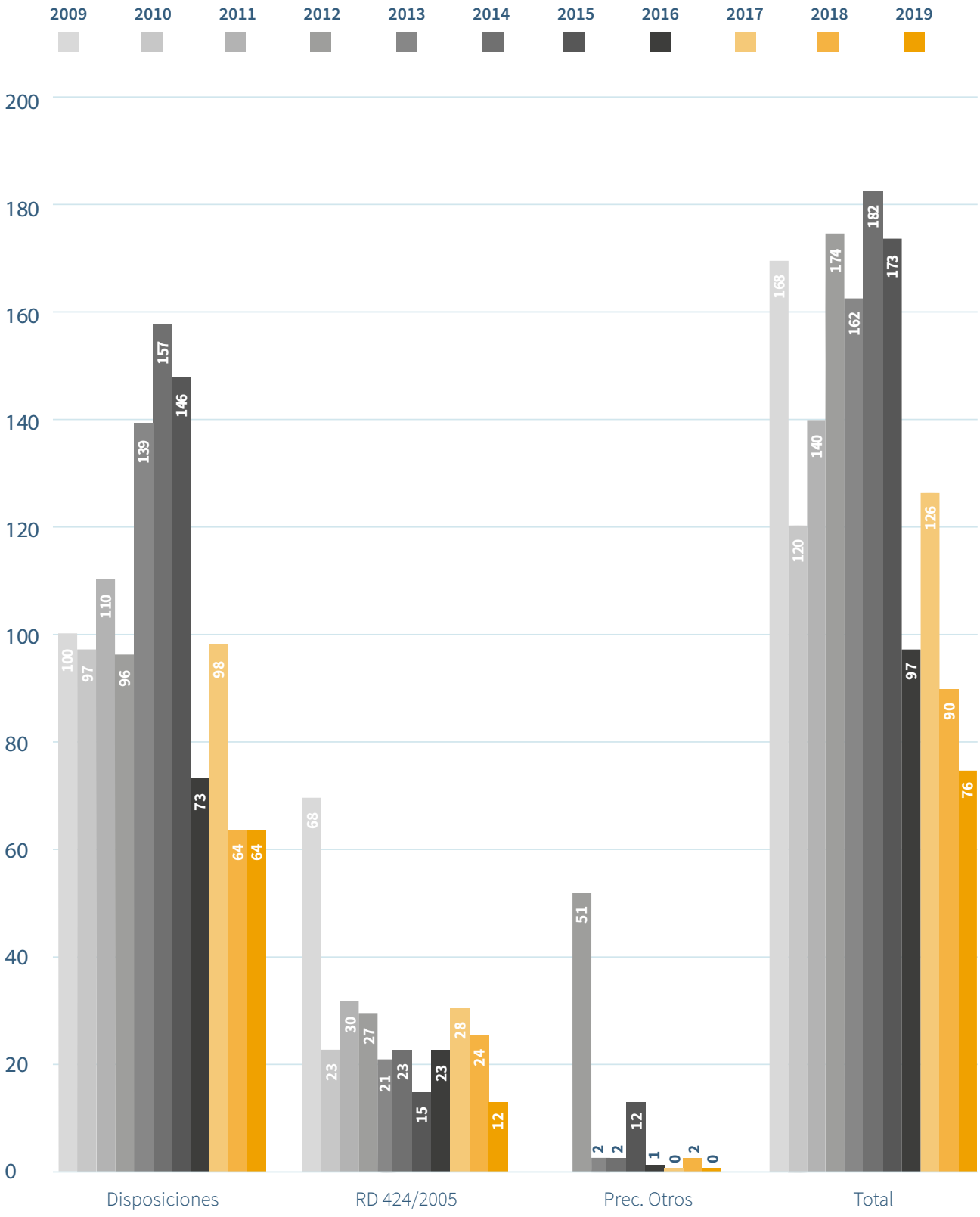


Nota: Existen consultas que versan sobre más de una materia y son clasificadas en el que mas relevancia tengan. Asimismo otras categorias, si bien estarían en desuso y tienden a desaparecer, se mantienen por razones comparativas con otros ejercicios.

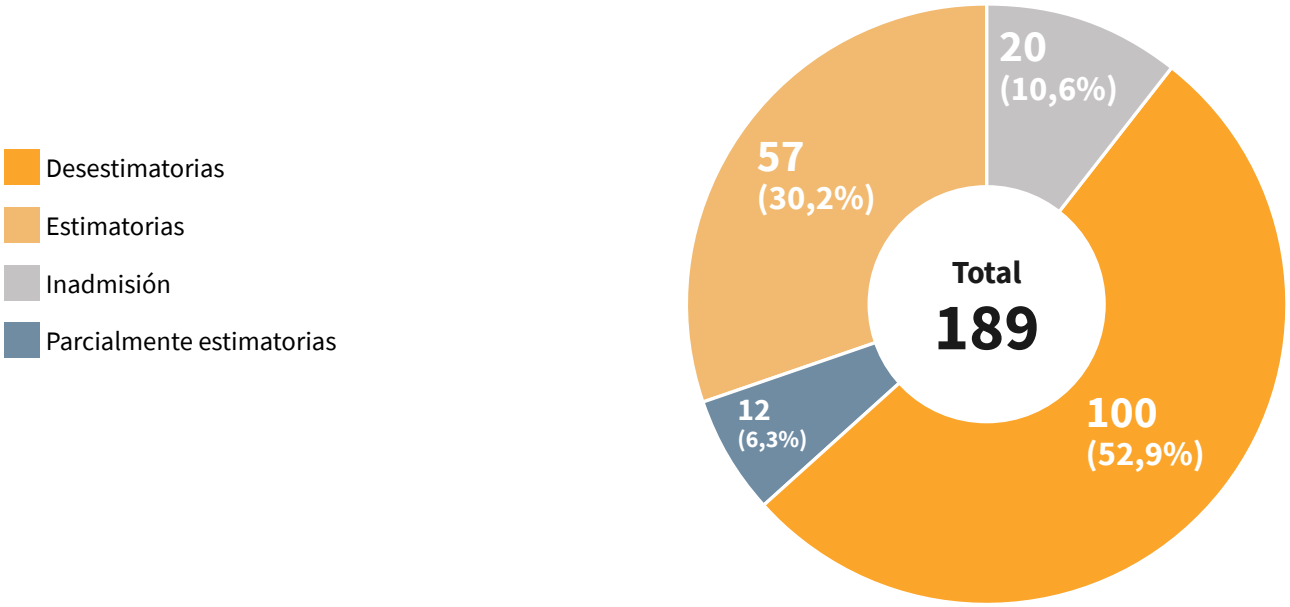
Evolución de informes preceptivos a disposiciones generales (2009-2019)



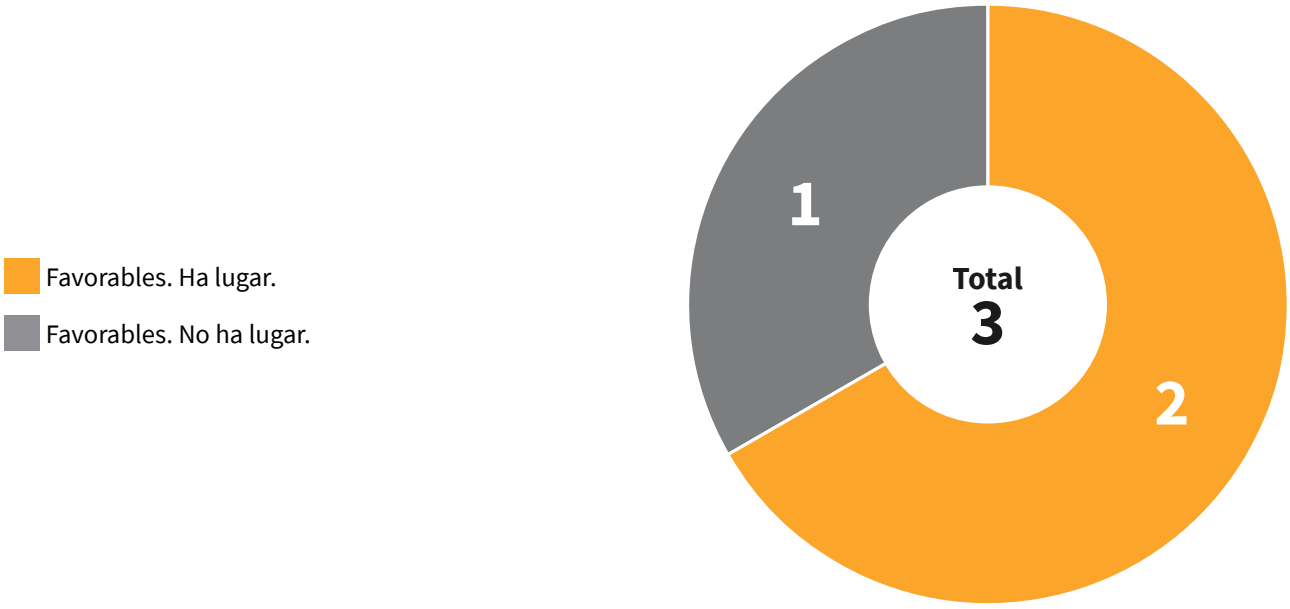
Evolución Informes Perceptivos (2009 - 2019)



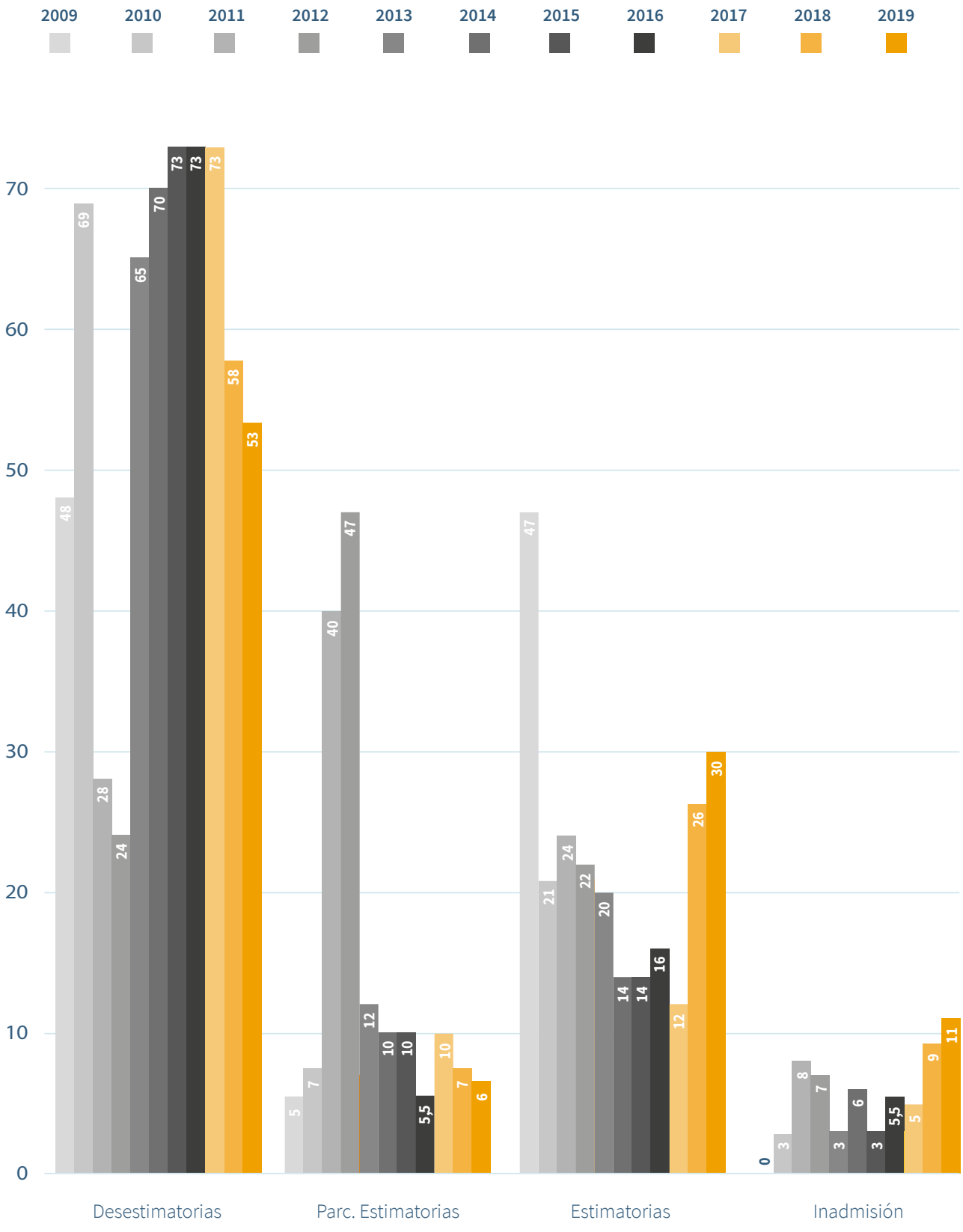
Sentencias Audiencia Nacional en 2019



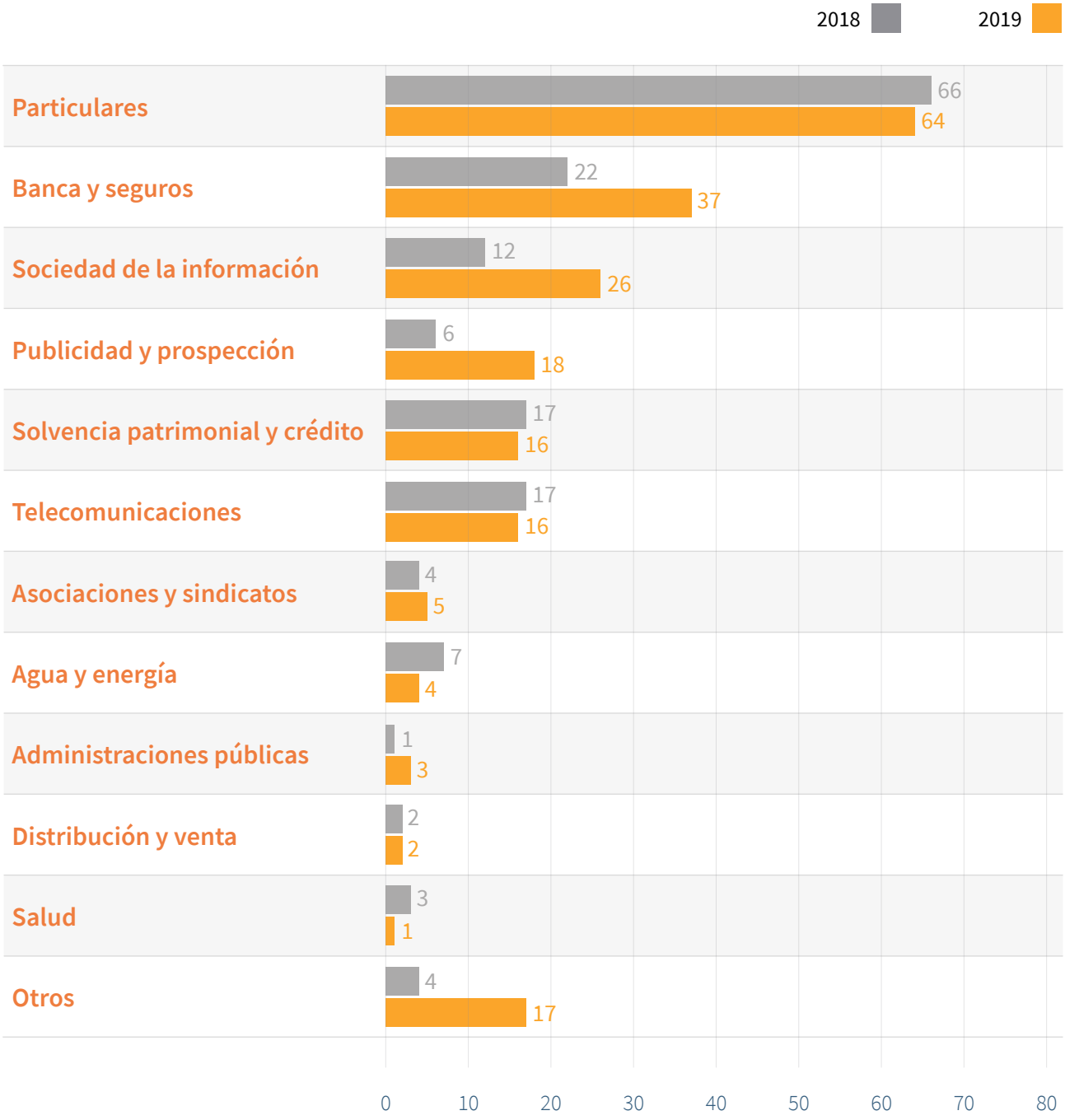
Sentencias Tribunal Supremo 2019



Evolución por sentido del fallo en porcentajes (2009 - 2019)



Comparativa por sector recurrente



TOTAL *	161	209

** En esta estadística se incluyen, ádemas de las Sentencias, los recursos que han finalizado mediante Auto de desistimiento y de caducidad.*

4. Atención al ciudadano y cumplimiento. Autorizaciones y Transparencia

Consultas totales planteadas ante el área de Atención al Ciudadano				
	2017	2018	2019	% 2018 - 2019
Presenciales	3.699	3.455	2.443	-29,29
Telefónicas	73.501	88.302	60.288	-31,72
FAQs	170.754	651.650	562.457	-13,68
Escritas (Correo electrónico y Sede electrónica)	7.954	5.613	10.082	+79,61
TOTAL	**255.298**	**749.020**	**635.270**	**-15,18**

Comparativa de visitas a la web (www.agpd.es)				
	2017	2018	2019	% 2018 - 2019
Visitas	6.724.113	7.925.300	6.723.331	-15,16%

Consultas especializadas sobre el tratamiento de datos de menores				
	2017	2018	2019	% 2018 - 2019
Teléfono	178	597	535	-10,39
WhatsApp	247	384	421	+9,64
Correo electrónico	246	388	380	-2,06
Sede electrónica	224	195	166	-14,87
TOTAL	**895**	**1.564**	**1.502**	**-3,96**

Accesos al portal de vídeos "Protege tus datos en internet"				
	2017	2018	2019	% 2018 - 2019
Accesos al canal	29.672	34.347	87.249	+154,02
Visualizaciones de vídeos*	33.283	334.455	175.418	-47,55

**Se puede acceder a los vídeos directamente sin para por el canal a través de la web "tudecideseninternet.es"*

Accesos a la web www.tudecideseninternet.es				
	2017	2018	2019	% 2018 - 2019
1. Visitantes distintos	66.810	121.998	71.651	-41,26
2. Número de visitas	101.500	169.689	117.234	-30,91

1. Visitante que ha solicitado al menos una página. Si este visitante ingresa numerosas veces sólo contará como una.

2. Número de visitas realizadas por todos los visitantes. Si cada visitante tiene una sesión, cada visita que realice aumentará este contador.

Canal INFORMA_RGPD		
	desde marzo 2018	2019
Consultas	4.116	2.758[1]

Herramienta Facilita[2]		
Sección	2018	2019
Accesos a Facilita_RGPD	622.550	197.279
Cuestionarios finalizados	150.360	49.086

Herramienta Gestiona[3]		
Sección	Abierto	Finalizado
Evaluaciones de impacto de la privacidad (EIPD)	5.403	2.750
Análisis de riesgos	5.398	2.651

[1] *Este dato es menor debido a una nueva clasificación en los documentos recibidos en registro de entrada.*

[2] *Facilita_RGPD, herramienta para facilitar la adecuación al RGPD de empresas y profesionales, implantada en septiembre de 2017.*

[3] *Gestiona EIPD: Asistente para el análisis de riesgos y evaluaciones de impacto en protección de datos.*

Temas más consultados en el catálogo de preguntas frecuentes (FAQs)		
Orden	**Temas de consulta**	**Accesos**
1	En qué te podemos ayudar y en qué no	268.431
2	Tratamiento de datos en el ámbito laboral	33.171
3	Cuestiones sobre la sede electrónica	32.304
4	Delegado de Protección de Datos	25.777
5	Comunidades de propietarios	25.772
6	Videovigilancia	24.336
7	Solvencia patrimonial (ficheros de morosos)	17.859
8	Menores y educación	17.254
9	Derechos de los afectados	12.491
10	Ámbito de aplicación	11.744

Temas más consultados en la atención presencial y telefónica			
Orden	**Temas de consulta**	**Accesos**	**%**
1	Reclamaciones	3.384	26,47
2	Reglamento general de protección de datos (RGPD)	2.313	18,09
3	Derechos	1.376	10,75
4	Cuestiones técnicas de la sede electrónica	911	7,12
5	Delegados de Protección de Datos	680	5,31
6	Herramienta FACILITA	523	4,09
7	Ficheros de solvencia patrimonial	729	5,70
8	Videovigilancia	706	5,52
9	Comunidades de propietarios	333	2,60
10	Menores y educación	88	0,68
11	Otras cuestiones	1.469	11,50

Otros contenidos	
Guías generales	**Descargas**
Guía para pacientes y usuarios de la Sanidad	12.927
Guía sobre el uso de las cookies	19.527
Guía sobre el uso de las cookies (versión en inglés)	1.171
Guía de Privacidad desde el diseño	11.550
Guía de Privacidad desde el diseño (versión en inglés)	2.356
Drones y Protección de Datos	12.496
Drones y Protección de Datos (versión en inglés)	123
Guía sobre el uso de videocámaras para seguridad y otras finalidades	95.710
Guía para la gestión y notificación de brechas de seguridad	35.572
Guía para la gestión y notificación de brechas de seguridad (versión en inglés)	5.938
Protección de datos: guía para el ciudadano	81.878
Listado de elementos para el cumplimiento normativo	26.871
Guía para el responsable de tratamiento de datos personales	99.617
Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD	59.909
Guía de evaluación de impacto en la protección de datos personales	49.248
Guía para el cumplimiento del deber de informar	62.359
Directrices para la elaboración de contratos entre responsables y encargados del tratamiento	40.066
Guías sectoriales	**Descargas**
Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para Administraciones Públicas	8.784
Guía de administradores de fincas	12.322
Compra segura en INTERNET - Guía Práctica	13.690
Guía de Privacidad y Seguridad en Internet	33.727
Protección de datos y Administración Local	40.803
Guía de protección de datos y prevención de delitos	20.493

Otros contenidos	
Guías sectoriales	**Descargas**
Guía de protección de datos y prevención de delitos: fichas prácticas	4.583
Informe utilización por profesores y alumnos de aplicaciones que almacenan datos en nube...	10.213
Código de buenas prácticas en protección de datos para proyectos Big Data	8.555
Cómo gestionar una fuga de información en un despacho de abogados	3.735
Orientaciones y Garantías en los procedimientos de anonimización	11.514
Guía para clientes que contraten servicios de Cloud Computing	9.391
Orientaciones para prestadores de servicios de Cloud Computing	2.071
Estudios	**Descargas**
La protección de datos como garantía en las políticas de prevención del acoso: recomendaciones de la AEPD	1.519
Introducción al hash como técnica de seudonimización de datos personales	4.253
Consecuencias administrativas, disciplinarias, civiles y penales de la difusión de contenidos sensibles	4.895
Adecuación a la normativa a 'coste cero' y otras prácticas fraudulentas	8.023
Análisis de los flujos de información en Android	3.732
Análisis de los flujos de información en Android (Versión en Inglés)	196
Fingerprinting o Huella digital del dispositivo	12.078
Fingerprinting o Huella digital del dispositivo (Versión en Inglés)	1.791
LOPD: Novedades para los ciudadanos	16.523
LOPD: Novedades para el Sector Privado	12.321
LOPD: Novedades para el Sector Público	14.273
Plan de inspección sectorial de oficio Hospitales Públicos	1.624
25 años de la Agencia Española de Protección de Datos	2.832
Encuesta sobre el grado de preparación de las empresas españolas ante el RGPD (AEPD-CEPYME)	1.466
Informe sobre políticas de privacidad en internet. Adaptación al RGPD	6.786
Decálogo para la adaptación al RGPD de las políticas de privacidad en internet	4.572

Otros contenidos	
Infografías	**Descargas**
Balance Plan Estratégico	1.143
10 consejos básicos para comprar en internet de forma segura	218
Canal prioritario para comunicar la difusión de contenido sensible y solicitar su retirada	10.546
Protege sus datos en la vuelta a clase	4.361
Protección de datos en vacaciones	4.412
Reglamento de Protección de Datos	4.370
Compra segura en internet	4.219
Juguetes conectados	1.603
Cómo evitar la publicidad no deseada	2.662
Los derechos que tienes para proteger tus datos personales	12.594
Adaptación al RGPD de las Administraciones Públicas	6.799
Adaptación al RGPD del Sector Privado	16.007
Decálogo para el personal sanitario y administrativo	9.579
Memorias	**Descargas**
Memoria 2018	2.752
Memoria 2017	1.891

Solicitudes de acceso a la información pública						
Solicitudes	**Concedidas**	**Inadmitidas***	**Consultas****	**Acceso RGPD*****	**Denegadas**	**Desistidas**
94	45	10	25	4	3	7

* *Solicitud abusiva no justificada con la finalidad de transparencia (2), información en curso de elaboración (1), información no obra en poder de la AEPD (1).*

** *No son ejercicios del derecho de acceso a la información pública, sino consultas sobre protección de datos.*

*** *No son ejercicios del derecho de acceso a la información pública, sino del derecho de acceso a los datos personales.*

Registro de Delegados de Protección de Datos comunicados		
Titularidad	**Total notificados**	
Entidades privadas	44.069	
Entidades públicas	6.257	
	Administración General del Estado	134
	Comunidades Autónomas	378
	Entidades Locales	2.593
	Otras personas Jurídico-Públicas · Consejo General del Poder Judicial · Notarios · Colegios Profesionales · Universidades · Cámaras de Comercio · Comunidades de Regantes	3.152
TOTAL		**50.356**

Solicitud de copia de contenido de la inscripción de ficheros como ayuda para elaborar el Registro de actividades de Tratamiento[4]			
		Nº Expedientes	**Días en responder**
Recibidas en papel (correo postal, fax o en mano)	Tit. Privada	3	4
	Tit. Pública	4	
Sede electrónica AEPD	Tit. Privada Firmada	431	21
	Tit. Privada Sin Firma	57	
	Tit. Pública Firmada	28	
	Tit. Pública Sin Firma	2	

[4] *El 15 de junio dejó de estar operativo el trámite de solicitud de Copia de Contenido*

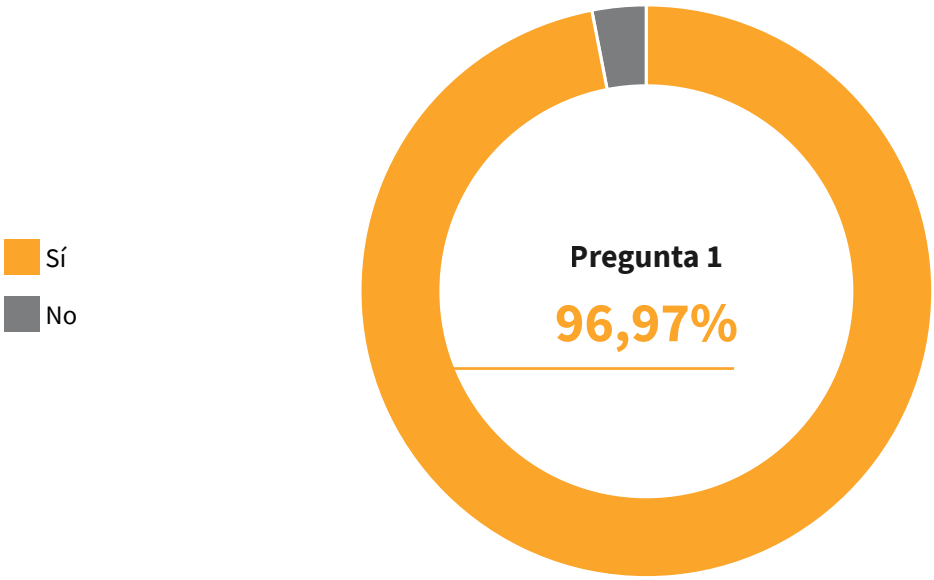
Transferencias Internacionales		
	2019	TOTAL
Autorizaciones TI	1 (Art. 46.3.a RGPD)	1
Actuaciones en la adopción de Normas Corporativas vinculantes (BCR)	6	69[5]

Encuestas de Calidad		
Resumen general		
	SI	NO
¿Está satisfecho con el contenido de la información recibida?	3.645	114
¿Considera que la persona que le atendió tiene los conocimientos técnicos suficientes?	3.652	107
¿Está satisfecho con la corrección en el trato por parte del operador?	3.699	60
TOTAL DE ENCUESTAS REALIZADAS	**3.759**	
Análisis de respuestas		
	SI	NO
¿Está satisfecho con el contenido de la información recibida?	96,97%	3,03%
¿Considera que la persona que le atendió tiene los conocimientos técnicos suficientes?	97,15%	2,85%
¿Está satisfecho con la corrección en el trato por parte del operador?	98,40%	1,60%
TOTAL DE ENCUESTAS REALIZADAS	**100%**	

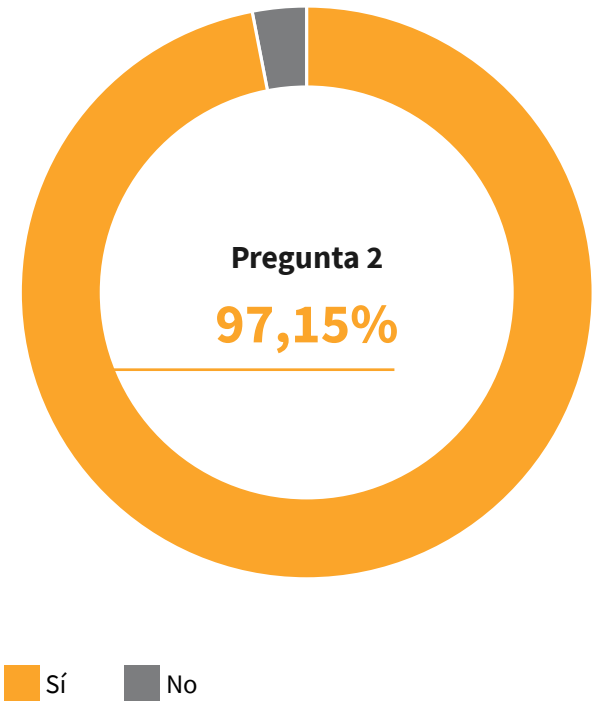
[5] *La AEPD actúa como autoridad líder en la revisión de 3 BCR*

Encuestas de Calidad - Total 3.759

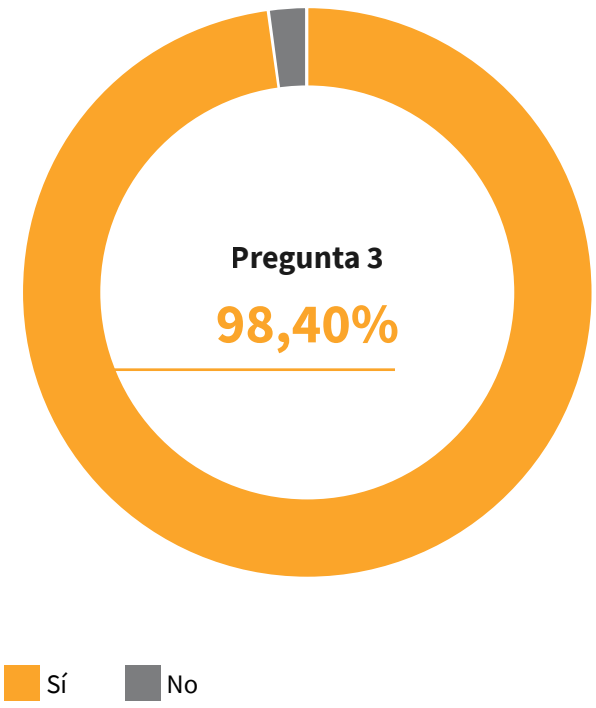
¿Está satisfecho con el contenido de la información recibida?



¿Considera que la persona que le atendió tiene los conocimientos técnicos suficientes?



¿Está satisfecho con la corrección en el trato por parte del operador?



5. Secretaría General

Evolución del presupuesto

	Crédito Ejercicio 2017	Crédito Ejercicio 2018	Crédito Ejercicio 2019
Capítulo I	7.360.820	7.986.570	**7.986.570**
Capítulo II	4.956.060	5.071.756	**4.956.060**
Capítulo III	160.950	80.950	**40.950**
Capítulo IV	284.440	284.440	**284.440**
Capítulo VI	1.316.000	937.860	**937.860**
Capítulo VIII	22.800	22.800	**22.800**
TOTAL	**14.101.070**	**14.384.376**	**14.228.680**

Gestión de recursos humanos

	Dotación	Cubiertos
Funcionarios	201	170
Laborales	4	1
Laborales fuera de Convenio	2	2
Alto cargo	1	1
TOTAL	**208**	**174**
MUJERES 93	**HOMBRES 81**	

Funcionarios

Nivel	30	29	28	26	24	22	20	18	17	16	15	14
Efectivos	7	3	26	55	0	23	5	28	2	2	10	9

Grupo	A1	A2	C1	C2
Efectivos	37	57	38	38

6. Presencia internacional de la AEPD

Reunión	Fecha	Lugar
Sesiones plenarias del Comité Europeo de Protección de Datos	22 y 23 de enero 12 y 13 de febrero 12 y 13 de marzo 9 y 10 de abril 14 y 15 de mayo 4 de junio 9 de julio 10 y 11 de septiembre 8 y 9 de octubre 12 y 13 de noviembre 2 y 3 de diciembre	Bruselas (Bélgica)

Reuniones de subgrupos del Comité Europeo de Protección de Datos

Reunión	Fecha	Lugar
Tecnología	16 de enero 20 y 21 de febrero 20 y 21 de marzo 24 y 25 de abril 22 de mayo 12 y 13 de junio 17 y 18 de julio 18 de septiembre 23 y 24 de octubre 20 de noviembre 17 de diciembre	Bruselas (Bélgica)
Usuarios de sistemas de información del CEPD (IT Users)	17 de enero 23 de mayo 7 de noviembre	
Supervisión del cumplimiento (Enforcement)	24 de enero 22 de febrero 15 de abril 17 de junio 24 de septiembre 18 de noviembre	
Subgrupo de asesoramiento (Strategic advisory)	9 de enero 31 de enero	

Reunión	Fecha	Lugar
Cooperación	20 de febrero 16 de abril 19 y 20 de junio 25 de septiembre 20 y 21 de noviembre	Bruselas (Bélgica)
Multas	21 de febrero 26 de septiembre 14 de octubre 19 de noviembre	
Asuntos financieros	14 de enero 27 de febrero 28 de marzo (videoconferencia) 20 de mayo 20 de septiembre 4 de noviembre	
Fronteras, viajeros y aplicación legislativa (BTLE)	19 de febrero 16 de abril 18 de junio 19 de septiembre 24 de octubre 12 de diciembre	
Disposiciones clave (Key Provisions)	15 de enero 18 de febrero (videoconferencia) 25 y 26 de marzo 30 de abril 23 de mayo 25 de junio (videoconferencia) 16 de julio 29 de septiembre 16 de octubre 25 y 26 de noviembre 12 de diciembre (videoconferencia)	
Cumplimiento, Gobierno electrónico y Salud (Compliance, E-goverment & Health)	10 de enero 31 de enero 4 de febrero (videoconferencia)	

Reunión	Fecha	Lugar
Cumplimiento, Gobierno electrónico y Salud (Compliance, E-goverment & Health)	25 de febrero 27 de marzo 6 de mayo 3 de junio 24 de junio 16 de septiembre 9 de diciembre 14 de octubre 15 de noviembre 9 de diciembre	Bruselas (Bélgica)
Transferencias Internacionales	29 de enero 19 y 20 de marzo 21 y 22 de mayo 18 y 19 de junio 17 y 18 de septiembre 15 y 16 de octubre 10 y 11 de diciembre	
Reglas de Procedimiento del CEPD	11 de abril 5 de junio 4 de julio	
Medios Sociales Digitales (Social Media)	26 de febrero 11 de junio 20 de septiembre 27 de noviembre	
Red de departamentos de comunicación del CEPD	17 de mayo	Viena (Austria)
Comité de Cooperación EUROPOL	8 de mayo 28 de noviembre	Bruselas (Bélgica)
Grupo de Supervisión Coordinada CIS	7 de mayo	
Grupo de Supervisión Coordinada del VIS + EURODAC	20 de junio 27 de noviembre	
Grupo de Supervisión Coordinada SIS II	19 de junio 26 de noviembre	
Plenario del órgano de supervisión conjunta de EUROJUST	7 de junio	La Haya (Países Bajos)

Reunión	Fecha	Lugar
Consejo de Europa:		
38º Plenario Convenio 108	13 y 14 de junio	Estrasburgo (Francia)
39º Plenario Convenio 108	19 y 20 de noviembre	Estrasburgo (Francia)
47ª Reunión del Convenio 108	20 al 22 de marzo	París (Francia)
48ª Reunión del Convenio 108	24 al 27 de septiembre	París (Francia)
Proyecto T4DATA - 3ª Reunión de Partners y Conferencia Final **Proyecto de la UE realizado por un consorcio liderado por la Fundación italiana Basso y del que forman parte las autoridades nacionales de supervisión de protección de datos de Italia, España, Croacia, Bulgaria y Polonia**	14 y 15 de noviembre	Roma (Italia)
41ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad	21 al 24 de octubre	Tirana (Albania)
Grupo de trabajo Auditor **Evento sobre certificaciones de protección de datos de servicios en la nube**	11 de abril	Bruselas (Bélgica)
Grupo Internacional de Protección de Datos en Telecomunicaciones (Grupo de Berlín)	9 y 10 de abril 10 y 11 de octubre	Lujbiana (Eslovenia) Bruselas (Bélgica)
I Reunión de Seguimiento del Convenio de Buenos Aires **Reunión en el marco del proyecto El PAcCTO, firmado por FIAPP F.S.P y la UE**	12 al 14 de marzo	Quito (Ecuador)
Comité Schengen **Presentación del informe de evaluación SIS 208 de la República de Letonia**	12 de junio	Bruselas (Bélgica)
Foro de Autoridades Iberoamericanas de Protección de Datos (AECID)	15 al 17 de mayo	Cartagena (Colombia)

Conferencia Blockchain Convergence	10 al 13 de noviembre	Málaga

Reunión	Fecha	Lugar
Grupo de trabajo Data Subjects Rights **Evento organizado por el CEPD con las partes interesadas sobre los derechos de los individuos según el Reglamento General de Protección de Datos de la UE**	5 de noviembre	Bruselas (Bélgica)
Conferencia Octopus **Evento organizado por el Consejo de Europa relacionado con la protección de datos en el entorno de la lucha contra el cibercrimen**	21 y 22 de noviembre	Estrasburgo (Francia)
Taller sobre Ética e inteligencia artificial	26 de noviembre	Bruselas (Bélgica)
Reunión con Director Fundamental Rights	24 de julio	Bruselas (Bélgica)
Grupo de trabajo Blockchain **Evento organizado por el Comité Europeo de Protección de Datos**	28 de marzo	Bruselas (Bélgica)

agencia española protección datos

www.aepd.es