agencia española protección datos

MEMORIA ANUAL

2023

prólogo

Me complace un año más presentar la Memoria anual de la Agencia Española de Protección de Datos, un documento en el que se puede encontrar el detalle de la actividad llevada a cabo por este organismo en todas sus áreas, un análisis de las tendencias más destacadas en materia de protección de datos y una exposición y valoración de los retos presentes y futuros.

Uno de los aspectos de mayor trascendencia es la contribución que ha hecho la Agencia para situar la protección de la infancia y adolescencia como un eje central y fundamental de las políticas públicas. El primer año de mi mandato, en 2015, creamos la Unidad de menores de la Agencia, conscientes de los grandes retos que teníamos por delante, y poco después creamos un grupo de trabajo transversal con expertos de áreas diversas para analizar el impacto que las tecnologías tienen en la salud, educación, vida familiar y social, privacidad y, en general, para el desarrollo integral de los menores.

Durante los últimos años hemos lanzado iniciativas que permitieran dar respuesta a situaciones excepcionalmente delicadas, como el Canal prioritario para solicitar la retirada urgente de contenidos sexuales o violentos publicados en Internet sin el consentimiento de las personas que aparecen en ellos. También en 2023 hemos seguido lanzando campañas y materiales de concienciación, varios de ellos en colaboración con otros organismos, de forma que tanto las familias como los centros docentes conozcan los riesgos asociados al mal uso las pantallas, Internet y las redes sociales y puedan convertirse en aliados para fomentar la educación y el espíritu crítico de los más jóvenes. En la actualidad nos hallamos ante un nuevo punto de inflexión para contribuir al desarrollo de hábitos saludables en Internet, encontrándonos en un marco multidisciplinar y proyecto de país especialmente propicio para tomar decisiones y llevar a cabo políticas públicas que permitan seguir dando pasos hacia una sociedad digital avanzada que protege a la ciudadanía y especialmente a su infancia.

En este sentido, las siguientes páginas recogen una amplia variedad de iniciativas de concienciación, difusión, colaboración e inspección. Una de las más destacadas ha sido la presentación del sistema de verificación de edad para proteger a los menores de edad ante el acceso a contenidos de adultos en Internet. Los principios desarrollados por la Agencia conjugan la protección a la infancia y el interés superior del menor con el derecho fundamental a la protección de datos de todos los ciudadanos, poniendo sobre la mesa una solución práctica, respetuosa y pionera en Europa.

El hecho de haber planteado un mecanismo que trate el atributo de la edad en el dispositivo del usuario, sin que la identidad de la persona ni su edad sea accesible para las páginas web o para los autodenominados "terceros de confianza" garantiza la privacidad de los adultos a la vez que impide la exposición temprana de los menores a unos contenidos que no son capaces de gestionar y que les afectan gravemente en sus conductas online, como ya señalan médicos y pediatras. Además, la atención que la Agencia presta a la protección de los menores en el ámbito digital ha llevado a diseñar una nueva estrategia reforzada en la que se agrupan las medidas que la Agencia está desplegando en sus actuaciones de 2024.

Las acciones mencionadas anteriormente se han puesto en marcha en paralelo a la gestión habitual de la Agencia, que puede consultarse en las siguientes páginas. Las memorias anteriores evidencian un incremento cuantitativo y cualitativo de la preocupación de la ciudadanía por la protección de sus datos, que se refleja en el volumen de reclamaciones planteadas ante la Agencia en los últimos años y, en particular, en el incremento de un 43% de las reclamaciones presentadas en 2023 respecto al año inmediatamente anterior, superando las 21.000. Así, por tercer año consecutivo, el número de reclamaciones recibidas ha sido el mayor de su historia. Esta situación no parece transitoria y está suponiendo nuevos retos de gestión para esta Agencia. Además, este importante aumento numérico en la carga de trabajo está acompañado de una mayor complejidad en su contenido, propiciada en gran medida por el avance tecnologías como la biometría, la inteligencia artificial o el big data. Por ello, se hace imprescindible ofrecer desde la Agencia recursos y materiales como los lanzados también este año, que facilitan el cumplimiento de la normativa a aquellos que tratan datos, así como la figura del traslado, que permite que el responsable del tratamiento ofrezca una respuesta más ágil al ciudadano de la que supondría la apertura de un procedimiento. En este sentido, es importante mencionar los más de 111.000 delegados de protección de datos notificados ante la Agencia, cuyo trabajo preventivo y de colaboración contribuye a mejorar la protección de la ciudadanía.

Por otro lado, es necesario hacer referencia a una de las iniciativas más innovadoras y relevantes en la que nos estamos adentrando: desarrollar propuestas para garantizar el tratamiento de los neurodatos en el marco del derecho a la protección de datos personales. Las neurotecnologías permiten el tratamiento de datos neurológicos o neurodatos y también permiten actuar sobre el sistema nervioso

y, aunque estos podrían tener distinta naturaleza, cuando están asociados a personas identificadas o identificables son datos personales.

Los neurodatos comparten características con los datos genéticos, ya que el cerebro es un identificador tan único como una huella dactilar o un genoma. Por ello, ya estamos trabajando en promover el reconocimiento normativo de los cinco neuroderechos propuestos en el ámbito internacional: la identidad personal, que protege la consciencia de la persona frente a los datos tecnológicos externos; el libre albedrío, que preserva la capacidad de las personas de tomar decisiones de forma libre y autónoma; la privacidad mental, que protege a las personas del uso de los datos obtenidos durante la medición de su actividad cerebral; el acceso equitativo, que busca la regulación para aumentar las capacidades cerebrales, de manera que no generen desigualdad en la sociedad y la protección contra los sesgos, para evitar que las personas sean discriminadas por cualquier factor, como pudiera ser un mero pensamiento. Esta área, junto con la protección de la infancia y la adolescencia en Internet, van a ser dos de las áreas prioritarias para esta Agencia en los próximos años.

Cada año finalizo este prólogo agradeciendo el trabajo realizado por los empleados públicos de esta Agencia. Es algo obligatorio y justo. Este organismo desempeña una labor que supone la garantía de un derecho constitucional que se enfrenta a indudables retos. Me consta la dedicación y el esfuerzo de todo el personal ya que, sin esos elementos, las acciones que se recogen en las siguientes páginas no hubieran sido posibles. Es un orgullo trabajar junto a un equipo tan comprometido, cohesionado y dispuesto a trabajar sobre los desafíos venideros.

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

Índice

Memoria 2023

Índice

Memoria 2023

Índice

Memoria 2023

Índice

Memoria 2023

Índice

Memoria 2023

La Agencia en cifras

1. Principales hitos de 2023

La Memoria del año 2022, partiendo de las implicaciones que ha generado la sociedad digital y, en particular, el modelo de negocio basado en la monetización de la información personal de los usuarios por parte de los prestadores de servicios de Internet, describió los principales hitos y riesgos que afectaban al derecho fundamental a la protección de datos y las iniciativas para garantizarlo y promover la confianza de los ciudadanos.

En la Memoria se destacó como una de las principales preocupaciones del actual entorno digital el relacionado con el acceso a los dispositivos móviles por parte de los menores, al periodo temporal en que los utilizan y a los servicios de Internet a los que acceden.

Es por ello que en esta Memoria ocupan un lugar destacado las iniciativas adoptadas para dar respuesta a esta situación.

Durante el año 2023 la AEPD ha tenido como objetivo prioritario el impulso de las reuniones del Grupo de Trabajo, lanzado en 2019, para la protección de los menores en el mundo digital "Menores, salud digital y privacidad", con la finalidad de abordar aquellas situaciones del uso de las TIC que afectan en su privacidad, bienestar y salud digital, en definitiva, a su desarrollo integral como personas, pues la protección de sus datos, de su privacidad es proteger su desarrollo.

Los menores de edad constituyen el colectivo de mayor uso de Internet, como se recoge en todos los estudios y encuestas, entre ellas la del Instituto Nacional de Estadística (INE) sobre el uso de Internet en los hogares de 2023 que indica que **el 90% de los menores de 10 años usan Internet, porcentaje que asciende al 98,3% a los 15 años.**

El Grupo de Trabajo ha centrado su labor durante 2023 en dos cuestiones principales: el uso problemático, o adictivo, de las pantallas, y el acceso a contenidos destinados a las personas adultas, en especial a la pornografía, cuyas consecuencias nocivas se han puesto de manifiesto, tanto por organizaciones de defensa de los derechos de los menores y su bienestar en el ámbito digital como por amplios sectores de la población que demandan actuaciones para hacer frente a los riesgos que comportan.

Los datos del tiempo y hábitos de uso de las pantallas y de los servicios y aplicaciones digitales que implica, igualmente puestos de manifiesto por distintas organizaciones y asociaciones, son preocupantes por las nocivas consecuencias que pueden producir y que, en personas vulnerables como los menores en pleno desarrollo de su personalidad, adquieren una mayor trascendencia.

Recientes estudios han advertido de que **el coeficiente intelectual de las nuevas generaciones está disminuyendo desde el cambio de milenio una media entre 2'5 y 4'3 puntos cada diez años.** El nivel de lectoescritura de los menores se ha visto afectado por el uso intensivo que realizan de los dispositivos electrónicos, que muestra un descenso en España de 7 puntos, los mismos que estamos por debajo de la media de la UE.

El último informe PISA incide en el descenso de la comprensión lectora de los alumnos respecto a la anterior edición de 2018, 3 puntos en España y 11 puntos en el ámbito de la OCDE, y de 8 puntos en matemáticas. Distraerse con los móviles supone perder la mitad de los conocimientos de un curso de matemáticas.

La UNESCO, en su Informe GEM (global Education Monitoring) 2023 sobre tecnología en la educación, recoge que el tiempo que los niños pasan frente a la pantalla ha aumentado, tanto con fines educativos como por ocio. Este incremento de tiempo puede afectar negativamente al autocontrol y a la estabilidad emocional, y aumentar la ansiedad y la depresión.

Estas circunstancias llevaron a la AEPD a proponer a las Administraciones educativas de su ámbito de actuación que valorasen la adopción de medidas de restricción o limitación del uso de dispositivos electrónicos en los centros escolares por los graves perjuicios que causan a la salud y a los resultados académicos de los menores, además de a la convivencia escolar. Propuesta que ha sido objeto de atención por las autoridades educativas.
El uso inadecuado o problemático y adictivo de Internet por los menores tiene unos efectos perjudiciales que afectan gravemente a su desarrollo personal, más en concreto a su salud (física, mental, psicosocial, sexual); su neurodesarrollo; su aprendizaje; la adquisición de las medidas cognitivas; las relaciones familiares y sociales; los hábitos de consumo; o la monetización de sus datos.

Además, la sobreexposición de información personal los hace más proclives a las situaciones de riesgo que el consumo intensivo de tecnología puede causar, como el ciberacoso, el sexting, o el grooming, con consecuencias en algunos casos lamentablemente irreparables.
Para hacer frente a este problema, la AEPD ha colaborado y difundido, a través de la campaña "Cambia el plan" y su traslado a las Administraciones Públicas competentes en la atención de los menores y sus familias, el Plan Familiar Digital de la Asociación Española de Pediatría, en el que se ofrecen orientaciones para prevenir, detectar y orientar a las familias ante conductas problemáticas y hacerles frente. Asimismo, ha establecido alianzas con organizaciones que velan por la salud y el bienestar digital de los menores como son los Consejos de Colegios Oficiales de Psicólogos y de Médicos.

En cuanto al **acceso online por los menores a contenidos para adultos, en especial a la pornografía** que, los estudios e informes de organizaciones especializadas señalan que se viene produciendo a edades muy tempranas de 9 años, y a gran escala, en un momento en el que su desarrollo cognitivo no les permite entender lo que están viendo, pues su personalidad no está formada, y genera importantes desórdenes en la concepción de las relaciones sexuales y del rol de la mujer.

A este respecto, la verificación de la edad para acceder a esos contenidos es uno de los elementos clave para proporcionar un entorno seguro y saludable de Internet a los menores, para lo que son necesarios sistemas que lo realicen de manera eficaz y plenamente respetuosos con los derechos y libertades de las personas, en particular con la protección de sus datos personales y su privacidad.

La AEPD, previas numerosas reuniones con diferentes organismos y entidades, ha adoptado un decálogo con los **principios que los sistemas de verificación de la edad han de aplicar**, de manera que los menores no accedan a esos contenidos sin que el sistema conozca ninguna información que pueda llegar a identificar o trazar al usuario. Principios cuya aplicación se ha probado con éxito a través de **pruebas de concepto realizadas por la Agencia con los principales sistemas operativos**.
El decálogo y las pruebas de concepto, junto con **la relación de FAQs** que se han elaborado para su mejor comprensión, fueron presentados el 14 de diciembre con motivo del 30º aniversario de la AEPD.

La atención que la Agencia presta a la protección de los menores en el ámbito digital ha llevado a apoyar la iniciativa por un **Pacto de Estado para la protección de los menores en el entorno digital**, promovida por relevantes entidades de la sociedad civil que defienden los derechos de la infancia y la adolescencia y el superior interés del menor, con la que se persigue el compromiso de todos los agentes involucrados para la adopción de medidas en los diferentes ámbitos de actuación.

Además, hemos diseñado **una nueva estrategia reforzada** que ha visto la luz ya en el mes de enero de 2024, en la que en torno a 3 ejes estratégicos de actuación se agrupan las medidas que la Agencia desplegará en su actuación en 2024.

2. Desafíos para la privacidad

La Memoria de 2022 planteó la necesidad de adoptar medidas que garantizaran una correcta interrelación entre el paquete digital de la Comisión Europea y, especialmente, la propuesta de Reglamento de Inteligencia Artificial.

Esta colaboración va a ser necesaria ya que el derecho a la privacidad y a la protección de los datos personales debe garantizarse durante todo el ciclo de vida del sistema de IA, manteniendo las autoridades de protección de datos sus competencias plenas en materia de protección de datos personales sobre los sistemas de inteligencia artificial.

En este sentido, la normativa de protección de datos se aplica a los sistemas de inteligencia artificial y, en especial, los principios de **minimización de datos y protección de datos desde el diseño y por defecto** cuando en los sistemas de inteligencia artificial se traten datos personales.

La interrelación entre ambas normas incide también en otros ámbitos como son el análisis de riesgos, las **evaluaciones de impacto** relativas a los derechos fundamentales que el Reglamento de IA establece como obligatorias para los sistemas que dicho considera de alto riesgo y las evaluaciones de impacto para la protección de datos o el concepto de **consentimiento informado** requerido en el Reglamento de IA como necesario para utilizar información de una persona en un sistema de IA que se va a someter a pruebas reales y el **consentimiento** del RGPD necesario para tratar sus datos personales en el sistema de inteligencia artificial. Tanto la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE) como las opiniones del SEPD (apartado II.5 de la Guía de Necesidad del SEPD) exponen que la evaluación de impacto de una normativa con relación a la protección de datos debe realizarse en los casos en que la medida legislativa propuesta implique el tratamiento de datos personales. Cualquier operación de tratamiento de datos prevista por la legislación supone una limitación del derecho a la protección de los datos personales, independientemente de que dicha limitación pueda estar justificada.

En relación con la evaluación de impacto para la protección de datos en el desarrollo normativo la Agencia publicó unas orientaciones para identificar en qué casos debe realizarse la evaluación de impacto, cómo debe realizarse en caso afirmativo identificando el rango adecuado de la norma, evaluando las limitaciones y riesgos para los derechos y libertades, su finalidad, idoneidad y necesidad, la proporcionalidad de las medidas, así como las medidas que deben plantearse para superar los riesgos sobre los derechos de los afectados.

Adicionalmente, ha propuesto que en todos los proyectos de disposiciones de carácter general se analicen sus implicaciones en la protección de datos recogiéndose en una disposición incluida en la norma, previsiones que faciliten su aplicación en este ámbito.

La relevancia que el Reglamento General de Protección de Datos (RGPD) atribuye a la figura del Delegado de Protección de Datos (DPD) ha exigido una conducta activa por parte de las Autoridades con la finalidad de analizar su situación en el ámbito público y privado y proponer medidas dirigidas a garantizar un adecuado desarrollo de sus funciones.

A este respecto, la Agencia ha participado en la acción europea coordinada para realizar la designación y situación de los Delegados de Protección de Datos que ha concluido con un informe en el que se formulan recomendaciones sobre su designación, conocimiento y experiencia; sus tareas y recursos y su posición en el marco de las organizaciones en las que prestan sus servicios con el fin de dar respuesta a las relevantes deficiencias que se han apreciado.

En el mismo sentido, la Agencia ha promovido encuentros con Delegados de Protección de Datos de las entidades locales que han permitido conocer su situación y promover buenas prácticas en este sector.

Complementariamente, diversos informes del Gabinete Jurídico han señalado los criterios que deben cumplirse sobre la necesidad de garantizar su autonomía organizativa, sobre los recursos que le permitan desarrollar su labor de manera efectiva, sobre la exigencia de evitar que en el desarrollo de las funciones que tiene atribuidas por parte del responsable se produzca un conflicto de intereses que afecte a su necesaria independencia y sobre las circunstancias que puedan concurrir para su posible remoción.

En cuanto a las implicaciones de las iniciativas de espacios de datos, con el fin de promover mayores niveles de seguridad jurídica en relación con el tratamiento de datos personales, la Agencia ha publicado el documento **Aproximación a los espacios de datos desde la perspectiva del RGPD**, en el que se recoge una descripción del marco normativo aplicable, la metodología para la identificación de los riesgos que pueden generarse y la realización de impacto que los aborde, se identifican los distintos agentes intervinientes en ellos y su posición jurídica en el marco del RGPD y se analizan las bases jurídicas y el ejercicio de derechos de protección de datos, así como las garantías para las transferencias internacionales de datos.

La AEPD está abordando como una de sus iniciativa más innovadoras y relevantes desarrollar propuestas para garantizar el tratamiento de los neurodatos en el marco de la normativa reguladora del derecho fundamental a la protección de datos personales, ante la ausencia de una regulación específica sobre esta materia.

Las neurotecnologías permiten el tratamiento de datos neurológicos o neurodatos y también permiten actuar sobre el sistema nervioso humano. Los neurodatos recogidos mediante neurotecnologías podrían tener distinta naturaleza. Sin embargo, en cuanto estén asociados a personas identificadas o identificables, son datos personales.

Es por ello que los riesgos asociados al tratamiento de neurodatos reclaman una atención específica respecto a la interpretación de su tratamiento con relación al RGPD.

Adicionalmente es necesario promover el reconocimiento normativo de los cinco neuroderechos propuestos en el ámbito internacional como son los de identidad personal, libre albedrío, privacidad mental, acceso equitativo y protección contra los sesgos.

Por último, debe hacerse una referencia a que los datos sobre reclamaciones presentadas que se recogen en las memorias de la Agencia de los últimos años ponen de manifiesto que la magnitud de los datos personales objeto de tratamiento y la evolución constante de las tecnologías que se utilizan para su tratamiento, evidencian un incremento cuantitativo y cualitativo de la preocupación de los ciudadanos que se ha reflejado en el volumen de reclamaciones planteadas ante la Agencia de Protección de Datos en los últimos años y en particular en el incremento de un 43% en el año 2023 respecto al año inmediatamente anterior.

La necesidad de seguir generando la confianza de los ciudadanos se ha traducido en la adopción por parte de la Agencia de nuevas medidas organizativas y en la propuesta de iniciativas legislativas para garantizar este derecho fundamental.

2.1 Jurídicos

2.1.1 Consultas

En el año 2023 la actividad del Gabinete Jurídico se ha centrado principalmente en la emisión de informes preceptivos sobre disposiciones legales y reglamentarias, así como aquellos otros asuntos de carácter general en materia de protección de datos que, dada su relevancia hacían necesario el pronunciamiento de esta institución.

En efecto, sobre la elaboración de disposiciones legales y reglamentarias, se sigue insistiendo en la necesidad de que por el órgano proponente de la norma que se trate, se realice y se incorpore a esta, el análisis de riesgos y en su caso, la evaluación de impacto normativo y que dicha incorporación se haga o bien en la propia norma o bien a través de disposiciones adicionales, o bien se incorpore en la memoria de análisis de impacto normativo.

Este mandato que se hace desde la AEPD es una llamada al cumplimiento del principio de responsabilidad activa del responsable del tratamiento, que requiere una intervención activa del Delegado de Protección de Datos en las Administraciones Públicas, a través de su intervención en la elaboración de disposiciones generales. En definitiva, se pretende que las disposiciones normativas incorporen, adaptándose al caso concreto, una regulación específica en materia de protección de datos.

No obstante, debe destacarse que esta insistencia en pasados ejercicios no ha sido en vano y en la actualidad se han aprobado disposiciones de carácter general cuyos proyectos y anteproyectos fueron informados por el Gabinete Jurídico, y que tienen su propia regulación en materia de protección de datos.

En este sentido procede citar la Ley Orgánica 11/2021, de 28 de diciembre, de lucha contra el dopaje en el deporte, (Disposición adicional cuarta); la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual, (DA cuarta); la Ley 20/2022, de 19 de octubre, de Memoria Democrática, (DA décima); la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, (Título VI, arts. 30 y 32); la Ley 3/2023, de 28 de febrero, de Empleo, (artículo 16); o la Ley 7/2023, de 28 de marzo, de protección de los derechos y el bienestar de los animales, (artículo 10, apartados 2, 4, 5, 6, 7, y artículo 12).

Por otra parte, destaca la labor del Gabinete Jurídico en la elaboración de la Circular 1/2023, de 26 de junio, sobre la aplicación del artículo 66.1.b) de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones, para lo que se emitieron los Informes 40/2023 y 52/2023. Esta Circular se hacía necesaria tras la entrada en vigor dicha regulación un año después de su aprobación, el 29 de junio de 2023 y que recogía el derecho de los usuarios a no recibir llamadas con fines de comunicación comercial no solicitadas, salvo que existiera consentimiento previo del propio usuario para recibir este tipo de comunicaciones o que estas puedan ampararse en otra base de legitimación de las previstas en el RGPD. En la Circular, entre otras cuestiones, se recogen los requisitos del consentimiento y se aborda una pormenorizada regulación del interés legítimo como supuesto legitimador de este tipo de tratamientos, recordándose que, en todo caso, se debe dar cumplimiento al principio de transparencia en relación con el derecho a la información del titular de los datos que van a ser objeto de tratamiento.

En cuanto a otras materias en las que el Gabinete Jurídico ha intervenido expresando el criterio de la AEPD, procede citar los siguientes informes agrupados por materias:

Comenzando por la figura del Delegado de Protección de Datos (DPD) y las políticas de protección de datos procede citar los Informes 34/2023 y 38/2023.

En el **Informe 34/2023** se somete a criterio de la AEPD el Proyecto de Decreto del Consell de Islas Baleares por el que se aprueba la Política General, Estructura Organizativa y Asignación de funciones en materia de Protección de Datos en la Administración del Consell y su Sector Público Instrumental. Se aborda por un lado la naturaleza y el contenido que deben tener las políticas de protección de datos y por otro, la estructura en la que se incardina la figura del DPD.

El informe parte de la doctrina sobre del reparto competencial entre el Estado y Comunidades Autónomas y el límite del contenido esencial del derecho fundamental a la protección de datos, indicando que la norma sometida a informe "únicamente podrá regular aspectos derivados del desarrollo normativo y de la ejecución y aplicación del RGPD y la LOPDGD en su ámbito de actividad, sin que en ningún caso sea conforme al rango de ley exigido (artículo 81.1 de la Constitución) y al reparto competencial que entren a regular aspectos esenciales del contenido del derecho fundamental."

A la vista del contenido de la norma proyectada se recuerda que lo que exige el RGPD con relación a las políticas de protección de datos es el aspecto

efectivo, práctico y ejecutivo de un conjunto de directrices, yendo más allá de la referencia al aspecto formal de la existencia de un documento llamado "política de protección de datos" donde se realiza la mera reproducción formal del articulado del RGPD y se reduce a una mera declaración de la voluntad de compromiso del responsable con el cumplimiento normativo. Por eso se pone de manifiesto que la "política de protección de datos" no debe ser una reproducción del RGPD o únicamente una declaración formal de asunción de compromisos de cumplimiento normativo. Y en cuanto al DPD, se parte de la obligación del responsable del tratamiento de, en virtud de su autonomía organizativa establecer la estructura que estime adecuada para garantizar el cumplimiento de las disposiciones del RGPD relativas al nombramiento, posición jurídica y funciones que corresponden al DPD, quien deberá contar con la autonomía y los recursos suficientes para desarrollar su labor de forma efectiva.

Por eso, una vez analizadas las funciones del DPD y de aquellos departamentos que forman parte del responsable del tratamiento, el informe concluye que dentro de la libertad que confiere la potestad autoorganizativa de la administración pública, nada obsta a que se determine en la estructura que conforma el responsable del tratamiento, otros niveles o departamentos que puedan participar en la determinación de los fines y de los medios del tratamiento y que en cierta medida asesoren y propongan al responsable la adopción de las medidas que estimen adecuadas, pero siempre tendrán que estar perfectamente diferenciadas de las del Delegado de Protección de datos, para así evitar que se confundan con las propias de asesoramiento de éste.

En la misma línea, el **Informe 38/2023** se abordan una serie de cuestiones relacionadas con la posición jurídica del DPD, recordando que la asignación de otras tareas al DPD deberá respectar, en todo caso, el carácter asesor y supervisor de este, sin que puedan implicar la intervención directa en la toma de decisiones referidas a los fines y medios del tratamiento, que afectaría a su independencia e implicarían la existencia de un conflicto de intereses. De este modo, la necesaria independencia del DPD y la necesidad de evitar los conflictos de intereses impide asignarle responsabilidades directas en un ámbito que va a tener que supervisar y en el que estaría sujeto a instrucciones de otros órganos.
Todo ello en línea con el criterio del Tribunal de Justicia de la Unión europea sobre la posición jurídica del DPD y la necesaria garantía de su independencia funcional en la Sentencia de 22 de junio de 2022, asunto C-534/20, Caso Leistritz AG contra LH y en la ya citada Sentencia de 9 de febrero de 2023, asunto C-453/21 Caso X-FAB Dresden GmbH & Co. KG contra FC.

Por último, el informe pone de manifiesto un aspecto esencial en la relación del DPD con la entidad a la que asesora y que resulta necesario aclarar, al indicar que "el empresario conserva los poderes que le otorga la normativa laboral para el adecuado cumplimiento y control del contrato de trabajo, que solo se ven modulados en la medida necesaria para garantizar la independencia funcional del DPD, pudiendo ejercerlos dentro del respeto a dicha independencia y de forma que la misma no se vea perjudicada y teniendo en cuenta que, conforme al artículo 36.2 de la LOPDGDD el DPD no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio." (…) lo que no obsta a que el DPD pueda ser removido o sancionado en caso de incurrir en dolo o negligencia grave en el ejercicio de sus funciones."

La entrada en vigor de la anteriormente citada Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, ha suscitado varias consultas en materia de protección de datos resueltas a través de los informes 54/2023, 60/2023 y 77/2023.

En el **Informe 54/2023** se resuelve una consulta que plantea si el órgano de gobierno de cada u órgano de administración de cada entidad sometida a dicha ley, debe ser considerado

responsable del tratamiento en los términos de su artículo 5.

El informe indica que en el sector público, la condición de responsable del tratamiento corresponderá a la entidad u organismo obligado por la ley y no a su órgano de gobierno, sin perjuicio de que en este ámbito sea una práctica frecuente en la elaboración de los registros de las actividades de tratamiento, la de identificar como responsable del tratamiento al órgano superior o directivo que ostenta las correspondientes competencias, contribuyendo, de este modo, a facilitar la identificación del órgano administrativo que adopta las correspondientes decisiones sobre el tratamiento de los datos personales y el ejercicio de los derechos de los afectados, práctica admitida y seguida por esta Agencia, pero sin que excluya la condición de responsable del tratamiento de la entidad u organismo correspondiente.

Por todo ello, la correcta interpretación del artículo 5 de la Ley 2/2023, de 20 de febrero, desde la perspectiva de la protección de datos personales, requiere identificar como responsable del tratamiento a la entidad u organismo obligado por la ley a disponer de un sistema interno de información, sin perjuicio de que las decisiones necesarias para su correcta implantación deban adoptarse por el correspondiente órgano de administración u órgano de gobierno.

En el **Informe 60/2023** se somete al criterio del Gabinete Jurídico los modos y plazos de conservación de los datos de carácter personal que hayan sido objeto de tratamiento como consecuencia de aplicación de la citada ley, y su coexistencia con aquellas normas que prevén distintas posibilidades de conservar determinada información, como las que se derivan del artículo 31 bis.2 y artículo 31 quarter.1, letra d) del Código Penal.

De la norma se deduce la existencia de dos espacios perfectamente diferenciados con un régimen distinto en términos cualitativos y cuantitativos.

Por un lado, el Sistema Interno de Información, dónde los plazos de conservación de la información son como máximo de tres meses si no se han iniciado las actuaciones correspondientes, y, si se han iniciado las actuaciones, deberá estarse a los plazos del "procedimiento" que tramite el sujeto obligado y que, si bien no se indica expresamente en la ley, de sus preceptos se puede deducir, en principio, que es de seis meses en determinados casos artículo 9. 2 d). En cualquier caso, tanto si no se han iniciado las actuaciones como si se han llevado a cabo, una vez transcurridos los plazos indicados, los datos personales deberán suprimirse del sistema, salvo que se conserven de manera anonimizada a los efectos de acreditar la existencia y funcionamiento del sistema, por ejemplo, ante la Autoridad Independiente de Protección del Informante.

Y, por otro lado, el libro-registro que contiene tanto las informaciones recibidas como las actuaciones realizadas, y cuyo acceso se encuentra más limitado, la propia norma indica que no es público, y únicamente se podrá acceder a petición razonada por la autoridad judicial competente, siendo los plazos de conservación los estrictamente necesarios para cumplir con la ley, y en todo caso de diez años como máximo.

Finalmente, estas obligaciones de conservación y supresión no impedirían que el responsable del tratamiento, a los efectos de poder ejercer con todas las garantías los derechos previstos en el artículo 24 de la Constitución, en un hipotético procedimiento penal, en relación con lo dispuesto en el artículo 31 bis 2 y artículo 31 quarter 1. d) del Código Penal, pueda conservar en un espacio ajeno y distinto a los que se derivan de la Ley 2/2023 de 20 de febrero, aquella información que resulte necesaria a tal fin, precisamente para cumplir con las finalidades que justificarían dicho tratamiento con arreglo a otras leyes que también les obligan. Lo que no libera al responsable de cumplir con la normativa de protección de datos, en el sentido de que necesitara la correspondiente base jurídica para otra finalidad, y en especial deberá tener en cuenta, aquellas obligaciones relacionadas con la transparencia del tratamiento, como por ejemplo, incluir ese tratamiento posible en el Registro de Actividades de Tratamiento (artículo 30 RGPD) y en su caso en el Inventario de Actividades de Tratamiento (artículo 31.2 LOPDGDD), así como el cumplimiento del principio de minimización,

tanto en su aspecto cuantitativo como temporal y sobre todo, a analizar y evaluar los riesgos asociados a este tipo de tratamiento tal como se deduce del articulo 28.2 c) de la LOPDGDD.

Por último, en el **Informe 77/2023** se aborda la posibilidad de tratar datos personales que se contengan en las informaciones recibidas en el marco del procedimiento de información de la Ley 2/2023, y que no superen el trámite de admisión por no estar bajo su ámbito de aplicación. Pero a diferencia de lo resuelto en el anterior informe, no se refiere su posterior uso al ejercicio de determinados derechos, sino al amparo del artículo 112 de la Ley 40/2015 de 1 de octubre del Régimen Jurídico del Sector Público. La consultante es la Sociedad Estatal Correos y pretende legitimar el uso de dicha información para cumplir el objetivo de "perseguir la eficiencia, transparencia y buen gobierno de las sociedades mercantiles".

La respuesta del Gabinete Jurídico es negativa, por cuanto que dicho artículo 112 no prevé, ni directa ni indirectamente la injerencia que supondría en el derecho fundamental a la protección de datos y tampoco justifica la obligación legal o el interés público que justificarían un tratamiento de datos personales diferente al previsto por la propia ley 2/2013, y obviamente tampoco se establecen garantías o límites de ninguna clase en la norma para el tratamiento concreto que se propone. El informe también analiza la posible concurrencia de un hipotético interés legítimo como base legitimadora para concluir desechando esta posibilidad, en la medida en que "difícilmente un hipotético informante que acude al Sistema interno de información, revestido por la ley de notas de confidencialidad y anonimato, puede esperar razonablemente que la información que aporta pueda usarse para otra finalidad como la que pretende la consultante."

El informe concluye que el nuevo tratamiento no encontraría base jurídica suficiente y tendría una finalidad incompatible con la inicial.

Otro aspecto con una evidente incidencia en materia de protección de datos son los sistemas de prevención del fraude, respecto de los que en el presente ejercicio se ha emitido el Informe 18/2023, que actualiza el régimen jurídico al que se somete el Fichero Confirma respecto de varios aspectos, como el rol que desempeñarían las entidades adheridas a dicho sistema y los nuevos tipos de anotaciones en relación con el cumplimiento de los principios del RGPD.

En lo que se refiere a los principios de protección de datos, se aborda el principio de licitud en los Informes 7/2023 y 70/2023 y que se refieren a las bases jurídicas que legitiman los requerimientos realizados por autoridades y que implican tratamiento de datos personales.

En el **Informe 7/2023** se analiza la solicitud de información que realiza la Dirección General de Ordenación del Juego (DGOJ), de la Secretaria General de Consumo y Juego, del Ministerio de Consumo, a la Real Federación Española de Fútbol (RFEF) al amparo de la Ley 13/2011, de 27 de mayo, de regulación del juego (LRJ).

La RFEF considera que cumplir el requerimiento de información puede contravenir el RGPD ya que podría ser contrario a los principios de licitud, finalidad y minimización.

El requerimiento hace referencia a "la identificación de todos los miembros que a fecha de contestación del presente requerimiento tengan 18 años o más y que formen parte del cuadro directivo, plantilla de jugadores y cuadro técnico (entrenador, asistentes, utilleros…), de las entidades deportivas adscritas a los cinco grupos de la categoría Segunda Federación de Fútbol durante la temporada 2022/2023. Dicha información, que se ha de reportar en formato Excel, contendrá al menos los siguientes): Equipo, Grupo, Nombre y Apellidos, NIF, Licencia, Domicilio y localidad, Tipo de vinculación (jugador, entrenador, directivo…)" El informe indica que, los requerimientos objeto de análisis no se realizan por una obligación legal aplicable al responsable del tratamiento, a la DGOJ, sino que se llevan a cabo en el ejercicio de las competencias que atribuyen a ésta los artículos 21 y 24 de la LRJ en relación con el artículo 6.2 de la misma norma.

En consecuencia, el tratamiento de los datos derivado del requerimiento que realiza la DGOJ a la RFEF encuentra su legitimación en el artículo 6.1 e) del RGPD y articulo 8.2 de la LOPDGDD siendo la norma que atribuye la competencia la LRJ.

Desde la perspectiva de la RFEF, atender al requerimiento y, por tanto, el tratamiento de datos derivado del mismo encuentra su legitimación en el artículo 6.1 c) del RGPD y el artículo 8.1 de la LOPDGDD, en consonancia con el deber genérico de colaboración que se desprende del artículo 18 de la Ley 39/2015 de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

En cuanto a los principios de minimización y limitación de la finalidad, se trae a colación el criterio mostrado en otros informes sobre los requerimientos de determinados organismos de supervisión y control a los obligados por la norma que le sea de aplicación -Agencia Estatal de la Administración Tributaria (por todos los Informes 369/2015 y 98/2016), la Agencia Española del Medicamento y Productos Sanitarios (Informe 59/2021) ,el Tribunal de Cuentas (Informe 28/2022) en el ámbito autonómico, la Sindicatura de Cuentas de Islas Baleares (37/2022)- siendo el criterio generalizado que el elemento delimitador es la utilidad del requerimiento, en el sentido si resulta útil para cumplir la finalidad que se deriva de los preceptos que atribuyen las funciones y competencias a dichos organismos. Dicho de otro modo, si los datos que van a ser objeto de tratamiento tienen trascendencia en relación con el propósito que se persigue.

Y se recuerdan las características concretas que deben revestir dichos requerimientos (Informe 59/2021 y STC17/2013): (i) habrá de evitarse el acceso indiscriminado y masivo a los datos personales (ii) el dato en cuestión solicitado habrá de ser pertinente y necesario (iii) para la finalidad establecida en el precepto (iv) la solicitud de acceso a los concretos datos personales habrá de motivarse y justificarse expresamente, (v) de manera que ello posibilite su control por el cedente (vi) y se evite un uso torticero de esa facultad con accesos masivos. Ello supone (vii) que ha de quedar garantizada la posibilidad de analizar si en cada caso concreto el acceso tenía amparo en lo establecido en la ley. Tras el exhaustivo análisis el informe concluye que los requerimientos de la DGOJ realizados a la RFEF son conformes a los principios de licitud, limitación de finalidad y minimización.

En el **Informe 70/2023** se plantea una consulta conjunta por los Delegados de Protección de Datos del Banco de España (BE) y la Agencia Estatal de la Administración Tributaria (AEAT), referida a la posibilidad de que en el procedimiento de recaudación -y en concreto ejerciendo la posibilidad del aplazamiento o fraccionamiento- instruido por la AEAT pueda solicitar al BE el informe de la Central de Información de Riesgos del Banco de España, CIRBE, que haga referencia al obligado al pago en dicho procedimiento, en relación a cuál sería la base jurídica de legitimación de dicho tratamiento de datos.

El informe señala que un hipotético acceso al informe de la CIRBE se basaría en el artículo 6.1 e) RGPD y articulo 8.2 LOPDGDD, por referirse al el ejercicio de competencias propias y que son necesarias para cumplir con una misión de interés público, y no en el consentimiento del interesado como proponen los consultantes, por mucho que el artículo 46.3 c) del Reglamento General de Recaudación, prevea una cláusula abierta en la que se podría incardinar la aportación del informe del CIRBE al indicar que en la solicitud de aplazamiento o fraccionamiento se deberá acompañar: c) los demás documentos o justificantes que estime oportunos (el interesado). La existencia de esa facultad en el interesado no elimina la existencia de una relación de sujeción que impide un consentimiento libre.

En segundo lugar, se aborda la aplicación del artículo 28.2 de la Ley 39/2015 de Ley 39/2015, de 1 de octubre, (LPACAP) para legitimar un hipotético acceso, ya que los consultantes lo plantean como una obligación legal. El informe rechaza ese planteamiento y reitera que la actuación de la administración como consecuencia de la aplicación del artículo 28.2 LPACAP, en cuanto a la normativa de protección de datos, se realiza al amparo del artículo 6.1 e) del RGPD y no en el cumplimiento de una obligación legal del articulo 6.1 c) RGPD.

No obstante, el informe concluye que, "para el tratamiento concreto, en coherencia con la regulación de la Ley de Medidas de Reforma del Sistema Financiero sobre la CIRBE, se debería acreditar la existencia de la autorización del interesado, -que no consentimiento al que se refiere la normativa de protección de datos- y la base jurídica que legitimará a la AEAT para acceder al informe de la CIRBE será la prevista en el artículo 6.1 e) del RGPD. Y recalca que tanto la aportación de la información que consta en el CIRBE por parte del interesado a la AEAT, como la citada autorización, debe surgir de la disposición libre del interesado que, en coherencia con la LMRSF, es el único titular del derecho de acceso y cuyo ejercicio pasa obviamente por su voluntariedad. (…) el interesado ha de decidir libremente dar su autorización al acceso a dichos datos, sin necesidad de ser inducido, sugerido o "recordado" a ello. (…)"

En cuanto a las categorías especiales de datos, destacan los informes 41/2023 y 55/2023 en los que se aborda el acceso a la historia clínica.

En el **Informe 41/2023** se resuelven una serie de cuestiones relacionadas con la legitimación para el tratamiento de datos personales mediante el intercambio de información de la historia clínica de los trabajadores entre los médicos del servicio público de salud (SPS) y los médicos de las Mutuas de Accidentes de Trabajo.

El informe tras analizar los requisitos para tratar categorías especiales de datos y la doctrina del Tribunal Constitucional al respecto (STC 76/2019 de 22 de mayo), aborda la legislación que regulan los tratamientos de salud a los que se refiere la consulta, partiendo del art. 71.3 del texto refundido de la Ley General de la Seguridad Social, aprobado por Real Decreto Legislativo 8/2015, de 30 de octubre, (TRLGSS).

Se recuerda que la Agencia en sus informes 39/2022 y 42/2022, relativos a los proyectos de disposiciones reglamentarias que desarrollan dicho precepto, considera que la Administración de la Seguridad Social, al poder recabar para esos fines la historia clínica de los trabajadores, y regularse esta en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente (LAP) está sujeta a las salvaguardas y garantías establecidas en la propia ley 41/2002 para su uso. Esta consideración permitiría salvar la circunstancia de que el art. 71.3 TRLGSS no establece, en sí mismo, estas garantías para los tratamientos de datos personales que se lleven a cabo para el cumplimiento de estos fines.

A lo que añade que ya en el Informe 101/2019, analiza la posibilidad de que, por parte de los servicios de Inspección Médica de la Comunidad Autónoma de Canarias, pueda accederse a las historias clínicas tanto de atención primaria como de atención especializada a los efectos realizar sus funciones de verificación control, confirmación y extinción de la incapacidad temporal y en el mismo se hace un especial análisis de las garantías contenidas en la Ley 41/2002.

Por lo que, una vez analizado el marco legal aplicable a los accesos a la historia clínica en los procedimientos de incapacidad temporal, se hace referencia a la naturaleza jurídica de las mutuas y su condición en relación con los tratamientos de datos personales, partiendo del artículo 80 del TRLGSS.

Afirmándose que la legitimación para el tratamiento propuesto se encontraría, tal y como ha reconocido expresamente el legislador en los artículos 6.1. e) y 9.2 h), del RGPD Ahora bien, dicha legitimación no permite un intercambio de la información que forma parte de la historia clínica como el que se pretende en la consulta, ya que, los tratamientos de datos de salud deben realizarse en los términos y con observancia de las limitaciones y garantías específicas recogidas en las normas legales que los legitiman, que no han previsto dicho intercambio generalizado, facultando el acceso a las historias clínicas, con carácter general, a las entidades gestoras y a la inspección médica. Y se advierte que un tratamiento como el pretendido también podría ser contrario a los principios recogidos en el artículo 5 del RGPD. En este sentido, ya existen precedentes de sanciones impuestas por esta Agencia como consecuencia

de la infracción de dichos principios en casos análogos al planteado, como el PS/00262/2021, en el cual se sancionó a un centro médico que facilitó a una mutua datos de salud previos a la realización de la prueba que había realizado a instancia de la mutua, por infracción del principio de confidencialidad del artículo 5.1.f) del RGPD. Cuestión distinta es cuando, atendiendo a las circunstancias del caso concreto, existe una vinculación y ese acceso se produce a través del Servicio de Inspección Médica, tal y como se razona en la Sentencia de la Audiencia Nacional de 20 de septiembre de 2020 (Recurso 186/2019).

El **Informe 55/2023** tiene por objeto el tratamiento consistente en que el Servicio de Prevención de Riesgos Laborales de los empleados públicos de la Administración Pública de la Región de Murcia pueda acceder a las historias clínicas de éstos con el fin de desarrollar diferentes actividades.

El informe comienza diferenciando la historia clínica laboral y la historia clínica "ordinaria" y las finalidades que persiguen cada una. Para a continuación analizar la normativa nacional y autonómica que regula el acceso a la historia clínica, concluyendo que, "con carácter general, la finalidad del uso de la historia clínica responde a la función asistencial que los médicos de atención primaria y especializada llevan a cabo. Fuera de esta finalidad, los distintos usos o excepciones que prevén las normas citadas están tasados (apartados 3 y 5 del artículo 16 LAP y apartados 4 y 5 del artículo 55 de la ley autonómica) y en ninguno de ellos se identifican a los Servicios de Prevención de Riesgos laborales como potenciales destinatarios de la misma. A lo que hay que añadir que el tratamiento de los datos de salud de la historia clínica debe respetar la intimidad, la confidencialidad y la protección de datos de carácter personal y cualquier acceso a dicha información debe estar previsto en la ley". No obstante, se recuerda lo indicado en el Informe 362/2010 en el que se señala que "Por otra parte, las limitaciones establecidas por el citado artículo 16 no implican necesariamente que los datos de la historia clínica puedan ser únicamente objeto de acceso en los supuestos allí enumerados, sino que podría ser admisible una cesión en caso de contarse con otra norma con rango de Ley que la habilitase. ", por lo que se acude a la normativa de aplicación a los Servicios de Prevención de riesgos laborales, para ver si en la misma se encuentran los tratamientos que propone la consultante y que impliquen necesariamente el acceso a la historia clínica ordinaria o convencional. La respuesta es negativa y se añade que de proceder como pretende la consulta "estaríamos ante el hipotético supuesto en que una persona acude al médico para una finalidad determinada y con posterioridad, esa información seria utilizada por los Servicios de Prevención del empleador de dicho paciente, incluso en el caso de que éste en su entorno laboral hubiera declinado la opción de realizarse el reconocimiento médico. Ninguna expectativa de privacidad ni previsibilidad del tratamiento haría formarse al titular de los datos cuando acude a la consulta o a una prueba determinada en relación con el tratamiento posterior que pretende la consultante."

El informe concluye que el tratamiento de datos analizado "no cumple el principio de licitud por resultar un tratamiento de categorías especiales de datos sin observar lo dispuesto en los artículos 9 y 6 del RGPD (…) y también resultaría contrario e incompatible con la finalidad del tratamiento inicial. Por tanto, tampoco se cumple el principio de limitación de finalidad."

También hay que destacar el Informe 43/2023 que, si bien no trata de categorías especiales de datos, se centra en el posible tratamiento de datos de naturaleza penal o policial y de infracciones administrativas, que tienen un régimen especial de tratamiento.

La consulta plantea si es conforme a la normativa sobre protección de datos personales la comunicación de datos relativos a antecedentes policiales de los progenitores de menores de edad a los equipos técnicos de la Administración competente a efectos de valorar si puede existir un riesgo social para el menor o una situación de desamparo.

Se considera necesario para que proceda la comunicación de dichos datos, además de que esté prevista por el Derecho de la Unión Europea o por la legislación española, que se valore si no

se perjudican los fines para los que se mantienen los datos en los ficheros policiales o se desvirtúen las concretas garantías que la Ley Orgánica 7/2021 establece.

En consecuencia, se analiza si el tratamiento propuesto se encuentre contemplado en una norma con rango de ley que contenga garantías específicas. La respuesta es afirmativa al acudir a lo dispuesto en el artículo 22 quater de la Ley Orgánica 1/1996 de 15 de enero de Protección Jurídica del Menor en el que se incluyen las salvaguardas que propuso el propio Gabinete Jurídico en el informe emitido a raíz de la tramitación de la modificación legislativa que introduce el precepto (Informe 195/2014) y se indica que dicho régimen de garantías se complementa, además, por el deber genérico de reserva recogido en el artículo 13.3 de la citada Ley Orgánica.

Ahora bien, el informe concluye que "la previsión legal del art. 22 quater de la Ley Orgánica 1/1996 no supone una habilitación genérica para la comunicación a la autoridad administrativa autonómica de todos los datos personales que puedan figurar en los ficheros policiales respecto del progenitor de un menor incurso en un procedimiento de posible declaración de la situación de desamparo, sino únicamente de aquellos datos que sean estrictamente necesarios en el seno del procedimiento tramitado por la autoridad autonómica para la adecuada protección de los menores por los poderes públicos mediante la prevención, detección y reparación de situaciones de riesgo, con el ejercicio de la guarda y, en los casos de declaración de desamparo, para la asunción de la tutela por ministerio de la ley.

(…) el requerimiento de tales datos por la Administración competente solamente podrá efectuarse cuando exista una situación comprobada de riesgo de exclusión social o desamparo del menor, lo que deberá ser suficiente y expresamente motivado y razonado por la Administración requirente (…) y estará sujeto al principio de minimización (…) sin que se ampare las cesiones masivas de datos, quedando limitada a los datos necesarios para la determinación de la medida o medidas que en favor del menor en situación de exclusión o de riesgo vayan a aplicarse.(…) y estrictamente al principio de finalidad, sin olvidar el régimen de responsabilidad proactiva que implicará que la administración receptora de la información "deberá garantizar la aplicación de las medidas técnicas y organizativas que resulten de la correspondiente evaluación de impacto en la protección de datos, en los términos previstos en el artículo 3 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad."

Otro informe que merece especial atención por la naturaleza de los titulares de los datos objeto de tratamiento, es decir, menores de edad y el contexto, plataformas digitales en el ámbito educativo,

es el **Informe 50/2023** que se emite a raíz de la consulta del Ministerio de Educación, Formación Profesional, sobre **la adecuación al marco jurídico vigente del Convenio** entre INTEF (Instituto Nacional de Tecnologías Educativas y de Formación de Profesorado) y Google para el uso de las herramientas de "Workspace for Education" en los Centros Educativos de Ceuta y Melilla.

El informe analiza varias cuestiones, unas estrictamente referidas al derecho a la protección de datos, y otras que, si bien tratan más de cuestiones relativas al derecho civil, referida a la validez y requisitos de los contratos, van a tener incidencia al menos de manera indirecta en la aplicación de la normativa de protección de datos.

Comenzando por estas últimas, el informe pone de manifiesto las carencias informativas en el contrato sobre aspectos esenciales y se rechaza la circunstancia de que haya que acudir a distintos sitios web para que el responsable conozca elementos fundamentales referidos al objeto del contrato, en qué consisten los servicios que forman parte de éste, el tipo de datos que se recogen o el detalle de las finalidades que se persiguen.

Asimismo, se pone de manifiesto que el Convenio permite modificar los servicios concretos al supuesto encargado del tratamiento, a Google, y que la interpretación del acuerdo en lo que se refiere a protección de datos se somete a un documento cambiante a voluntad de Google.

También al analizar las finalidades de los tratamientos se observa que varias responden a finalidades propias del encargado del tratamiento, y que se alejan de la finalidad de ofrecer al alumnado la posibilidad de adquirir competencias digitales en el ámbito educativo. Esta cuestión tiene importantes consecuencias a la hora de determinar la base jurídica que legitima los tratamientos, por cuanto si éstos sirven a una finalidad propia del encargado, ya no pueden sustentarse en la base jurídica del articulo 6.1 e) y en su caso apartado c) del RGPD que es la que legitima el tratamiento de datos en entornos digitales por la administración educativa para fines educativos.

Estos aspectos resultan esenciales para cuestionar el papel de Google en la prestación del servicio contratado a la administración educativa como un simple encargado del tratamiento, sino que el rol que desempeña se aproxima más a la figura de un responsable del tratamiento. El informe también rechaza determinadas cláusulas sobre la aplicación del RGPD y sobre la elección del subencargado del tratamiento por resultar confusas y ser contrarias al marco jurídico actual.

Finalmente, en el informe se exponen los elementos que el responsable del tratamiento ha de tener en cuenta para valorar la adecuación al principio de proporcionalidad, en relación con los riesgos asumidos, la minimización de datos y la privacidad desde el diseño y por defecto.

Por todo lo anterior, se informa desfavorablemente la firma del convenio por parte de la administración educativa.

Por último, procede citar los siguientes informes que tratan sobre el tratamiento de datos personales derivado del acceso a archivos judiciales y a archivos históricos.

En el **Informe 49/2023** se responde a una consulta planteada con motivo del cumplimiento de 50 años desde el atentado terrorista perpetrado contra quien entonces era Presidente del Gobierno y respecto de la solicitud de acceso al Sumario instruido al efecto por una productora con la finalidad de ilustrar una serie documental televisiva.

Tras analizar la normativa aplicable a los archivos judiciales, determinar que el responsable del tratamiento es el juzgado o tribunal que instruyó el sumario, y que de acuerdo con la STJUE 24 de marzo de 2022 (asunto C-245/20), en relación con el acceso de periodistas a datos personales que figuran en un expediente judicial, y su apartado 34 que interpreta ampliamente del concepto de "tratamientos “con fines jurisdiccionales” recogido en el artículo 236.bis de la LOPJ, se estima que dicho tratamiento entrarían dentro de las competencias que el artículo 236.octies de la LOPJ atribuye al Consejo General del Poder Judicial y no a la AEPD.

No obstante, en el informe se exponen los criterios que se han venido aplicando en supuestos análogos en relación con el tratamiento de los datos personales correspondientes a datos personales de jueces, magistrados, médicos forenses y otros funcionarios presentes en diversas causas judiciales, (Informe 44/2019), en el sentido de que “el tratamiento de datos personales de cargos públicos, en determinados supuestos referidos al ejercicio de los mismos y no a informaciones sobre su vida privada y en el marco de una investigación histórica, podría revestir interés general, reforzándose su publicación por el derecho a la información y por el derecho a la libertad de expresión.” También se pronuncia sobre la procedencia a valorar la existencia de datos referidos a condenas e infracciones penales (artículos 10 del RGPD y 10 de la LOPDGDD) todo ello en relación lo dispuesto en el artículo 57.1 c) de la Ley de Patrimonio Histórico Español, y los modos de acceder dependiendo si los afectados están vivos o no, y los plazos que resultarían de aplicación.

El **Informe 66/2023** resuelve la consulta referida a cómo proceder en aquellos casos en los que se solicita acceso al Archivo General del Ministerio del Interior para ejercer los derechos que confiere

Ley 20/2022, de 19 de octubre, de Memoria Democrática (LMD), en el sentido de si es dicha norma la que prevalece o la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español (LPHE) a la que remite aquella en alguno de sus preceptos.

La consultante sostiene que, en la práctica y en aplicación de la LPHE, opta por anonimizar la información que proporciona a los solicitantes de acceso, frente a lo que recibe numerosas reclamaciones por que éstos entienden que la información así proporcionada impide la realización efectiva de sus derechos.

El informe indica que el responsable del archivo debe realizar una ponderación de si, aplicando estrictamente la LPHE y en concreto el Decreto 1708/2011, de 18 de noviembre, (RDSEA) en su artículo 28.4 sobre la anonimización, a la hora de resolver las solicitudes de acceso a documentos ex articulo 6 LMD, puede verse afectado el derecho de una persona a acreditar su condición de víctima de tal modo que se impida su realización efectiva si se llevase a cabo dicha anonimización de los datos de terceros.

Todo ello porque hay una evidente diferencia entre el acceso a que se refiere el art. 27.2 LMD que pretendan personas que son potenciales titulares del derecho del articulo 6 LMD a ser considerados "víctimas", del resto de las personas que quieran acceder con carácter general a los documentos sobre el golpe de Estado, la Guerra y la Dictadura por diferentes motivos.

El informe sostiene que "una práctica generalizada de la anonimización en base a la remisión normativa del articulo 27.3 LMD, sin analizar caso por caso el contenido de las solicitudes, podrían imposibilitar o dificultar de facto, el ejercicio del derecho que reconoce expresamente el artículo 6 de la LMD."

Por eso, respecto de dichos solicitantes, el informe concluye que se puede aplicar el principio de especialidad normativa, y no anonimizar la información por mucho que lo permita el artículo 28.4 del RDSEA, y en consecuencia proporcionar la información solicitada de modo íntegro tal como prevé dicho *artículo en su apartado 2*.

2.1.2 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 cabe mencionar las siguientes:

- Anteproyecto de Ley Orgánica por la que se modifican la LO 6/1985, de 1 de julio del Poder Judicial, la Ley de Enjuiciamiento Criminal y la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones.

- Anteproyecto de Ley Orgánica integral contra la trata y la explotación de seres humanos.

- Anteproyecto de Ley Orgánica de representación paritaria de mujeres y hombres en órganos de decisión.

- Anteproyecto de Ley de Industria.

- Anteproyecto de Ley de condiciones básicas para la igualdad en el acceso y disfrute de los servicios sociales.

- Anteproyecto de Ley por la que se modifica el texto refundido de la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor, aprobado por Real Decreto Legislativo 8/2004 de 29 de octubre.

- Proyecto de Real Decreto aprobatorio del Reglamento del Registro Estatal de Asociaciones de Consumidores y Usuarios.

- Proyecto de Real Decreto por el que se modifica el Real Decreto 390/2021 de 1 de junio, por el que se aprueba el procedimiento básico para la certificación de la eficiencia energética de los edificios.

- Proyecto de Real Decreto por el que se modifica el Real Decreto 1799/2003, de 26 de diciembre, por el que se regula el contenido de las listas electorales y de las copias del censo electoral.

- Proyecto de Real Decreto por el que se modifica el Reglamento de dominio público hidráulico aprobado por Real Decreto 849/1986, de 11 de abril y el Reglamento de la administración pública del agua, aprobado por Real Decreto 927/1988, de 29 de julio.

- Proyecto de Real Decreto por el que se establecen las normas reguladoras del bono cultural joven.

- Proyecto de Real Decreto por el que se crea y regula la Red Estatal de Vigilancia de Salud Pública.

- Proyecto de Real Decreto por el que se crea la Agencia Estatal de Administración Digital y se aprueba su estatuto.

- Proyecto de Real Decreto por el que se modifica el Real Decreto 1110/2015, de 11 de diciembre, por el que se regula el Registro Central de Delincuentes Sexuales.

- Proyecto de Real Decreto de modificación de los Real Decreto 928/1998 que aprueba el Reglamento general sobre procedimientos para la imposición de sanciones por infracciones de orden social y para los expedientes liquidatarios de la SS y el RD138/2000 aprueba el Reglamento de organización y funcionamiento de la Inspección de trabajo y SS en materia de Administración digital.

- Proyecto de Real Decreto por el que se regulan los productos sanitarios para diagnostico in vitro.

- Proyecto de Real Decreto por el que se aprueba el reglamento de registro de la propiedad intelectual.

- Proyecto de Real Decreto por el que se desarrollan la composición y el funcionamiento de la Sección Segunda de la Comisión de Propiedad Intelectual.

- Proyecto de Real Decreto por el que se aprueba el Estatuto de la Autoridad Independiente de Protección del Informante.

- Proyecto de Real Decreto por el que se modifica el Real Decreto 1051/20136, de 27 de dic., por el que se regulan las prestaciones de sistema para la autonomía y atención a la dependencia, establecidas en la Ley 39/2006, de 14 de dic., de Promoción de la Autonomía personal y Atención a las personas en situación de dependencia.

- Proyecto de Real Decreto por el que se regula la admisión del alumnado en centros públicos y privados concertados, en el ámbito de gestión del Ministerio de Educación y Formación Profesional de las ciudades de Ceuta y Melilla.

- Proyecto de Real Decreto por el que se modifica el Reglamento regulador de las escuelas particulares de conductores, aprobado por Real Decreto 1295/2003 de 17 de octubre, y el Reglamento general de conductores, aprobado por Real Decreto 818/2009 de 8 de mayo.

- Proyecto de Real Decreto relativo a la gestión de los residuos de los productos del tabaco con filtros y los filtros comercializados para utilizarse con productos del tabaco.

- Proyecto de Real Decreto por el que se regula la ayuda económica establecida en el art. 41 de la Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de libertad sexual.

- Proyecto de Real Decreto por el que se modifica el artículo 9 del Reglamento de armas, aprobado por Real Decreto137/1993, de 29 de enero.

- Proyecto de Real Decreto por el que se regula el Registro Estatal de comunicación audiovisual.
- Proyecto de Real Decreto por el que se modifica el Real Decreto 1082/20212, de 13 de julio, por el que se aprueba el Reglamento de desarrollo de la Ley 35/2003, de 4 de noviembre, de Instituciones de inversión colectiva.
- Proyecto de Real Decreto por el que se regula el Consejo de la Memoria Democrática y el Registro Estatal de Entidades de Memoria Democrática.
- Proyecto de Real Decreto por el que se establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo, por la que se establecen normas armonizadas en materia de IA.
- Proyecto de Real Decreto por el que se modifica por el que se modifica el Reglamento de población y Demarcación territorial de las entidades locales, aprobado por Real Decreto 1690/1986, de 11 de julio.
- Proyecto de Real Decreto Transposición de la Directiva UE 2021/514 del Consejo de 22 de marzo de 2021, por la que se modifica la Directiva 2011/16/UE relativa a la cooperación administrativa en el ámbito de la fiscalidad, y otras normas tributarias.
- Proyecto de Real Decreto por el que se aprueba el Reglamento relativo a las infracciones administrativas de contrabando.
- Proyecto de Real Decreto por el que se regula el procedimiento de certificación y la supervisión continua de los proveedores civiles de servicios meteorológicos de navegación aérea.
- Proyecto de Real Decreto por el que se regula el Registro Público Concursal.
- Proyecto de Real Decreto por el que se modifica el Real Decreto 95/2009, de 6 de febrero, por el que se regula el sistema de registros administrativos de apoyo a la administración de justicia.
- Proyecto de Real Decreto Registro huella de carbono.
- Proyecto de Real Decreto por el que se desarrolla el Reglamento de la Administración Concursal.
- Proyecto de Real Decreto por el que se modifica el Real Decreto 183/2004, de 30 de enero, por el que se regula la tarjeta sanitaria individual. *
- Proyecto de Decreto del Consell por el que se aprueba la política general, estructura organizativa y asignación de funciones en materia de protección de datos en la Administración de la Generalitat y su Sector Público Instrumental.
- Proyecto de Decreto del Gobierno de Aragón por el que se aprueba la Política de Protección de Datos y Seguridad de la Información de la Administración de la Comunidad Autónoma de Aragón. *
- Proyecto de Orden Ministerial por la que se aprueba la Política de Seguridad del Ministerio de Justicia.
- Proyecto de Orden Ministerial por la que se regula el registro de producción y gestión de residuos.
- Proyecto de Orden Ministerial por la que se desarrollan diversas disposiciones del RD 36/2023, de 24 de enero, por el que se establece un sistema de Certificados de Ahorro Energético.

- Proyecto de Orden Ministerial por la que se crea en el ámbito de la Administración General del Estado, el Registro de Seguridad de presas y embalses.

- Proyecto de Orden Ministerial por la que se regula la duración, el contenido y los requisitos de los cursos de conducción segura y eficiente, cuya realización conlleve la recuperación o bonificación de puntos, así como los mecanismos de certificación y control.

- Proyecto de Orden Ministerial por la que se regula el procedimiento administrativo de adquisición y pérdida de la condición de punto de atención al emprendedor.

- Proyecto de Circular sobre la aplicación del artículo 66.1.b de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones.

- Propuesta de Circular por la que se regula el procedimiento para el suministro y recepción de los datos de abonados, de conformidad con el artículo 8.2. i del Estatuto Orgánico de la CNMC, aprobado por Real Decreto 657/2013, de 30 de Agosto.

2.1.3 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.

En este apartado se recogen, por un lado, las Sentencias de la Audiencia Nacional, que es órgano judicial competente para conocer de los recursos interpuestos contra las resoluciones de la AEPD, y en su caso, las Sentencias del Tribunal Supremo que conocen de los recursos de casación que se interpongan contra las Sentencias de la Audiencia Nacional. Y por otro, se incluye aquella jurisprudencia del Tribunal Constitucional y de los Tribunales Europeos que versen sobre la materia y que por su interés merecen ser destacadas.

Durante el año 2023 se han dictado por la Sala de lo contencioso-administrativo de la Audiencia Nacional, 43 resoluciones, de las cuales:

- 24 fueron desestimatorias de los recursos formulados contra resoluciones de la Agencia (que quedaron plenamente confirmadas);

- 1 estimó parcialmente el recurso;

- 7 estimaron íntegramente las pretensiones anulatorias de las resoluciones de la Agencia;

- 11 inadmitieron los recursos interpuestos contra resoluciones de la Agencia.

Por su parte, el **Tribunal Supremo dictó dos resoluciones**, de las cuales una confirmó el criterio de la AEPD y la otra estimó las pretensiones de los recurrentes.

En cuanto a los sectores de actividad de los recurrentes tanto en la Audiencia Nacional como en el Tribunal Supremo, de 63 resoluciones que resuelven recursos frente a las resoluciones de la AEPD, y en su caso, frente a Sentencias de la Audiencia Nacional que confirman las resoluciones de la AEPD, la mayor parte han sido interpuestos por particulares (42).

No obstante, un alto número de ellas son desestimatorias, siendo el motivo más común la falta de indicios o inconsistencia fáctica y jurídica de la denuncia, que desaconsejan si quiera iniciar actuaciones de investigación, tal como también aprecia tribunal.

Al igual que en el ejercicio anterior, un buen número se concreta en las que el fallo es la declaración de inadmisibilidad del recurso por falta de legitimación activa por cuanto se solicita al tribunal a quo, no sólo la revocación de la resolución de la AEPD sino la imposición de una sanción, recordándose por la Sala la ausencia en los particulares de un derecho subjetivo en ese sentido, reiterando la doctrina de que el ius puniendi no está en manos de los particulares.

Asimismo, entre las desestimatorias, procede citar aquellas que versan sobre el ejercicio de derechos, tanto aquellos referidos al derecho de acceso con carácter general, como aquellos referidos a la supresión de antecedentes policiales y que confirman el criterio de la AEPD por cuanto se considera que el responsable ha dado respuesta válida en derecho al titular de los datos personales, siendo un cuestión distinta que dicha respuesta no satisfaga los intereses particulares del afectado, y aquellas en las que se pone el acento en los requisitos formales de la solicitud del derecho o en el carácter repetitivo de la misma. A los particulares les siguen aquellas resoluciones referidas al sector de la salud (4), el sector energético (3) y en igual medida los sectores de Telecomunicaciones, Banca-Seguros y Asociaciones-Sindicatos (2) y finalmente el sector de Sociedad de la Información (1).

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

Comenzando por aquellas resoluciones que tratan de los principios relativos al tratamiento de datos, como el de licitud y el de integridad y confidencialidad (artículo 5.1 a) y f) del RPGD), destaca la **Sentencia de 27 de enero de 2023**, recaída en el Recurso Núm. 543/2020 que desestima las pretensiones del recurrente en un caso referido a la **aportación de datos personales a procesos judiciales**.

La pareja del recurrente se encontraba inmersa en un proceso civil de formación de inventario del régimen económico matrimonial, en el que la representación del excónyuge de aquella, a través del juzgado, solicitó a la entidad bancaria el extracto de las cuentas “a nombre de” aquella. La entidad bancaria al aportar dicha información también incorpora a la causa los datos personales del recurrente dónde era titular y su pareja figuraba únicamente como persona autorizada.

Se analiza una posible vulneración del principio de licitud y de confidencialidad y se concluye que el tratamiento encontraba legitimación en el artículo 6.1 c) del RGPD por cuanto al amparo de lo dispuesto en el artículo 118 de la Constitución Española y articulo 17 de la Ley Orgánica del Poder Judicial, existía en la entidad bancaria una obligación de cumplir los requerimientos judiciales. Resultando irrelevante el título de aquella en relación con la cuenta bancaria, por cuanto apareciendo como autorizada, era una cuenta que “existía a su nombre”.

Finalmente, respecto del principio de confidencialidad, la Sala sostiene que la posible difusión de los datos del recurrente fue “muy limitada” resaltando el deber de secreto de los funcionarios de la administración de justicia y de la otra parte interviniente en el proceso que le asiste el deber de confidencialidad. Por todo ello se desestiman las pretensiones del recurrente y se confirma la resolución de inadmisión de la AEPD.

Siguiendo con el principio de confidencialidad, en la **Sentencia de 9 de enero de 2023**, recaída en el Recurso Núm. 433/2020 que desestima las pretensiones del recurrente en un caso referido a la **publicación de datos en tablones de anuncios en comunidades de propietarios**.

Se presenta reclamación contra el Secretario Administrador de la Comunidad de Propietarios por publicar una convocatoria de la Junta General Ordinario de Propietarios en el tablón de anuncios del portal del edificio dónde se hacía constar una deuda asociada a la vivienda del recurrente.

La resolución de la AEPD centra sus argumentos en que, con carácter general, no resulta preciso que, en el ámbito interno de la Comunidad, los propietarios consientan el uso de sus propios datos personales y en relación con la morosidad, los artículos 16.2 y 19 de la Ley de Propiedad Horizontal habilitan la inclusión de los datos identificativos de los propietarios deudores en las Convocatorias de la Junta y en sus Actas. Asimismo, la convocatoria fue expuesta en un lugar que no se encuentra cerrado con llave, concretamente en un tablón en la pared del portal de la finca. Dicha circunstancia resulta determinante en la medida que no se puede identificar al presunto responsable de la conducta reprochada, ni por tanto se podría valorar si se han cumplido los requisitos previos de notificación a la publicación de la situación contable de la afectada. En este sentido se debe tener en consideración que la exposición del documento en un lugar abierto permitiría a una pluralidad de personas llevar a cabo la conducta reclamada A lo que debe añadirse que tan solo se publica, en relación con las deudas la identificación de la finca, pero no los datos de su propietario, por lo que (…) esta Agencia únicamente podría entrar a conocer este asunto en el caso de que la documentación aportada permitiera acreditar que el propietario afectado resulta identificable, circunstancia que tampoco se aprecia a partir de la documentación aportada y obrante en el expediente de análisis (…).

Por el recurrente se invoca la vulneración del artículo 9 de la LPH, dado que no consta el previo intento de notificación en el domicilio y del artículo 5 de la LOPDGDD referido a la confidencialidad de los datos.

La Sala rechaza los argumentos del recurrente recordando el criterio sostenido en estos supuestos en sus Sentencia de 17 de marzo de 2011 (Recurso Núm. 2015/2019) y de 24 de enero de 2020 (Recurso Núm. 597/2017) sobre la posibilidad de publicación de la convocatoria en el tablón del edificio de la comunidad (…)haciendo constar la existencia de una deuda de uno de dichos comuneros del modo en que se hizo, pues en definitiva dicha fijación de la suma adeudada se encuentra legalmente amparada y constituye un tema de interés para tal Comunidad, y al no estar identificada la persona deudora como tal, contrariamente a lo invocado en la demanda, tampoco es accesible a terceros o visitantes.(…)

Por su parte, la **Sentencia de 28 de abril de 2023** recaída en el Recurso Núm. 409/2021 analiza la adecuación al **principio de integridad y confidencialidad**, al abordar el recurso interpuesto por un **sindicato de funcionarios** que es sancionado por la AEPD.

Los hechos se concretan en que la (…) la delegada sindical (…) ha publicado en un grupo abierto de WhatsApp en el que se encuentran casi todos los trabajadores de la Unidad Central de Radiodiagnóstico de la Comunidad de Madrid un listado del censo electoral de publicidad exclusiva para los sindicatos, figurando datos como nombre y apellidos y el DNI de todos los votantes que forman el personal estatutario, (…)

La sancionada manifiesta que tiene amparo legal para dicha publicación, sin embargo, la AEPD en su resolución argumenta que: Ese amparo legal no se encuentra en el Estatuto de los Trabajadores, art. 74, pues en la forma en que se ha hecho mediante la publicación de los datos a través de un grupo abierto de WhatsApp no es una publicidad que se incardine en ese art. 74 ET. (…), igualmente, El RD 1844/1994 que aprueba el Reglamento de elecciones a órganos de representación de los trabajadores de la empresa (…) no existe una base legal para la publicación de los datos en la forma en que se ha hecho dando nombres y apellidos y DNI a través del WhatsApp. Quien tiene la respon-

sabilidad de publicar el censo es la Mesa Electoral y es una publicación que se realiza mediante el tablón de anuncios para que pueda ser visada por los electores a efectos de poder rectificar errores. El delegado sindical trató ilícitamente estos datos personales revelando un DNI de las personas integrantes del grupo de WhatsApp, por ello existe una infracción del art. 5.1.f RGPD en relación con el art. 6.1 (…) La libertad sindical ha sido ponderada en la resolución, y refiere que la Ley de Libertad Sindical en el art. 8.1.c dispone que los trabajadores afiliados a un sindicato podrán, en el ámbito de su empresa o centro de trabajo… c: Recibir la información que le remita su sindicato. Y conforme al mismo precepto apartado 2.a: con la finalidad de facilitar la difusión de aquellos avisos que puedan interesar a los afiliados al sindicato y a los trabajadores en general, la empresa pondrá a su disposición un tablón de anuncios...". Pero la libertad sindical se respeta y materializa dando la información en la forma que se prevé sin necesidad de acudir a ese medio WhatsApp que nada aporta a la libertad sindical.

La Sala concluye que (…) la publicación por la delegada sindical de CSIF en un grupo abierto de WhatsApp los DNI de los trabajadores que lo formaban no se realizaron en el marco del ejercicio de las funciones inherentes a la libertad sindical, pues la publicación por WhatsApp de ese dato personal no reviste ningún interés sindical. Es un listado del censo electoral en el que figura un DNI cuando legalmente está previsto en el estatuto de los Trabajadores, art. 74, que la lista de electores se hará pública a través del tablón de anuncios mediante su exposición. El RD 1844/1994 igualmente establece que la lista de electores y elegibles se hará pública en los tablones de anuncios. El RD 1846/1994 de 9 septiembre, art. 14, señala que en ese censo se hará constar nombre, apellidos… DNI, y se trata de una lista que se hará pública en los tablones de anuncios.

En definitiva, la normativa sectorial prevé la publicación de estos datos en los tablones de anuncios, pero desde luego no se contempla su publicación mediante WhatsApp, una aplicación de mensajería instantánea que puede considerarse que forma parte de las nuevas tecnologías de la comunicación, que puede servir para comunicar información a los trabajadores, pero que por sus características no aporta seguridad a la confidencialidad de los datos personales. Nada impide al sindicato el empleo de estos mecanismos como WhatsApp o similares, pero en modo alguno puede aceptarse el empleo de esta mensajería instantánea de manera automática para la publicación de datos personales tan relevantes como el DNI y cuya publicación no guarda relación alguna con el derecho a la libertad sindical, con el derecho de los trabajadores. El contenido del WhatsApp afectada a todos o casi todos los trabajadores de la Unidad Central de radiodiagnóstico de la CAM estén o no afiliados al CSIF, a otros sindicatos o a ninguno, y desde luego la publicación del DNI de los afectados en el WhatsApp no es una materia directamente relacionada con los derechos sindicales, por lo que debemos rechazar esta cuestión. (…)

La transmisión de esos DNI a través de WhatsApp por parte de la delegada sindical de la recurrente no indica que haya actuado en el ejercicio legítimo de su derecho a la libertad sindical. Su derecho a informar a los trabajadores de hechos de relevancia sindical no incluye enviar información sobre el DNI de los trabajadores que formaban parte del grupo de mensajería WhatsApp. Por todo lo anterior, se confirma la resolución de la AEPD.

También **relacionada con el principio de confidencialidad** procede citar la **Sentencia de 9 de febrero de 2023** recaída en el Recurso Núm. 770/2020 que desestima el recurso interpuesto por una compañía de telefonía contra la resolución sancionadora de la AEPD, en relación con la **emisión de duplicados de tarjetas SIM**.

Considera la AEPD que los hechos controvertidos vulneran el art. 5.1.f) RGPD porque el principio de confidencialidad de los datos se ha visto afectado dado que la compañía de telefonía facilitó a personas distintas del titular del teléfono móvil duplicados de tarjetas SIM, que constituyen el soporte mediante el cual se accede a datos de carácter personal del afectado. Acceso a datos personales del titular por un tercero que se

produjo debido a que la compañía no contaba con medidas suficientes ni adecuadas en los términos del reseñado art. 5.1.f) del RGPD para comprobar que la persona que solicita el duplicado de la tarjeta SIM es el titular de la misma.

Por el recurrente se alega, entre otras cuestiones, que la tipificación que hace la Agencia carece de motivación suficiente, por cuanto los hechos deben subsumirse en el artículo 32 RGPD y no en el artículo 5.1 f).

La Sala considera suficientemente motivada la tipificación y confirma el criterio de la Agencia indicando que (…) el artículo 32, como pone de relieve el Abogado del Estado, aunque relacionado con el 5.1.f), no circunscribe el principio en su totalidad, pues el artículo 5.1.f) del RGPD requiere para su aplicación una pérdida de confidencialidad. pérdida de confidencialidad de los datos, que según razona la resolución sancionadora (página 671 del expediente), va acompañada de medidas de seguridad insuficientes. Alega la actora que el art 5.1.f) RGPD se limita a enunciar los principios informadores de la protección de datos, mientras que el artículo 32 recoge una infracción concreta de medidas de seguridad. Sin embargo, de la lectura del artículo 5.1.f) RGPD, transcrito más arriba, se desprende que no se limita a enunciar uno de los principios básicos para el tratamiento (de integridad y confidencialidad), ni puede conceptuarse de genérico e impreciso, o de insuficiente determinación de la conducta sancionada, sino que permite predecir con suficiente grado de certeza las conductas que constituyen infracción, por lo que conforme reiterada doctrina del Tribunal Constitucional (…)no vulnera el principio de tipicidad. (…)

También se alega la falta de culpabilidad ya que la entidad entiende que se le está exigiendo una responsabilidad objetiva. La Sala rechaza estos argumentos y confirma el criterio de la Agencia al señalar que Sobre la supuesta responsabilidad objetiva, la resolución recurrida no considera responsable a (…) por el resultado, sino por una pérdida de confidencialidad vinculada a la insuficiencia de las medidas de seguridad implantadas y, en definitiva, debido a una falta de diligencia de dicha entidad(…)la mera comprobación de la información básica de una persona, como puede ser el nombre, apellidos y DNI resulta inútil para los fines para los que está prevista, pues es de suponer que unos delincuentes que ya han obtenido una serie de datos como los datos de acceso o las credenciales de la banca online de una persona y el número de teléfono asociado a esa cuenta, cuentan seguramente con la información básica de dicha persona. Se esgrime por (…) que fue engañada al haberse aportado junto con la solicitud de duplicado de tarjeta SIM correspondiente al reclamante 1, un DNI y una denuncia de hurto falsos, y si bien es cierto que en ese caso se aportó documentación falsificada, omite que en el caso del reclamante 2, el duplicado de la SIM se activó por el canal telefónico y aportada la grabación, se verificó que el operador preguntó el número de línea y el propio operador le dice el nombre y le pregunta si es él, pero ni siquiera le pide el DNI. Esta última forma de actuación se produce también en otros casos de activación de duplicados por canal telefónico que examina la resolución recurrida.

Por tanto, se ha producido una pérdida de confidencialidad de los datos debido a que las medidas de seguridad implementadas por el responsable del tratamiento no resultaban adecuadas ni eran suficientes para garantizarla. Esa falta de diligencia de (…), como responsable del tratamiento, a la hora de implementar en origen las medidas de seguridad adecuadas para comprobar que la persona que solicita o activa el duplicado de la tarjeta SIM es el titular de ésta es lo que constituye el elemento de la culpabilidad.

Otro aspecto relevante que se aborda en la Sentencia es la consideración de dato personal de la tarjeta SIM. Alega la recurrente que no se vulnera la confidencialidad de los datos personales puesto que la tarjeta SIM no identifica ningún número de teléfono ya que dicho número se guarda en los servidores de la compañía y el único dato que incluye dicha tarjeta es el IMSI que se almacena de forma cifrada de modo que no es accesible al usuario, por lo que no se pierde la confidencialidad de los datos.

Frente a ello la Sala razona que siguiendo a la Fiscalía General del Estado en su informe de julio

de 2016, la tarjeta SIM almacena el IMSI que es el código de identificación en la red de comunicaciones móviles celulares y es fundamental para identificar al abonado, por lo que, quien tenga dicha tarjeta (el suplantador) tiene el IMSI almacenado. Además, en cuanto el suplantador introduzca la SIM en un terminal y lo encienda, el IMSI va a ser accedido e intercambiado con la red. En la medida que e IMSI instalado en la tarjeta SIM permite singularizar a un individuo y por tanto identificarle, ha de ser considerado como dato personal, según el artículo 4 del RGPD.

Y concluye indicando que (…) tanto los datos personales (nombre, apellidos y DNI) que se tratan para emitir un duplicado de la tarjeta SIM, como la propia tarjeta SIM que identifica de forma inequívoca al abonado en la red, son datos de carácter personal y su tratamiento, así como la seguridad y confidencialidad de dichos datos vinculados a la emisión/activación de un duplicado de la tarjeta SIM, están sujetos a la normativa de protección de datos. (…)

En cuanto al **principio de licitud**, la **Sentencia de 10 de febrero de 2023** recaída en el Recurso Núm. 41/2021 aborda un **supuesto de contratación fraudulenta en el ámbito del sector energético** por lo que la compañía es sancionada por la AEPD por la vulneración del artículo 6.1 del RGPD.

Señala la resolución que (…)la existencia de la infracción se deduce claramente de la concisa relación de hechos probados de la que destaca que el titular de un contrato de distribución y suministro de energía con una compañía (ENDESA), vio cómo, sin su conocimiento ni consentimiento, la compañía suministradora pasaba a ser otra diferente (EDP), así como el titular del contrato; la resolución no estima que el tratamiento de datos se produzca mediante el acceso al CUPS cuya función y contenido expondremos más adelante, sino por la falta de consentimiento del titular del contrato así como por la falta de comprobación adecuada de la identidad y consentimiento del nuevo titular que, en este caso, actuaba por medio de un representante.(…)

La Sala aclara que el Código Universal de Punto de Suministro (CUPS), se compone de varios datos, entre los que se encuentran en sus apartados c), z) y aa) datos personales cuyo acceso se prohíbe a las entidades comercializadoras y a la CNMC, junto a cualesquiera que identifiquen al titular del punto de suministro. Por ello, no es el acceso al CUPS, que es permitido por la normativa sectorial (Real Decreto 1435/2002, de 27 de diciembre) lo que se sanciona, sino el cambio de titularidad de la compañía suministradora, sin contar con el consentimiento del anterior y del nuevo titular, lo que corresponde a la nueva comercializadora o comercializadora entrante, en este caso EDP, como se expone en la Resolución impugnada y, en este caso, no se ha acreditado tal consentimiento lo que se evidencia, además, por la denuncia del titular inicial del contrato que, durante unos días vio cambiada su relación contractual sin haberlo autorizado y sin asegurarse tampoco del consentimiento del nuevo titular.

Siguiendo con el **principio de licitud**, en la **Sentencia de 14 de febrero de 2023** recaída en el Recurso Núm. 463/2020 se analizan los **requisitos del consentimiento para el tratamiento de datos**.

La resolución desestima el recurso interpuesto por un hospital que es sancionado por la AEPD, por obtener el consentimiento de los titulares de los datos sin cumplir los requisitos que impone el RGPD.

Los hechos se concretan en que en el año 2019 una persona acude al servicio de urgencias de un hospital de la sanidad privada y rellena un formulario de recogida de datos personales dónde se indica que de acuerdo con la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, los datos serán tratados con la finalidad de asistencia y gestión sanitaria, identificando al responsable, y respecto de la cesión a terceros distintos de éstos consta que:

“Si no desea que se facilite esta información a terceros, marque esta casilla (-) Asimismo, y salvo indicación expresa, autorizo al responsable del

fichero (…), a la utilización de los datos personales del paciente para el envío de información de sus productos y servicios, pudiendo revocar dicho consentimiento en cualquier momento.

Si no desea autorizar envío de publicidad, marque esta casilla (-)".

La Sala confirma la sanción impuesta por la AEPD considerando que la normativa de protección de datos excluye en la actualidad el consentimiento tácito y exige que el mismo sea explícito. Solo resultará válido el consentimiento expreso, que debe otorgarse a través de un acto afirmativo claro que evidencie una declaración de voluntad libre, específica, informada e inequívoca del titular de los datos de carácter personal, en el sentido de que no exista la más mínima duda de que ha habido voluntad manifiesta por parte de dicho afectado.

En el caso analizado resulta que se incumplen, en el formulario de solicitud de Ingreso Urgente en el Hospital, los referidos requisitos, en cuanto se requiere dicho consentimiento del paciente, tanto para ceder a terceras entidades sus datos como para remitir publicidad, no a través de una conducta activa, sino de una inacción del interesado (si no desea…marque esta casilla), tratándose en definitiva de un consentimiento tácito, sin que resulte inteligible la información para la que dicho consentimiento se exige, en cuanto su sentido negativo puede dar lugar a confusión, no resultando comprensible al integrante medio de la audiencia.

También relacionada con el **principio de licitud**, en la **Sentencia de 7 de marzo de 2023** recaída en el Recuro Núm. 229/2021 se analiza el **tratamiento de datos que realiza la Agencia Estatal de la Administración Tributaria** (AEAT).

Se denuncia por la recurrente que la AEAT, en el marco de un procedimiento de inspección tributaria contra un tercero, ha emitido acuerdos de liquidación de IVA y de IRPF donde constan sus datos personales no siendo interesada en dichas actuaciones, y por tanto se ha producido una cesión de datos personales de la recurrente en favor de la obligada tributaria por parte de la AEAT. En concreto, indica que en los citados acuerdos de liquidación se menciona a la reclamante con su nombre y apellidos, DNI, se hace referencia a sus vínculos familiares con terceras personas, se desvelan datos de carácter patrimonial y económicos al mencionar a la reclamante como titular de un estanco y administradora de una sociedad de responsabilidad limitada, datos que no eran conocidos en su totalidad, con anterioridad a la notificación de los acuerdos de liquidación, por la obligada tributaria.

La postura del Abogado del Estado se concretaba en que los acuerdos de liquidación responden a la competencia que tiene atribuida la Administración tributaria en orden a la aplicación de los tributos, así como al cumplimiento de la obligación que pesa sobre la misma en cuanto a la motivación de las liquidaciones tributarias, ex artículo 102.2.c) Ley General Tributaria.

En estos términos, indica que en los acuerdos de liquidación se cuestiona por la AEAT las facturas de gastos procedentes de la entidad donde es administradora la recurrente, como proveedor de servicios de la obligada tributaria y al objeto de fundamentar la obligación legal de la Administración de justificar la no deducción por parte de la misma de los gastos que le habían sido facturados por la entidad donde es administradora la recurrente, resultaba imprescindible poner de manifiesto la actividad y operaciones del resto de estancos de personas vinculadas familiarmente, al objeto de fundamentar la instrumentalización de dicha entidad para disminuir la tributación de las personas titulares de los estancos y de la propia sociedad registrando gastos que en realidad son personales de los administradores y familiares (entre ellos la recurrente).

Pues bien, la Sala tras indicar que son de aplicación los artículos 6.1 c) y e) del RGPD y 8 de la LOPDGDD, recuerda lo indicado en el artículo 95.1 de la LGT que alude al carácter reservado de los datos tributarios en poder de la Administración tributaria, destacando que solo pueden ser utilizados con fines tributarios dentro de sus funciones y en el marco o ámbito de sus competencias.

En consecuencia, los acuerdos de liquidación, referidos a la obligada tributaria, responden a la competencia que tiene atribuida la Administración tributaria en orden a la aplicación de los tributos y que se desarrolla, "a través de los procedimientos administrativos de gestión, inspección y recaudación y los demás previstos en este título.", artículo 83.3 LGT.

Liquidaciones tributarias que la Administración tributaria tiene obligación de motivar "cuando no se ajusten a los datos consignados por el obligado tributario o a la aplicación o interpretación de la normativa realizada por el mismo, con expresión de los hechos y elementos esenciales que las originen, así como de los fundamentos de derecho." (art. 102.2.c) LGT).

En efecto, para motivar de forma suficiente y acreditar por parte de la Administración tributaria las razones del rechazo de los citados gastos resultaba imprescindible consignar los datos personales que se plasmaron en dichos acuerdos, entre otros, NIF, nombre y apellidos, administradora de la sociedad etc., Ello permitía poner de relieve esas vinculaciones familiares y con la sociedad, que se consideraban determinantes, junto con otros datos, de la falta de justificación de lo facturado por la sociedad de la que era administradora la recurrente a la obligada tributaria.

Por tanto, no se trata de que los datos de la recurrente incluidos en los acuerdos de liquidación en cuestión se hayan cedido a un tercero (obligado tributario), sino que dichos datos se han utilizado por parte de la AEAT en el ejercicio de sus funciones y de las potestades atribuidas a la Administración tributaria al servicio de los intereses públicos, con fines tributarios, con el objeto de fundamentar, como resulta legalmente exigible, la instrumentalización de la sociedad de la que era administradora la recurrente para disminuir la tributación, entre otras personas, de la obligada tributaria y justificar, en suma, porque no consideraba deducibles, el importe de las facturas de gastos de la citada sociedad que la misma pretendía. Por lo tanto, el fallo de la sentencia es desestimatorio confirmándose la resolución de la AEPD.

En cuanto a otros principios como el de minimización, en relación con el principio de proporcionalidad en el ámbito de la **videovigilancia**, procede citar la **Sentencia de 25 de mayo de 2023** recaída en el Recurso Núm. 574/2022 interpuesta frente a la resolución sancionadora de la AEPD por una **Comunidad de Propietarios**.

La Sala desestima el recurso teniendo en cuenta que el hecho de que un sistema de videovigilancia haya podido ser instalado conforme a la normativa de seguridad, no autoriza a realizar grabaciones de imágenes en la vía pública más allá de lo que resulta idóneo, adecuado y proporcional, siendo lo esencial si a través de ellas es susceptible de captar o no a personas que se encuentran en la vía pública, en cuyo caso tal tratamiento ha de respetar el principio de proporcionalidad, esencial en esta materia.

Reza la resolución "A través de la documentación obrante en el expediente (página 1) se acredita que con las repetidas cámaras se alcanza un ángulo de visión de la zona de tránsito público que rodea la urbanización, siendo susceptible de captar la imagen de personas que transiten por la misma.

Durante el proceso judicial se aportó una recolocación de las cámaras, y a pesar de ello, se aprecia, como a pesar de que parte de las imágenes están ocultas por una máscara, en alguna de ellas se refleja parcialmente la acera o incluso la calzada posibilitando así la captación de imágenes de transeúntes o vehículos. Y ello pese a que dichas imágenes se han tomado el 13 de enero de 2022, el mismo día que se le notificó la resolución sancionadora - y tras tener conocimiento de la misma y del reajuste realizado del ángulo de visibilidad de las cámaras exteriores.

Es decir, se realiza un tratamiento excesivo y no proporcional de las imágenes captadas, en relación con el ámbito y las finalidades que podrían justificar su recogida, toda vez que la seguridad demandada podría igualmente obtenerse por medios menos intrusivos para la intimidad de las personas afectadas. Por todo lo cual se considera acreditada la infracción apreciada por la resolución recurrida.

En relación con los derechos previstos en los artículos 15 a 22 del RGPD deben diferenciarse aquellas que versan sobre el denominado Derecho al Olvido, de aquellas otras que tratan del resto de derechos.

Comenzando por éstas últimas en la se aborda el **Sentencia de 3 de febrero de 2023** recaída en el Recurso Núm. 1630/2020 ejercicio de los derechos respecto de **datos personales de personas fallecidas**.

Este caso tiene especial relevancia por cuanto se trata del acceso a categorías especiales de datos, a la historia clínica de un fallecido por parte de su primo.

La Agencia resolvió la concesión del derecho de acceso, frente a cuya resolución el Hospital presentó el recurso que fue estimado parcialmente.

La Sala razona que una interpretación tanto literal como sistemática y asimismo teleológica de los artículos 3.1 de la LOPDGDD y artículo 18.3 de la Ley de Autonomía del Paciente, "nos llevan a considerar que por familiares vinculados al fallecido ha de entenderse tanto el cónyuge como los hermanos y los ascendientes y descendientes del primer grado, más no el resto de los familiares. Ello así se desprende de una interpretación literal dado que vínculo, según el diccionario de la RAE, y en la acepción que aquí interesa, significa unión o atadura de una persona o cosa con otra, unión o atadura que por tanto no puede extenderse a cualquier relación familiar, por lejana que sea, sino solo a las más cercanas."

La interpretación de los repetidos preceptos además ha de relacionarse con el concepto de herederos forzosos del artículo 807 del Código Civil y con lo previsto en el artículo 4 de la Ley Orgánica 1/1982, que limita el ejercicio de acciones de protección de los derechos del honor, intimidad e imagen, al cónyuge, descendientes, ascendientes y hermanos del fallecido. Debiendo asimismo traerse a colación el criterio de la AEPD en su anterior resolución R/01546/2016, y el de la Agencia Vasca de Protección de Datos en su Dictamen nº D19-008.

Limitación del acceso a los datos de la persona fallecida a sus ascendientes, descendientes, cónyuge y hermano, por último, que es la que en mayor medida tutela el derecho a la protección de datos personales, derecho fundamental (artículo 18.4 CE) que solo permite el tratamiento de dichos datos personales cuando, o bien exista consentimiento de su titular o bien otro motivo de licitud o legitimación de dicho tratamiento, conforme a lo previsto en los artículos 5 y 6 del RGPD y artículos 4 a 8 de la LOPDGDD.

Razones, que conllevan la estimación de la pretensión de la demanda, en cuanto procede denegar el derecho a acceder a la Historia clínica de su prima fallecida.

Siguiendo con el **derecho de acceso**, en la **Sentencia de 10 de febrero de 2023** recaída en el Recurso Núm. 22/2021 se analiza la competencia de la AEPD para conocer del **correcto o incorrecto proceder del responsable del tratamiento al resolver la petición**.

La parte actora presenta recurso frente al archivo acordado por la AEPD por una presunta vulneración del artículo 22 de la Ley Orgánica 7/2021, de 25 de mayo, al haber denegado, la Dirección General de la Guardia Civil, el acceso a sus datos contenidos en el fichero FGDO-T03.

La Sala confirma el criterio de la AEPD, indicando que el fichero en cuestión está sometido a la normativa sobre materias clasificadas y por tanto excluido del ámbito de aplicación de las leyes de protección de datos.

A continuación, se hace referencia a las sentencias más destacadas referidas al ejercicio de los derechos frente a los ficheros que contienen información sobre antecedentes policiales.

En estos supuestos hay que resaltar que el debate jurídico siempre se centra en el análisis de la motivación por al que se deniega la supresión de antecedentes. Motivación que analiza en sede administrativa la AEPD y que en sede judicial es la Audiencia Nacional la que aborda su adecuación a derecho.

Siendo elementos frecuentes en estos casos, el hecho de que los recurrentes ponen en valor que o bien han cumplido condena, o bien se han cancelado los antecedentes penales, o bien fueron detenidos, pero no fueron condenados por el sobreseimiento de la causa, etc. En definitiva, motivos que los recurrentes entienden que justificarían la improcedencia de que sus datos personales siguieran tratándose en sistemas relativos a antecedentes policiales.

Asimismo, en estos casos se aborda la aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, por aplicación de la Disposición transitoria cuarta de la LOPDGDD, para aquellos supuestos anteriores a la aplicación de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

La **Sentencia de 26 de abril de 2023** recaída en el Recurso Núm. 1805/2021 analiza la conformidad a derecho de la resolución de la AEPD que **desestima el procedimiento de tutela de derechos interpuesto por el recurrente**.

Los hechos se concretan en que el reclamante ve desestimada su petición de supresión de antecedentes policiales frente al fichero de la Dirección General de la Policía (DGP), alegando que es de nacionalidad argelina y está casado con una ciudadana española, que posee tarjeta de residencia permanente de familiar de ciudadano de la UE. Que la detención del recurrente se produjo el 6 de abril de 1997, es decir, hace más de veinticuatro años, y, desde dicha fecha, la reinserción del actor ha sido total. Añade que se ha cumplido la condena y que el antecedente penal ha sido cancelado.

La Sentencia recuerda lo dispuesto en el artículo 23 de la LOPD de 1999 (aplicable en el momento de la petición) en lo referente a la posibilidad de la denegación de la cancelación en "función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando".

Para a continuación analizar la contestación de la denegación que hace la DGP a la AEPD y que se centra en la detención del recurrente como presunto autor de delitos de pertenencia a banda armada, falsedad documental y tenencia ilícita de armas, la orden de búsqueda y captura emitida por el Juzgado Central de Instrucción, así como la prohibición de salida del territorio nacional por colaboración por banda armada y finalmente que fue condenado a 14 años de prisión.

La DGP concluye que: "Además, tal y como ha recordado la Audiencia Nacional en sentencia de 15 de septiembre de 2016, la cancelación de datos policiales queda sujeta a un régimen jurídico especial, con independencia de que se haya llegado a un pronunciamiento absolutorio ya que, desde la perspectiva de la protección de datos, resultan justificados los motivos de seguridad pública invocados, y que amparan la denegación de la cancelación de los antecedentes policiales solicitados"

Teniendo en cuenta lo anterior, la Sala acuerda que la denegación de la supresión es conforme a derecho, con independencia de que se haya producido la cancelación de los antecedentes penales, "vista la gravedad y naturaleza de los hechos (…)resultan efectivamente justificados y subsistentes del art. 23.1 de la LOPD, los motivos de las necesidades de las investigaciones que se estén realizando, la prevención o la represión de infracciones penales, invocados motivadamente por la Dirección General de la Policía, que amparan, en este caso específico, la denegación de la cancelación de los antecedentes policiales solicitados."

La **Sentencia de 31 de mayo de 2023** recaída en el Recurso Núm. 1/2022, también aborda la **supresión de datos referidos a antecedentes policiales**. La DGP deniega la supresión de antecedentes solicitada por el recurrente, por estar relacionada con una condena como autor de un delito de **pornografía de menores** y por qué, en la actualidad, aquel está inscrito en el Registro Central de Delincuentes Sexuales y de Trata de Seres Humanos, regulado por Real Decreto 1110/2015, de 11 de diciembre.

Sobre este último aspecto, la Sala tiene en cuenta que también por el recurrente se solicitó la cancelación del citado registro y fue denegada el 18 de junio de 2020 y confirmada por Sentencia de 13 de enero de 2021. Esta circunstancia también debe ser valorada en el presente caso.

La Sala desestima el recurso indicando que (…)La circunstancia anterior se debe poner en relación con los demás datos mencionados en la Resolución administrativa, como el carácter de los datos almacenados, la fecha de la sentencia y el sentido condenatorio de su fallo por un delito de corrupción de menores, así como la fecha de la remisión definitiva de la condena, inmediatamente anterior a la solicitud de cancelación, todo lo cual justifica la denegación de la cancelación o supresión de los datos en atención a la prevención y averiguación de infracciones penales y a la defensa de los derechos e intereses de terceros, en este caso los menores de edad, víctimas de esta clase de delitos, por lo que la valoración de que la denegación es necesaria y proporcionada en este caso, es conforme con lo dispuesto en el artículo 23.1 del Reglamento General y procede por ello confirmarla al estar suficientemente motivada y ser esta motivación conforme con las normas mencionadas (…)

Sobre hechos similares la **Sentencia de 5 de junio de 2023** recaída en el Recurso Núm. 1789/2021.
Al recurrente se le **denegó la supresión del fichero PERSONAS** por figurar inscrito en el **Registro Central de Delincuentes Sexuales y de Trata de Seres Humanos**. La Sala pone en valor la naturaleza del fichero PERSONAS al indicar que Este registro policial-administrativo respecto de quien ha sido condenado por un delito de corrupción de menores contiene una información muy relevante a los fines de prevención e investigación de este tipo de delitos y como afirma la DG Policía es necesario este fichero para procedimientos, investigaciones y prevención de estos delitos y aun cuando se haya producido la cancelación de los antecedentes penales es importante el mantenimientos de estos datos en la ficha policial siendo el fin ulterior del fichero la base para una lucha contra esta criminalidad que facilita las investigaciones policiales.

La Sentencia desestima las pretensiones del recurrente por estimar conforme a derecho la motivación ofrecida por la DGP y así apreciada por la AEPD, haciendo suyas las razones ofrecidas al concluir que: los datos cuya cancelación se solicita, que constan en el fichero PERSONAS, tienen su origen en una detención y en una condena penal por corrupción de menores. Y el mantenimiento de esos datos personales en el fichero PERSONAS responden a razones de seguridad pública, a la necesidad de prevención e investigación de estos delitos, lo que hace imprescindible que se mantengan tales datos en el fichero policial.

Cierran este grupo de resoluciones las **Sentencias de 9 de junio y 25 de octubre de 2023**, recursos 559/2021 y 61/2022 respectivamente. En esta última se aborda como elemento de análisis el **mantenimiento de los antecedentes policiales a pesar del sobreseimiento provisional de la causa** relacionada con dichos antecedentes.

Siguiendo con las resoluciones relativas al ejercicio de los derechos, el siguiente bloque aborda aquellas sentencias relacionadas con el denominado derecho de supresión referido a los resultados de búsquedas en internet, también denominado derecho al olvido cuya regulación se encuentra principalmente en el artículo 17 del RGPD y articulo 93 de la LOPDGDD.

La **Sentencia de 3 de febrero de 2023** recaída en el Recurso Núm. 2563/2019 **desestima las pretensiones del recurrente y confirma la resolución de la AEPD**.

Los hechos se concretan en que el afectado en el año 2018 ejerce el derecho de supresión frente a Google por el resultado que se muestra al realizar una búsqueda por su nombre y apellido referida a un enlace a una noticia de prensa aparecida el 6 de octubre de 2016 en un medio de comunicación mejicano, concretamente en el periódico proceso.com.mx, que lleva por título "Emerge el lavado de dinero en Puebla de Moreno Valle" y que se refiere al afectado como uno de los dos principales accionistas de una de las (al menos) 12 empresas vinculadas a un esquema de lavado de dinero producto del narcotráfico, según las investigaciones de la por la Procuraduría General de la República (PGR) y la Secretaría de Hacienda mejicanas.

El recurrente sostiene que debe prevalecer derecho al olvido por inexactitud de los datos frente al derecho a la información.

La Sala tras recordar la doctrina del derecho al olvido en la SSTC 58/2018 de 4 de junio, y 89/2022 de 13 de septiembre referidas al y SSTC 23/2010 ,de 27 de abril, y 9/2007, de 15 de enero, invocando el articulo 18.1 y 4 de la Constitución y la de los derechos de libertad de expresión e información consagrados en el artículo 20 de la Constitución, todo ello en relación con el interés general (SSTC 107/1988, de 8 de junio, 20/2002, de 28 de enero, 151/2004, de 20 de septiembre, y 9/2007, de 15 de enero) tiene en cuenta que nos encontramos ante una noticia publicada el 6 de octubre de 2016, y que se refiere a unas actuaciones de investigación (al parecer de gran complejidad) iniciadas por la Procuraduría General de la República y la Secretaría de Hacienda mejicanas, en el año 2015, por lo que la información no puede considerarse obsoleta, dado el tiempo transcurrido desde la emisión de la noticia y los hechos a que hace referencia, que además, y por referirse al dinero supuestamente proveniente del narcotráfico, adquiere una gran relevancia pública en un país como Méjico, lo que no permite apreciar obsolescencia. Relevancia pública que se confirma al referirse a la vida profesional y no personal del recurrente.

Y en segundo término indica que "a pesar de los intentos del demandante para negar la exactitud y veracidad de la información publicada, adjuntando al efecto tanto el certificado de carencia de antecedentes penales en su país de origen (Méjico) como en datos sobre constitución y titularidad de la empresa Blueicon Technology SA, lo cierto es que ni se refiere en la noticia que dicho actor haya sido condenando, sino el inicio de actuaciones de investigación frente a él, ni solo su participación en la referida empresa, sino la constitución, junto con su socio, de 47 empresas, en las que están registrados como accionistas y/o representantes legales, compartiendo cargos de dirección en 12 de ellas. Se trata por tanto de documentación claramente insuficiente y carente de efectos probatorios a fin de contrarrestar la veracidad de la noticia publicada."

La **Sentencia de 7 de marzo de 2023** recaída en el Recurso 1984/2021 **desestima el recurso interpuesto por el recurrente contra la resolución de inadmisión** emitida por la AEPD. Lo relevante en este supuesto es el carácter ambiguo y genérico de la petición de supresión.

La inadmisión de la AEPD se basó en que el reclamante ejerció su derecho frente al buscador en relación a un elevado número de enlaces (287), deduciéndose de ello que podría tratarse de una pretensión contraria a la normativa de protección de datos al tratar de hacer uso de la misma con la única intención de reescribir de forma indiscriminada hechos pasados; también fundamentó su decisión en que la información de las URLs disputadas trascienden del ámbito personal al situarse en un contexto de carácter profesional de la que no se ha acreditado que sea inexacta ni obsoleta, prevaleciendo, por tanto, el derecho a la libertad de expresión y de información regulado en el artículo 20 de la Constitución Española; el recurso de reposición contra esta resolución fue desestimado.

La Sala confirma la resolución recurrida teniendo en cuenta varios factores, entre los que destaca que el demandante solicitó la supresión de un elevado número de urls (287, según la resolución

de la Agencia) que asociaban su nombre con determinada empresa, sin precisar datos tan relevantes como si se trataba de acceder a páginas de medios de comunicación publicando información, a foros de opinión o a redes sociales o a otra clase de enlaces; además, no precisó en ningún momento la naturaleza de la información disponible a través de los enlaces. La genérica pretensión de que se dexindexara cualquier información que asociase su nombre con el de una determinada empresa, no podría ser estimada pues bien puede tratarse simplemente de información neutra sobre la existencia de litigios o discrepancias con determinadas personas, en las que fuera mencionada la empresa lo que impediría considerar como exacta o no tal información, o de opiniones, en contra o a favor del reclamante; dicho de otra manera, la falta de datos sobre la clase de los enlaces y el contenido de la información, incumple las obligaciones que le incumbían (puntos 67, 68 y 72-74 de la sentencia TJUE de 8 de diciembre de 2022 citada) e impide valorar la procedencia de su petición y, consiguientemente, realizar correctamente el juicio de ponderación sobre los derechos en juego.

Y finaliza indicando que "A esta conclusión no puede oponerse eficazmente el hecho de que el buscador "Bing" haya accedido a suprimir el acceso a las urls que solicitó pues se trata de 12 enlaces, frente a los 287 de este caso y no se precisa si en aquella ocasión justificó debidamente la naturaleza de los enlaces y el contenido de la información."

Otra Sentencia que se refiere al **derecho de supresión y al de oposición**, pero ya no en relación con los buscadores de internet, pero si en el contexto de internet (**en el medio digital de una editorial periodística**) es la **Sentencia de 16 de marzo de 2023**, recaída en el Recurso Núm. 1549/2020.

La Sala sostiene que estamos ante una noticia publicada sobre la base de la libertad de información, insertándose un vídeo que aparece en las redes sociales, que es también un medio o canal de obtención de información pública. La noticia se refiere a unos hechos acaecidos en la vía pública, filmados por una persona que captaba las imágenes, hechos en los que era protagonista el recurrente. La noticia, por tanto, es una noticia veraz; al estar grabada en imágenes se demuestra con exactitud lo sucedido, por lo que no es inexacta; y su publicación en medios de comunicación está amparada por el art. 20.1.d CE. (…) nos encontramos con una mera noticia, esa noticia no contiene referencias personales del recurrente, no se refiere, en ningún momento a su vida personal, se refiere tan solo a un hecho público protagonizado por el actor con la suficiente intensidad y teatralidad como para dar a conocer lo que ha ocurrido con su desafortunado comportamiento.

Ni tan siquiera esta noticia contiene una opinión o juicio de valor respecto de los hechos, se limita a narrar tales hechos y sus consecuencias. Dentro de esa narrativa de hechos es muy relevante el vídeo grabado por un tercero que aporta realidad a los hechos pues no se ha demostrado manipulación de tipo alguno. Y lo que es muy importante esa publicación no ha tenido consecuencias perjudiciales ni para el recurrente ni para terceros, por lo que su publicación es meramente informativa, no es más que una mera publicación de una noticia que se ha producido en la calle, que parece molestar o disgustar al recurrente pero que, en el momento de su grabación, por lo que consta en la referida noticia, mostraba una alegre aceptación a esa grabación. Es una noticia publicada el 24 abril 2017 pero no se puede considerar obsoleta, si bien ha transcurrido un tiempo desde que ocurrieron los hechos y se publicó la noticia, lo cierto es que tienen una relevancia pública, no deja de ser una noticia pública, una información que no adolece de obsolescencia (como requiere el articulo 17.3 RGPD). Y en lo referente al derecho de oposición, los supuestos del articulo 21 RGPD no han sido justificada la concurrencia de ninguno para ejercer dicho derecho."

Por todo ello se desestima el recurso y se confirma la resolución de la AEPD.

En cuanto a la jurisprudencia del **Tribunal Supremo**, destaca la **Sentencia de 22 de noviembre de 2023** número 1520/2023 que **resuelve el recurso de Casación 5352/2022**.

La cuestión de interés casacional se concreta en determinar si la actuación de la Agencia Estatal de la Administración Tributaria (AEAT) vulnera el artículo 8 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales con la inclusión de cualesquiera datos personales de terceras personas no interesadas en los procedimientos tributarios, y si su tratamiento en dichos procedimientos tiene la consideración de cesión de datos personales fundado en el cumplimiento de una obligación legal a los efectos de la vigente normativa de protección de datos.

Dice el alto tribunal que la utilización de datos personales de terceras personas, distintas al obligado tributario, por la Administración Tributaria, sin el preceptivo consentimiento, debe considerarse legítimo, tal como se infiere de la doctrina del Tribunal de Justicia de la Unión Europea expuesta en las sentencias de 27 de septiembre de 2017 (asunto C-73/16) y 22 de julio de 2021 (asunto C-439/19), en aquellos supuestos, responda a objetivos de interés general relacionados con la persecución del fraude fiscal, y se acredite el tratamiento de datos personales es proporcionado y no excede de lo estrictamente necesario para cumplir tal fin, y se produzca en el marco de un procedimiento en cuya tramitación se hayan garantizado la protección de los derechos fundamentales y libertades de los interesados y afectados.

También descarta la vulneración del artículo 95 de la Ley 58/2003, de 17 de diciembre, General Tributaria, por cuanto la AEAT no pues la consignación de determinados datos personales del recurrente, referidos a la identificación del nombre y apellidos, DNI, vínculos familiares y datos económicos, se efectúa para la efectiva aplicación de los tributos, tal como dispone el artículo 5 de la Ley General Tributaria, en el marco de las competencias de la Agencia Estatal de Administración Tributaria, en el curso de un procedimiento de comprobación del cumplimiento de las obligaciones tributarias, revelándose idónea y necesaria para la efectiva aplicación de la normativa tributaria, en la medida que era imprescindible para el correcto ejercicio de la función recaudatoria.

Tampoco aprecia que se infrinja el artículo 102.2 c) de la Ley General Tributaria, puesto que la utilización de los datos personales del actual recurrente era necesaria, en razón de las circunstancias concurrentes, referidas a los vínculos familiares y profesionales existentes entre el empleado de la empresa proveedora de servicios profesionales que giraba las facturas y la obligada tributaria, para poder fundamentar los Acuerdos de liquidación, y garantizar el derecho de defensa de la obligada tributaria, que tiene derecho a conocer con precisión la relación de hechos que justifican el levantamiento de las actas de propuesta de liquidación por la Hacienda Púbica, lo que comporta que, a efectos de cumplir la exigencia de motivación de los actos tributarios, deban figurar aquellos datos personales del actual recurrente que, como hemos expuesto, se revelan adecuados, idóneos y proporcionados para el cumplimiento del mismo fin.

Por lo tanto fija la siguiente doctrina de interés casacional: El artículo 8 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y el artículo 6.2 c) y e) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que disponen que el tratamiento de datos personales será lícito, entre otros supuestos, cuando sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento, o cuando sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, no se oponen a que la Agencia Estatal de Administración Tributaria, en el curso de la tramitación y resolución de un procedimiento de gestión, inspección o recaudación tributaria, utilice datos de carácter personal de terceras personas físicas, distintas al sujeto obligado tributario sometido al expediente administrativo, siempre y cuando el tratamiento

de los datos se ampare en las facultades que se confieren a las autoridades tributarias para luchar contra el fraude fiscal, que la inclusión de los datos se limite a aquellos que se revelen adecuados, idóneos, pertinentes y necesarios para la determinación de los hechos y motivar las resoluciones que se adopten, y que sea proporcionada al fin legitimo perseguido para lo que son tratados.

Por último, en cuanto a la jurisprudencia del Tribunal de Justicia de la Unión Europea, destacan durante el ejercicio 2023, las siguientes Sentencias tratan sobre aspectos esenciales del derecho de acceso previsto en el artículo 15 del RGPD.

En primer lugar, **la STJUE de 12 de enero de 2023**, Asunto C-154/21 que aborda si en el derecho de acceso se incluye saber **a quién se han comunicado los datos**, se analiza si es necesaria la identificación especifico o se satisface con informar sobre las categorías de cesionarios.

El derecho se solicita ante un operador postal, y en el proceso judicial se informó que los datos habían sido transmitidos a empresas informáticas, proveedores de directorios, anunciantes que operan a través de establecimientos de venta por correspondencia, ONGs y partidos políticos, entre otros. El Tribunal inicia que el responsable del tratamiento está obligado a facilitar al interesado, previa solicitud, la identidad real de dichos destinatarios. Solo cuando (todavía) no sea posible identificar a dichos destinatarios, el responsable del tratamiento podrá limitarse a indicar únicamente las categorías de destinatarios de que se trate.

En segundo lugar, **la STJUE de 4 de mayo de 2023**, Asunto C-487/21, aclara que el derecho a obtener una "copia" de los datos personales implica que **se entregue al interesado una reproducción auténtica e inteligible de todos esos datos**.
Este derecho implica el de obtener copia de extractos de documentos, o incluso de documentos enteros, o de extractos de bases de datos, que contengan dichos datos, si ello es indispensable para permitir al interesado ejercer efectivamente los derechos que le confiere el RGPD.

Una descripción puramente general de los datos objeto de tratamiento o una remisión a categorías de datos personales no se correspondería con la "copia". Se ha de interpretar como el derecho a obtener una reproducción auténtica de sus datos personales.

Y, en tercer lugar, y estrechamente relacionada con la STJUE de 12 de enero antes referenciada, procede citar la **STJUE de 22 de junio de 2023**, Asunto C-579/21, el empleado y cliente de una entidad financiera tiene conocimiento de que otros empleados han consultado sus datos. Ante lo cual **solicita la identidad de las personas que accedieron a sus datos, las fechas exactas de dichos accesos y los propósitos** para los cuales se trataban dichos datos.

La entidad se negó a proporcionar toda esa información porque constituía una cesión de los datos personales de aquellas personas, pero si proporcionó las fechas y las finalidades de los accesos.

El Tribunal indica que, ante un conflicto entre el ejercicio de los derechos del interesado y los derechos de terceros, debe hacerse una ponderación entre tales derechos y libertades. Y si como resultado de esa ponderación se estima que el conocimiento de esa información resulta indispensable para permitir al interesado ejercer los derechos y libertades, dicho acceso podrá tener lugar.

2.2 Tecnológicos

2.2.1 Gestión de notificaciones de brechas de datos personales

En cumplimiento de la obligación que establece el artículo 33 del RGPD, durante el 2023 se han recibido en la AEPD un total de 2.004 notificaciones de brechas de datos personales, con un incremento del 10% sobre 2022. De las notificaciones de brecha recibidas aproximadamente el 18% corresponde al sector público y el 82% corresponden al sector privado. En general, las brechas que afectan a un número más elevado de personas son las relacionadas con ciberincidentes de tipo ransomware e intrusiones en sistemas de información que resultan en exfiltración de grandes volúmenes de datos personales. Este tipo de brechas afecta tanto a entidades públicas como privadas.

Como resultado de las notificaciones se han emitido 30 resoluciones para obligar la comunicación de las brechas a los propios interesados. Al mismo tiempo, como resultado del análisis inicial de las brechas realizado desde la DIT, se han trasladado a la Subdirección General de Inspección de Datos en 16 ocasiones para un segundo análisis más exhaustivo.

En total, como resultado de las obligaciones que establece el artículo 34 del RGPD **aproximadamente 17 millones de interesados afectados** fueron comunicados por los responsables acerca del hecho de que **sus datos fueron objeto de una brecha**.

En el ámbito de la colaboración con el Centro Criptológico Nacional (CCN) fue actualizado el mensaje de la AEPD en la herramienta LUCIA en el que se recuerdan a las entidades que comunican una brecha al CCN sus obligaciones con relación a lo establecido en los artículos 32 y 33 del RGPD en aquellos casos en los que la brecha comunicada al CCN afecta al ámbito de la protección de datos personales.

2.2.2 Consultas previas

Se han recibido 3 consultas previas que han sido resueltas de forma negativa al no cumplir los requisitos mínimos a los que refiere la Instrucción 1/2021, de 2 de noviembre, de la Agencia Española de Protección de Datos, por la que se establecen directrices respecto de la función consultiva de la Agencia, de conformidad con el RGPD. A pesar de lo establecido en la Instrucción 1/2021, en general, se mantiene una interpretación errónea con relación al cumplimiento y la gestión del riesgo entendiendo que ambos conceptos son idénticos. Igualmente se persiste la interpretación errónea con relación a la finalidad de la consulta previa en cuanto a una validación previa por la Autoridad de Control de lo que se señala en la Evaluación de Impacto en la Protección de Datos (EIPD) en lugar del asesoramiento de la Autoridad de Control con relación a aquellos riesgos en que el responsable no ha podido mitigar suficientemente como exige el artículo 36 del RGPD.

2.2.3 Recursos de ayuda: guías y herramientas

Dentro de la labor de impulso de la protección de datos como un factor de confianza y garantía de calidad para favorecer el desarrollo de la economía digital la División de Innovación y Tecnología ha publicado tres guías que viene a aclarar los criterios existentes en materia de espacios de datos, sistemas criptográficos y tratamientos de control de presencia mediante operaciones de tratamiento biométrico:

- **Aproximación a los Espacios de Datos desde el RGPD**
- **Orientaciones para la validación de sistemas criptográficos en la protección de datos**
- **Guía sobre Tratamientos de datos de control de presencia mediante sistemas biométricos**

En la línea de trabajo de evolución de las herramientas, se ha actualizado la herramienta **GESTIONA-RGPD** añadiendo funcionalidades para la identificación del riesgo, medidas de mitigación y capacidad para la gestión de múltiples tratamientos de alto y escaso riesgo para dar respuesta a las obligaciones del RGPD en materia de gestión del riesgo, registro de actividades de tratamiento, inventario de tratamiento y medidas de seguridad. Al igual que otras herramientas, GESTIONA-RGPD ha sido dotada de capacidad para emitir informes orientados a la firma por los responsables y encargados, así como borradores relativos al registro de actividades de tratamiento y el inventario de tratamiento. La herramienta dispone en la actualidad de capacidad para gestionar en un único archivo más de quinientos tratamientos de un mismo responsable por lo que se espera que sea de gran utilidad para los responsables y, en especial, para las Administraciones Públicas.

Para complementar la guía de Orientaciones para la para la validación de sistemas criptográficos en la protección de datos se ha desarrollado y publicado la herramienta **VALIDA-CRIPTO RGPD**, donde se vienen a trasladar los criterios de la guía para facilitar la gestión los requisitos de cifrado de los tratamientos de datos personales con un enfoque eminentemente práctico, dando así respuesta a las consultas que en ocasiones se realizan a la AEPD con relación a la validez o no de los sistemas criptográficos sobre cuyos requisitos corresponde al responsable tomar las decisiones adecuadas para proteger los datos de los interesados.

Con relación a las obligaciones de los artículos 33 y 34 del RGPD relativos a la notificación y comunicación de brechas de datos, han sido actualizadas las herramientas **ASESORA-BRECHA** y **COMUNICA-BRECHA** dotando a estas herramientas de capacidad para emitir informes que pueden ser utilizados como documentación para demostrar cumplimiento. Esta demanda fue recogida desde la DIT de delegados de protección de datos del sector público quienes manifestaron que dichos informes eran de gran utilidad para la gestión de los tratamientos de datos personales.

2.2.4 Impulso al desarrollo de la economía digital

Con relación a los nuevos desarrollos de la economía digital, desde la DIT se ha llevado a cabo la organización de la **Conferencia Internacional AEPD-ENISA sobre Espacios de Datos** europeos en la que expertos y profesionales de la administración pública europea, la investigación y la empresa privada participaron en conferencias y mesas redondas retransmitidas en abierto y en grupos de trabajo donde fueron analizados de forma práctica las sinergias que pueden establecer entre las garantías para proteger los derechos fundamentales de las personas y el mercado de acceso a los datos. Esta actividad supone un hito en las actividades de la DIT y de la AEPD dado que es la primera ocasión en la que desde ENISA se inicia una línea de colaboración a la vista del interés suscitado por los documentos que sobre espacios de datos y otras materias se han venido desarrollando en los últimos años.

Desde la DIT se ha impulsado el desarrollo de proyectos como el proyecto sobre **blockchain** para dar conformidad al RGPD en colaboración con GMV o el Proyecto con la Fundación Éticas sobre **inteligencia artificial y pymes**, materia sobre en la que actualmente se sigue trabajando.

Una de las tareas que ha requerido una mayor implicación de la DIT es la relacionada con los menores, en especial, con el acceso de menores a contenidos no adecuados para su edad. En este aspecto y con el objetivo de valorar las posibilidades que ofrece la tecnología en la actualidad desde la DIT se ha fomentado la participación de entidades públicas y privadas dando lugar a 16 reuniones con entidades públicas y 25 reuniones con entidades privadas, así como 11 reuniones con entidades internacionales. Además de estas reuniones se han evaluado 12 herramientas de verificación de edad para terminar resumiendo las conclusiones de estas actividades en el desarrollo de 3 pruebas de concepto de sistemas de verificación de edad para la protección del menor. En el ámbito de estas actividades se ha realizado la contratación con el Consejo General de Colegios Oficiales de Ingenieros de Informática de Galicia a fin de reforzar el impulso que se ha venido realizando desde la DIT, por otra parte y en relación con la evaluación de sistemas de verificación de edad se ha realizado un contrato de estudio con la URJC.

Dentro de la línea de protección del menor, la DIT ha estado activa participando en el **Grupo de Acceso de Menores a Contenidos Inadecuados** y en el **Grupo de Verificación de edad de menores** desde donde se ha venido colaborando en el análisis de la situación y las posibles opciones que ofrece la tecnología en este ámbito.

La DIT continúa colaborando en el desarrollo de directrices de **anonimización** en el ámbito de las actividades que se desarrollan conjuntamente en el EDPB y se ha participado con la **SEDIA en el Grupo del Dato** mediante una ponencia sobre anonimización a fin de impulsar este requisito que exige el artículo 32 del RGPD como garantía de privacidad.

Con el objetivo del impulso de la protección de datos en sus aspectos tecnológicos para salvaguardar los derechos y libertades de las personas físicas en el ámbito del desarrollo de la economía digital, **la DIT ha desarrollado y colaborado las siguientes ponencias y actividades**:

- Ponencia en Blockchain Intelligence Law Institut
- Ponencia en el Observatorio BIDA presentando las Orientaciones sobre Espacios de Datos
- Ponencia en el Global PETs Network for Data Protection Authorities sobre Validación de Sistemas de Cifrado
- Ponencia en el IPEN sobre temas de IA
- Conferencia en el CEDPO "Conferederation of European Data Protections Organizations" sobre IA
- Ponencia APEP sobre brechas de datos
- Ponencia ISMS Forum cifrado
- Podcast Observatorio AUTELSI sobre IA
- Presentación en el GDPR Seminar for Korean Businesses in EU
- Presentación en el GPEN de las Orientaciones sobre cifrado
- Conferencia en la Reunión Autoridades Competentes en IA
- Jornada inaugural Curso Superior de Protección de Datos Escuela Gallega de Administración pública
- Congreso Ciberseguridad en Sanidad

- INNOVA Sevilla S3: Perspectiva Nacional en la gestión de Espacios de Datos
- Asociación de Fundaciones - Foro Demos – Seguridad
- Future of Privacy Forum - Verificación de edad
- AECOPS Zaragoza
- Congreso de Contratación Pública Inteligente – Valencia
- Congreso Consejería Educación Generalitat Valencia
- Conferencia Verificación de Edad EU-Consent
- Seminario de Jurisprudencia y Actualidad Internacionales

2.2.5 Impulso a la investigación científico-técnica

Otro de los aspectos en los que la DIT desarrolla sus actividades es el impulso del desarrollo de la investigación científico-técnica. Para ello se ha contado con la c**olaboración de entidades públicas y privadas con las que se han desarrollado las actividades** que se señalan a continuación:

- Protocolo de colaboración con la Universidad de las Naciones Unidas en el campo de Blockchain
- Protocolo de colaboración con el Observatorio de Bioética y Derecho de la cátedra UNESCO Universidad de Barcelona
- Tercera y Cuarta reunión Espacio de Estudio de IA de expertos para asesoramiento mutuo en temas de privacidad/investigación

2.2.6 Adecuación de las administraciones públicas guías y recomendaciones

La DIT desarrolla actividades orientadas al impulso de la protección en el ámbito de las administraciones públicas. Con el objeto de dar respuesta a los retos de los que han surgido en este ámbito, se han desarrollado artículos con recomendaciones sobre los siguientes aspectos:

- **Internet:** **Orientación para el uso de cookies en las AAPP**
- **Brechas:** **Orientaciones sobre brechas masivas en las AAPP**
- **EIPD:** **Orientaciones en la Evaluación de Impacto Normativo**

En ámbitos como brechas y documentos de índole tecnológica se mantiene la colaboración con las Autoridades Autonómicas que ya forma parte de las actividades diarias de esta División.

También en el ámbito de las Administraciones Locales la DIT ha colaborado en la Jornada de protección de datos organizada por la FEMP.

Con relación a los procesos electorales desde la DIT se ha participado en la Red de Coordinación para la seguridad en procesos electorales.

En cuanto a las implicaciones de la IA se ha colaborado en el sandbox de IA en la revisión de guías que darán respuesta a los requisitos que deberán abordar los proyectos de IA que se ofrezcan a participar en este sandbox.

2.2.7 Proyección internacional en responsabilidad proactiva: marco europeo

En el ámbito de la **proyección internacional** de la DIT las actividades que se han desarrollado pueden agruparse de la siguiente forma:

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS:

- Participación en el Subgrupo de Tecnología
- Finalización del proyecto EDPB/ETicas sobre IA
- Co-ponentes en la “Guía de Blockchain”
- Co-ponentes en la “Guía de anonimización”
- Co-ponentes en la "Guía de seudonimización"
- Co-ponentes en el drafting team del interplay AIA-GDPR
- Participación en el Mobile Apps Expert Exchange
- Questions on SMEs & Días
- Finalización de la “Coordinated action: Use of cloud based services in the public sector”

AUTORIDADES EUROPEAS:

- Colaboración con la CNIL en herramientas sobre brechas de datos
- Participación en la TaskForce ChatGPT

ENISA:

- Publicación ENISA Engineering Personal Data Sharing (coponentes)
- Participación como observadores en el ENISA's Ad-Hoc Working group en Ingeniería de la Privacidad

EU4DigitalUA:

- Conferencia Internacional en Varsovia AEPD-Autoridad Ucraniana-Autoridad Polaca
- MoU con la Autoridad Ucraniana
- Realización de dos acciones de Internship con un total de 7 miembros de la Autoridad Ucraniana
- Desarrollo de un workshop online de herramientas
- Desarrollo de tres actividades: AA.PP., Retirada de Contenidos, Inteligencia Artificial

BLOCKCHAIN:

- Observadores del European Blockchain Regulatory Sandbox

PET´s:

- Reunión con la Global PET Network of DPAs

2.2.8 Acciones de difusión

Las acciones de difusión realizadas desde la DIT vienen a dar respuesta a los nuevos planteamientos que los desarrollos tecnológicos suponen con relación a la privacidad y la protección de los derechos y libertades de las personas físicas. En particular cuando estos desarrollos tecnológicos son novedosos, o bien, cuando se muestran errores de concepto en las consultas planteadas a la AEPD o en los foros en los que participan miembros de esta División.

La respuesta a estos planteamientos novedosos o a estas dificultades de concepto se realiza mediante documentos breves en forma de artículos de carácter tecnológico publicados, por lo general, en el **blog de la AEPD**, los artículos publicados durante 2023 fueron los siguientes:

1. Neurodatos II
2. Revisión de medidas de privacidad
3. Riesgo de reidentificación
4. Análisis de comportamiento de usuarios (UEBA) y protección de datos

5. AI-1: Sistema vs Tratamiento
6. Federated Learning: Inteligencia Artificial sin comprometer la privacidad
7. Inteligencia Artificial: principio de exactitud en los tratamientos
8. Carpeta Ciudadana: Transparencia de las AAPP y ejercicio de los derechos de los ciudadanos
9. Monedas digitales
10. Inteligencia Artificial: Transparencia
11. Espacios de datos, soberanía y protección de datos desde el diseño
12. Datos sintéticos y protección de datos
13. Sistema de Inteligencia Artificial: ¿solo un algoritmo o varios algoritmos?

Asimismo, la DIT participa en los webinarios desarrollados dentro de la cuarta temporada del ciclo mujer y ciencia, que se enmarca en el ámbito de las actividades de responsabilidad social de la AEPD y en el que se viene a poner de relieve el prestigio y liderazgo de la mujer en el ámbito de la ciencia y la tecnología y donde mujeres de reconocido prestigio cuentan en primera persona su visión como profesionales con relación a la protección de datos personales.

Durante esta cuarta temporada se desarrollaron las siguientes **conferencias**:

- **Dependencia online, desinformación, manipulación, acoso y vigilancia**, Esther Paniagua
- **Viaje al mundo de la ingeniería de la privacidad**, Isabel Barberá
- **El futuro de la criptografía**, María Isabel González
- **¿Podemos considerar las brechas de datos un tipo de cibercrisis?**, Cristina del Real

3. Al servicio de los ciudadanos. La protección de las personas en un mundo digital

El equipo de atención al ciudadano, de conformidad con las funciones atribuidas a la AEPD por los artículos 57.1.b) y e) del RGPD y 47 de la LOPDPGDD; y la Instrucción 1/2021 de la AEPD, ha contestado en 2023 más de 50.000 consultas individuales de los ciudadanos, escritas, formuladas a través de la sede electrónica, telefónicas y mediante la atención presencial.

En todas las respuestas se ha informado y sensibilizado a los 51.544 ciudadanos que han consultado a la Agencia sobre sus derechos de protección de datos, cómo ejercerlos y la posibilidad de formular reclamaciones; y, además, se ha procurado facilitar la comprensión de los riesgos, garantías y derechos relacionados con los tratamientos de datos que les afectan.

Además de estas actuaciones consultivas, una importante novedad que refuerza la promoción informativa de la Agencia ha sido la puesta en marcha, en abril de 2023, de un canal de atención continuada (24h x 7d) e inmediata a las dudas y preguntas más habituales. Este canal se ofrece a través de la página web de la Agencia y se identifica en la web con un globo azul. El nuevo canal se presta a través de un mecanismo de Chatbot y ofrece la posibilidad de que, si no se encuentra la ayuda en la respuesta robótica, se deriva la consulta a un operador personal.

Los resultados del Chatbot en su primer año de funcionamiento han sido excelentes, arrojando unas cifras de 17.337 consultas resueltas en 7 meses de funcionamiento y con un nivel de satisfacción reportado por los propios usuarios del 75%. Toda la base del conocimiento del Chatbot ha sido preparada por equipo de atención al ciudadano de la Agencia y se actualiza regularmente adaptándolo a los cambios normativos y de criterio que se producen.

Conviene subrayar que la **actividad consultiva de la Agencia se ha incrementado en un 48,33% respecto al año anterior**, lo que ha puesto de manifiesto el compromiso del equipo de atención al ciudadano.

También, como en años anteriores, **se han actualizado las preguntas frecuentes** (FAQs, por su acrónimo inglés) publicadas en la web de la AEPD, con la finalidad de acercar y hacer más accesible y ágil el acceso de los ciudadanos a las cuestiones más demandadas en protección de datos.

Respecto de las materias objeto de las consultas, a lo largo del año 2023 las consultas más frecuentes han sido las relacionadas con reclamaciones, seguidas por las consultas sobre la aplicación del Reglamento General de Protección de Datos y derechos.

En este año cabe **señalar** un número importante de consultas referidas al **control horario mediante datos biométricos** y también sobre **llamadas publicitarias de comercializadores de energía**, aun en casos en los que los ciudadanos se encontraban en la lista de exclusión publicitaria.

Respecto de las **quejas recibidas**, se observa lo siguiente:

- Una utilización inadecuada del formulario de queja, que se usa para comunicar la oposición o desacuerdo ante determinados tratamientos de datos: publicidad spam, acoso publicitario, ficheros de morosos y cámaras de vídeo vigilancia conflictiva. **Se trata de "quejas" frente a la actuación de otros responsables, o terceros, pero no del funcionamiento de la Agencia**. Estas mal llamadas quejas se canalizan y responden como consultas y computan a efectos estadísticos como consultas.

- También se han recibido **quejas relacionadas con problemas de acceso a la web**, y con el uso de formularios para interponer reclamaciones, cuyo uso se puso en marcha este año.

- En el período de referencia, de un total de **136 registros presentados con formulario de queja, 111 se han tramitado como consulta**, porque no eran propiamente quejas, y solo 25 se han tramitado como quejas.

3.1 Educación y menores

El Área de Educación y Menores **ha recibido 4.049 consultas durante 2023**, cuyo detalle se recoge en la segunda parte de esta Memoria en el apartado La Agencia en cifras. **Esta cifra representa un incremento del 71% respecto al año anterior**.

Las consultas se han categorizado según quién las formula, o desde dónde, tal y como se ha realizado en las Memorias de años anteriores. Los canales habilitados por la AEPD para consultar cuestiones relacionadas con Educación y Menores son: **Sede electrónic**a, correo de **canaljoven@aepd.es**, WhatsApp y teléfono.

Antes de valorar la clasificación de las consultas, hay que destacar el significativo incremento de **llamadas recibidas** durante este año, un total de **2.029**, que representa un **incremento del 63%** frente a las del mismo periodo del año anterior.

Debe precisarse que no todas las consultas recibidas por este medio responden al ámbito del Área de Educación y Menores (1.005), que no han sido incluidas en la clasificación al ser ajenas a su materia.

Tomando en cuenta las consultas del ámbito educativo y de menores de edad y realizando una división por la categoría de "quién realiza la consulta", cabe indicar que la mayoría de ellas proceden de progenitores (52%) sobre los tratamientos de datos de sus hijos, tanto en sus relaciones con terceros (educación, deporte, redes sociales) como en el plano familiar. En este último, se plantean fundamentalmente consultas sobre la publicación por familiares de imágenes en redes sociales. En principio esta difusión se podría valorar como personal o doméstica (art. 2.2.c RGPD) y, por tanto, fuera del ámbito de la normativa de protección de datos, pero la mayoría de las publicaciones las realizan familiares, no solo los progenitores.

Otras consultas recurrentes realizadas por los progenitores son las relacionadas con el tratamiento de datos personales de menores en el ámbito deportivo, cuestión que preocupa cada vez más a las familias, en especial en los casos de la grabación y difusión de imágenes de niños y niñas mientras realizan prácticas deportivas en competiciones organizadas habitualmente por Federaciones deportivas.

En el ámbito educativo, el porcentaje de consultas realizadas por docentes, jefes de estudios y directores de centros educativos, CEIP y IES llega al 11% del total. Las consultas están relacionadas con los tratamientos de datos personales que realizan los centros educativos y, sobre todo, se solicita información de carácter general con el argumento del desconocimiento que se tiene sobre la materia y la carencia de formación en protección de datos.

En cuanto a las consultas que realizan los **profesionales de universidades, un 2%**, la mayoría está centrada en tratamientos de datos con ocasión de la realización de exámenes online o de los trabajos fin de grado y fin de master.

También se han recibido consultas de **empresas privadas (7%)**, normalmente clubes deportivos, empresas de ocio infantil o academias de idiomas o música que tratan datos personales de menores de edad, motivadas por la necesidad de conocer la normativa de protección de datos personales, fundamentalmente en cuanto a tratamientos de videovigilancia y publicación de imágenes en sus webs o redes sociales (RRSS).

En este ámbito concreto cobran especial significado las consultas sobre publicación de imágenes de menores en internet recogidas en actividades organizadas por los propios responsables de las empresas o clubes.

En el apartado de **Organismos Públicos, un 2%**, formulan consultas de las entidades locales. Las dos tipologías más comunes en este ámbito son la publicación de imágenes de menores que desarrollan actividades deportivas en pabellones municipales y la publicación de imágenes en perfiles de RRSS de la entidad local recogidas durante eventos o fiestas populares.

Otro apartado a destacar es el de las consultas formuladas por el **alumnado**, tanto menores como mayores de edad, en este caso de alumnos universitarios (5%). Fundamentalmente las consultas vienen motivadas por la información que los centros educativos y universitarios trasladan a sus progenitores, como pueden ser la información sobre las calificaciones de sus hijos e hijas.

Por último, dentro de esta valoración de las consultas recibidas en 2023, conviene tener en cuenta que se han atendido numerosas consultas, un 14%, realizadas por progenitores o profesionales que quieren reclamar el tratamiento de sus datos personales llevado a cabo tanto por empresas como por Administraciones Públicas. Desde esta Unidad la Agencia facilita información precisa, ya que en múltiples ocasiones no parece que las reclamaciones tengan una base fundada para su admisión por la AEPD. Habitualmente el error viene dado por la todavía creencia de que, para cualquier tratamiento de datos personales, se requiere el consentimiento del interesado.

Al margen de las consultas recibidas en el Área de Educación y Menores, hay que indicar que, desde el **Canal Prioritario de la AEPD**, cuya gestión se lleva por la Subdirección General de Inspección de Datos, se han derivado a esta área un total de 33 reclamaciones formuladas a través del canal específico para menores de edad (14 – 17 años), pero que, al no cumplir los requisitos del Canal Prioritario, se da traslado para su tratamiento como consultas.

Se han podido contestar 29 de ellas y, el resto se archivaron, dado que, entre otras cuestiones, no se disponía de datos de contacto suficientes para poder establecer contacto con los reclamantes.

En el ámbito de la **protección de los menores de edad en el ámbito digita**l se han mantenido durante 2023 las siguientes:

Reuniones

- **Consejo Escolar del Estado** el 9 y 24 de febrero.
- **Grupo de Trabajo Adicciones Digitales y Acceso online por menores a contenidos inadecuados** (actualmente "Menores, salud digital y privacidad), con representantes de diferentes organismos públicos de ámbito estatal para valorar e impulsar iniciativas en materia de acceso, por menores de edad, a contenidos online para adultos y de conductas adictivas a la tecnología que constituyen un grave riesgo para su desarrollo y comportan serias consecuencias en su ámbito familiar, educativo y social, 23 de febrero.
- **Grupo de Trabajo Verificación de edad**, con representantes de diferentes organismos públicos de ámbito estatal (Ministerio Asuntos Económicos y Transformación Digital, CNMC, FNMT y Ministerio del Interior) sobre la creación de un atributo para la verificación de edad de los menores (+18 años) previa al acceso a contenido inapropiado en internet, (pornografía, apuestas online), 24 de marzo.
- **Grupo de Trabajo Pautas uso responsable de Internet** con el Ministerio de Educación y Formación Profesional, la Delegación del Gobierno para el Plan Nacional sobre Drogas, el INCIBE y los Consejos de Colegios Oficiales de Médicos y Psicólogos, para abordar medidas de actuación frente al uso adictivo o problemático que los menores hacen de las TIC, 29 de marzo.
- **Grupo de Trabajo Uso problemático o adictivo de internet por menores** con los Consejos de Colegios Oficiales de Médicos y Psicólogos, el Ministerio de Educación y Formación Profesional, la Delegación del Gobierno para el Plan Nacional sobre Drogas, el INCIBE, la Dirección General de Salud Pública y el Consejo Escolar del Estado, con el objetivo de abordar medidas de actuación frente a dichas conductas, búsqueda de

recursos para la identificación del problema y medidas de actuación para las familias, 4 de mayo.

- **Asociación Española de Pediatría**. Al objeto de impulsar vías de colaboración, así como la difusión de materiales y contenidos de apoyo a las familias en relación con adicciones comportamentales, 8 de junio.

Colaboración en actividades formativas

- **Curso NOOC Menores y seguridad en Red**, 4ª edición realizada en colaboración con INTEF e INCIBE, con el objetivo de dar a conocer pautas, herramientas y estrategias que permitan evitar los riesgos de un uso inadecuado o poco seguro de la red, y orientar y acompañar a los menores en el entorno digital y salvaguardar su intimidad y bienestar personales. Dirigido a toda la comunidad educativa. Se matricularon de 1.583 alumnos.
- **Curso MOOC Educar en seguridad y privacidad digital**, 2ª Edición gestionada desde la plataforma educativa de cursos abiertos en línea de INTEF en el que participan INCIBE, INTEF y AEPD. En esta edición se han matriculado 1.372 alumnos, con un perfil docente.
- **Curso Tutorizado Protección de datos personales en centros educativos**, 3ª Edición 3, organizado por INTEF y AEPD, participan 150 profesores de centros no universitarios e inspectores de educación de las distintas CCAA.
- Participación AULA 23 (IFEMA), 25 de marzo, en colaboración con el Consejo Escolar del Estado, formando a representantes de 30 AMPAS.
- Aulas Digitales de la Fundación Coca Cola donde se presentó la **Guía que no viene con el móvil** con las 10 claves que las familias han de tener en la entrega del primer móvil a sus hijos. III Congreso de Familia en Málaga, donde intervendrá en una Mesa Redonda titulada "Desafíos actuales en menores y adolescentes: Acoso en redes sociales. Bullying".
- Conferencia organizada por el Grupo Previsión Sanitaria Nacional, bajo el título Conectados y ¿protegidos?, sobre los riesgos que existen en el uso que los menores hacen de los dispositivos móviles.

Materiales publicados por el Área de Educación y Menores

- **Criterios básicos para el Tratamiento de datos personales en Centros Educativos**, publicado en septiembre.

Difusión de materiales relacionados con menores e internet

- Difusión campaña **"Mas que un móvil"**: envío de la información y documentación sobre la campaña, que incluye la "Guía que no viene con el móvil" a los colaboradores y contactos del Área de Educación y Menores desde Canal Joven, el 12 febrero.
- Difusión Premios Buenas Prácticas educativas 2023, tras la publicación en el BOE de la convocatoria de los Premios de la AEPD, se difunde la información a colaboradores, Consejerías de Educación de las CC. AA, Delegados de Protección de Datos de las Consejerías de Educación de CC. AA, CEAPA, CONCAPA y Asociaciones de Familias a través del Canal Joven, el 22 de mayo.
- Difusión del **Plan Digital Familiar** de la Asociación Española de Pediatría (AEP), definido como una plataforma con información útil sobre el uso adecuado de internet por parte de los niños, niñas y adolescentes y dirigido a familias y pediatras, se envía a través del Canal Joven, el 16 de octubre. La información se ha enviado a los Delegados de Protección de Datos de las Consejerías de Familia, Educación y Sanidad de las distintas CC. AA, y a las Asociaciones de Familias más representativas (CEAPA, CONCAPA …). Además de información general, en la comunicación se ha añadido la **infografía resumen**.
- Difusión de los **Criterios básicos para el Tratamiento de datos personales en Centros Educativos**, 18 de septiembre.

3.2 Comunicación

Las acciones realizadas por Agencia en 2023 han estado acompañadas de sus respectivas iniciativas de comunicación con el objetivo de fomentar su difusión entre la ciudadanía, los responsables y encargados de tratamiento y los delegados de protección de datos. A continuación, se recogen las relacionadas con el departamento de prensa y comunicación, así como la agenda institucional puesta en marcha por la AEPD para fomentar el conocimiento de las mismas.

3.2.1 Redes sociales

X, LinkedIn, YouTube e Instagram

La Agencia ha seguido en 2023 difundiendo materiales y consejos **a través de su perfil en la red social X** (antes Twitter), incrementando en casi 2.000 los nuevos seguidores y con más de 800 tuits publicados este año. **Superó así los 37.600 seguidores**, siendo los tuits más destacados los siguientes: el inicio de actuaciones previas de investigación a OpenAI, los cambios del artículo 66.1 b) de la Ley General de Telecomunicaciones y consejos para familias relacionados con la protección de datos y la educación digital de menores y adolescentes.

La Agencia activó en mayo de 2022 su **perfil en la red social LinkedIn** para ampliar tanto su presencia online en redes sociales como la difusión de los contenidos e iniciativas que realiza, por lo que 2023 es el primer año que puede analizarse su evolución de forma completa. Los temas son comunes con los que la Agencia aborda en otras redes sociales, pero las características propias de LinkedIn permiten explicar los asuntos que se difunden de forma más detallada, generando una reacción directa en los usuarios. El perfil de ha aumentado en más 7.000 los seguidores en 2023, superando los 20.000, con más de 220 post publicados (que fueron vistos por más de un millón de usuarios de LinkedIn -un 36% más que en 2022) y más de 72.000 interacciones. Así, **hubo más de 28.000 reacciones, se dejaron casi 300 comentarios, casi 7.000 usuarios compartieron los posts en su perfil de LinkedIn y pincharon en los enlaces de los posts 37.000 veces**.

Los **temas más destacados** que se publicaron en el perfil de LinkedIn son los siguientes: Inicio de investigación a OpenAI, la modificación de la LOPDGDD, y los cambios del artículo 66.1 b) la Ley General de Telecomunicaciones.

Asimismo, también se ha seguido trabajando en el **perfil que la Agencia mantiene abierto en YouTube**. La AEPD realiza contenidos multimedia con los que pretende facilitar la comprensión de algunos conceptos de protección de datos, así como difundir las iniciativas que lleva a cabo. En el año 2023, ha habido más de 240.000 reproducciones de los vídeos del canal y se han publicado 13 vídeos nuevos.

Este canal engloba **cuatro tipologías** de vídeos:

- la grabación de conferencias, charlas o webinarios organizados por la Agencia;
- vídeos con consejos o recomendaciones;
- videotutoriales para configurar las opciones de privacidad en navegadores, sistemas operativos, redes sociales y apps más populares,
- y las campañas de concienciación realizadas por la AEPD.

De forma agregada, los contenidos más vistos en el canal de la Agencia en YouTube están relacionados con la **configuración de las opciones de privacidad de redes sociales y otros servicios de Internet** (Configura tu privacidad en Facebook, TikTok, YouTube y Whatsapp), además del vídeo de la campaña **'Por todo lo que hay detrás'** (Se suicidó porque todos vieron el vídeo en el que aparecía).

En cuanto a los vídeos más visto de 2023, destaca la campaña **'Cambia el Plan'**, realizada junto a la Asociación Española de Pediatría, así como los vídeos de configuración de la privacidad y los webinarios del ciclo 'Mujer y ciencia', que además de emitirse en directo también se graban y quedan a disposición de los usuarios en el canal de YouTube.

En cuanto a **Instagram**, la Agencia lanzó en septiembre de 2022 su **perfil oficial en la red social** para potenciar tanto su presencia online en redes sociales como la difusión de los contenidos e iniciativas que realiza. 2023 es el primer año completo en el que la Agencia tiene perfil en esta red social. Durante este año se han publicado más de 150 post y casi 35.000 usuarios vieron publicaciones de la AEPD, siendo el contenido más visto la publicación del spot de **'Cambia el plan'**, que llegó también a los usuarios de @enfamiliaaep al hacer una publicación colaborativa.

En número de **'Me gusta'**, la publicación que tuvo más éxito fue la del Canal prioritario de la campaña **'Se suicidó porque todos vieron el vídeo en el que aparecía. No es por el vídeo, es por todo lo que hay detrás'**.

3.2.2 Otras acciones de difusión

• 3.2.2.1 Boletín informativo mensual AEPD

La Agencia elabora y envía un boletín informativo mensual que tiene como destinatarios principales a las entidades adheridas al Pacto Digital, los delegados de protección de datos registrados en la Agencia y las personas y/o entidades que se han inscrito específicamente para su recepción. El objetivo del mismo es agrupar los lanzamientos y novedades de la Agencia orientadas fundamentalmente a responsables de tratamiento, aunque también recoge algunos temas centrados en el ciudadano, así como asuntos que, sin ser novedades, se consideran de utilidad.

El boletín se publica también en la web, lo que permite consultarlo de forma retroactiva y bajo demanda. También se envía a todo el personal de la Agencia, de forma que todas las personas trabajadoras de la AEPD conozcan las novedades sobre las iniciativas puestas en marcha.

• 3.2.2.2 El blog de la Agencia

El objetivo del **blog de la Agencia** es servir como altavoz para la difusión de diferentes iniciativas puestas en marcha, así como informes, guías, infografías o documentos, entre otras materias, aportando una visión cercana tanto del trabajo que se realiza en el organismo como de la protección de datos en un plano global.

Durante 2023 el Blog de la Agencia ha recibido más de 650.000 visitas únicas.

Entre los posts que han despertado un mayor interés se encuentran los relacionados con:

- Difusión de vídeos con contenido violento en redes sociales
- Anonimización y seudonimización
- Empleo de datos biométricos
- Brechas de seguridad de datos personales: qué son y cómo actuar
- Cuándo hay que revisar las medidas de protección de datos
- ¿Pueden los colegios tomar imágenes de los alumnos durante su actividad escolar? ¿Y subirlas a internet?.

• 3.2.2.3 Espacio "Protegemos tu privacidad"

El espacio 'Protegemos tu privacidad' de la **Agencia Española de Protección de Datos y Radio 5** ofrece a los ciudadanos recomendaciones para conocer sus derechos y saber cómo ejercerlos, así como consejos para facilitar el cumplimiento de la normativa a las organizaciones que tratan datos. Se estrena todos los miércoles y se realiza redifusión a lo largo de la semana, y todos los programas emitidos pueden escucharse en cualquier momento en la **página web de Radio 5**. La emisión comenzó el 4 de julio de 2018 y desde entonces se han emitido 201 piezas temáticas, 30 de ellas en 2023.

• 3.2.2.4 Relaciones con los medios

La difusión de la protección de datos por parte de los medios de comunicación es imprescindible tanto para concienciar a los ciudadanos en relación con sus derechos como difundiendo las obligaciones y la forma de cumplir los requerimientos establecidos en la normativa. A lo largo de 2023, **la Agencia atendió más de 500 consultas de medios de comunicación relacionadas con este derecho fundamental**. Esta labor de atención personalizada a los medios se vio complementada con el envío proactivo de notas de prensa a medios y a los departamentos de comunicación de las organizaciones adheridas al Pacto Digital. Asimismo, **estas notas se publican en la página principal de la Agencia, habiendo recibido casi 700.000 visitas**.

Las **seis notas de prensa más consultadas** en 2023 han sido las siguientes:

- **Modificación de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales**
- **La AEPD publica la Circular sobre el derecho de los usuarios a no recibir llamadas comerciales no solicitadas**
- **La AEPD recibió en 2022 el mayor número de reclamaciones de su historia**
- **La AEPD publica una guía sobre protección de datos y relaciones laborales**
- **La AEPD actualiza su Guía sobre el uso de cookies para adaptarla a las nuevas directrices del CEPD**
- **La AEPD inicia de oficio actuaciones de investigación a OpenAI, propietaria de ChatGPT**

Asimismo, en relación con notas de agenda informativa publicadas en la web, la Agencia publicó en 2023 más de 130 reuniones o actos públicos en los que participaron diferentes miembros de esta institución. Esta actividad de comunicación se vio complementada con la participación de la Agencia en las notas de prensa de las reuniones plenarias que periódicamente organiza el Comité Europeo de Protección de Datos (CEPD).

3.3 Agenda institucional

Durante 2023 la Agencia continuó con su misión de fomentar entre ciudadanos y organizaciones la cultura de la protección de datos, así como de contribuir al constante análisis de las implicaciones de la normativa de este derecho fundamental en la actividad de distintos sectores, mediante su participación virtual o presencial en numerosas reuniones, jornadas, foros, congresos, cursos, seminarios web, actos y presentaciones, como entidad organizadora o invitada.

La **relación completa de la agenda institucional** de la AEPD puede **consultarse** en esta sección web.

Dentro del ámbito del sector público, la AEPD participó en diversos foros, congresos, cursos, seminarios, reuniones, jornadas o talleres, como el curso especializado para Delegados de Protección de Datos de las Administraciones Públicas; las II Jornadas de delegados de protección de datos de la Universidad Rey Juan Carlos; las II Jornadas Aragonesas de Protección de Datos, Transparencia y Ciberseguridad, organizadas por la Asociación Aragonesa de Delegados de Protección de Datos; la III Semana Antirracista, organizada por el Ministerio de Igualdad; el curso sobre Sostenibilidad y Tecnología de la Universidad Carlos III de Madrid; la IV Jornada de Protección de Datos del Ayuntamiento de Madrid; el Curso 'Derechos Digitales e inteligencia artificial: más allá de ChatGPT', de la Universidad de Málaga o el seminario 'Retos para la protección de datos en el momento actual', de la Universidad Internacional Menéndez Pelayo (UIMP) de Santander.

Igualmente, participó en el encuentro sobre 'Salud digital basada en valor: hacia el factor humano y la medicina de precisión', organizado por la Consejería de Sanidad del Gobierno de Cantabria y Cluster TERA; el curso 'Nuevos Retos Tecnológicos en la Protección de Datos Personales. Especial Referencia a la Elaboración de Perfiles, Big Data e Inteligencia Artificial', de la Universidad Internacional de Andalucía; la 11ª Conferencia sobre Protección de Datos en las Fuerzas y Cuerpos de Seguridad, organizada por la Red de Expertos de Protección de Datos de Europol (EDEN) en cooperación con el Ministerio del Interior, Policía Nacional y Guardia Civil; el curso 'Administración de justicia y el derecho fundamental a la protección de datos' del Centro de Estudios Jurídicos; el I Congreso de protección de datos en la comunidad educativa, organizado por la Delegación de Protección de Datos de la Generalitat Valenciana y la I Jornada 'La Dimensión Digital de la Violencia contra la Mujer', organizada por la Subdelegación del Gobierno de Segovia.

Otros encuentros en los que la Agencia también participó fueron el I Congreso Internacional de Comunicación Clara de las universidades Rey Juan Carlos, Católica de Murcia y Autónoma de Barcelona; el I Ciclo de diálogos 'Horizonte Iberoamérica Digital', organizado por la Secretaría General Iberoamericana; la I Semana Digital del Ministerio de Industria, Comercio y Turismo; el curso 'Educar en seguridad y privacidad digital' del INTEF; el taller de certificación de las operaciones de tratamiento de datos y como herramienta de transferencias internacionales, organizado por la Comisión Nacional de Protección de Datos de Portugal bajo el impulso del Subgrupo de Cumplimiento Normativo del EDPB que coordina la Agencia; la reunión sobre Inteligencia Artificial organizada por la Cátedra Fundación Íntegra sobre Identidad y Derechos Digitales y por la Cátedra de Privacidad y Transformación Digital Microsoft-Universitat de Valencia, y la Jornada sobre violencia de género organizada por el Ministerio de Justicia.

Por otra parte, en el marco de su Instrucción 1/2021, la Agencia mantuvo un encuentro con Delegados de Protección de Datos de entidades locales (Diputaciones provinciales, Cabildos y Consejos Insulares, capitales de provincia y ciudades de más de 10.000 habitantes), con la finalidad de repasar la situación en las que ejercen sus funciones, e intercambiar opiniones. También lo hizo con representantes de la Asociación de DPD de Parlamentos, con el objetivo de conocer sus objetivos como asociación de reciente creación y contribuir al desarrollo de buenas prácticas.

La búsqueda de **espacios de colaboración para la protección de los menores en el ámbito online** fue una prioridad y una constante durante 2023, que se tradujo en numerosos encuentros con distintas entidades, como el Consejo Escolar del Estado y las organizaciones representantes de padres y madres del alumnado (CEAPA y CONCAPA); Eurochild; la Asociación Española de Pediatría (AEP); la Fundación FAD Juventud y la Asociación Europea para la Transición Digital o la Comisión Nacional de los Mercados y la Competencia, y en la asistencia a actos como la presentación del Plan Digital Familiar de la AEP.

Este objetivo también tuvo su reflejo en la celebración de reuniones con diferentes cargos públicos, encaminadas a abordar el impulso de medidas para la protección de los menores en el mundo digital dentro del marco del Pacto de Estado **'Protegiendo a la infancia y adolescencia en el entorno digital'**, como las mantenidas con la alcaldesa de Santander, Gema Igual Ortiz; el consejero de Educación, FP y Universidades de Cantabria, Sergio Silva, la presidenta del Consejo Escolar de la Comunidad de Madrid, Pilar Ponce Velasco, así como con la directora general de la Asociación de Revistas de Información (ARI), Yolanda Ausín.

Además, la directora de la AEPD mantuvo un encuentro con el fiscal de Sala Coordinador de Menores en la Fiscalía General del Estado, Eduardo Esteban, y la vicepresidenta de la Asociación Europea para la Transición Digital (AETD), Ana Caballero, con motivo del Día Mundial de la Infancia, en el que se expuso la experiencia práctica de la AEPD y las diferentes acciones llevadas a cabo para concienciar a las familias del impacto que puede tener en los menores el uso prematuro y sin control de Internet y las redes sociales, los delitos más frecuentes que sufren los menores en el ámbito digital y las novedades respecto a la propuesta del Pacto de Estado para la protección de los menores de edad en internet y las redes sociales.

La AEPD tuvo reuniones con representantes del Consejo General de la Psicología, el Consejo General de Colegios Oficiales de Médicos, Ministerio de Educación, Plan Nacional sobre Drogas e INCIBE, para abordar las graves consecuencias del uso problemático de las TIC por los menores y el establecimiento de iniciativas de prevención, métodos de detección temprana, basados en la evidencia científica, y ofrecer pautas para las familias y centros educativos.

En marzo de 2023, dentro del marco del Grupo de Trabajo de Menores establecido para la protección de los menores de edad en el ámbito digital, la AEPD convocó una nueva reunión, a partir de la cual se comenzó a trabajar en dos líneas de actuación: una dedicada a los riesgos que el uso problemático o adictivo de las tecnologías digitales y a sus consecuencias y cómo prevenir, detectar y atender a estas situaciones, mientras que la segunda orientó sus esfuerzos a trabajar en la verificación de la edad para evitar el acceso online de los menores a contenidos para adultos, en particular la pornografía.

En consecuencia, el Grupo de Trabajo se adecuó a estos objetivos constituyéndose conforme a cada una de las finalidades. Se formó un Grupo Técnico, compuesto por representantes de la Agencia, los Ministerios del Interior, Asuntos Económicos y Transformación Digital, y Defensa, Dirección General de la Policía, CNMC, FNMT y SGAD, encargado de los sistemas de verificación de la edad, en abril de 2023, a la que siguieron diversas reuniones de carácter técnico.

Este intenso trabajo se materializó, antes de finalizar el año, con la adopción por la AEPD de una propuesta de sistema de verificación de edad y protección de las personas menores de edad en Internet ante el acceso a contenidos para adultos, que contempla, entre otros materiales, un **Decálogo de principios** que habrían de cumplir los sistemas de verificación de la edad para ser eficaces y respetuosos con los derechos y libertades de las personas, en particular con el derecho a la protección de datos de carácter personal y la privacidad, así como una **nota técnica** con los detalles del proyecto y **tres vídeos prácticos** que demuestran cómo funciona el sistema en diferentes dispositivos, con sistemas operativos distintos y empleando varios proveedores de identidad.

La propuesta de sistema de verificación de edad, el Decálogo y el resto de los materiales **fueron presentados públicamente el 14 de diciembre** con motivo del 30º Aniversario de la Agencia, por la directora de la AEPD, Mar España, la consejera de la Comisión Nacional de los Mercados y la Competencia (CNMC), Pilar Sánchez Núñez, y la presidenta-directora de la Fábrica Nacional de Moneda y Timbre (FNMT), Isabel Valldecabres. Esta presentación supondría el inicio de una ronda de encuentros con grandes empresas de internet como Google, Meta o TikTok, para trasladarles la propuesta y demostrar que técnicamente es posible proteger a los menores del acceso a contenidos inadecuados a la vez que se garantiza el anonimato de los adultos en su navegación por internet.

Por otra parte, en el marco de las relaciones de cooperación institucional entre autoridades, la AEPD asistió en Barcelona a una reunión organizada por la Autoridad Catalana de Protección de Datos, en la que también participaron la Agencia Vasca de Protección de Datos (AVPD) y el Consejo de Transparencia y Protección de Datos de Andalucía. La Agencia también mantuvo un encuentro con representantes de la AVPD, ambas en el marco de las relaciones de cooperación institucional entre autoridades.

Finalmente, la AEPD continuó impulsando iniciativas para fomentar el **Pacto Digital para la Protección de las Personas**, como los encuentros mantenidos con la Asociación de Medios de Información (AMI) y el fiscal de Sala coordinador de la Unidad de Menores, Eduardo Esteban Rincón; con la Fundación Mapfre, así como con representantes de ASISA para la firma por parte de esta de la adhesión al citado Pacto Digital.

En el ámbito privado, la AEPD participó en el seminario 'Privacy Day' de la Asociación de Expertos Nacionales de la Abogacía Tecnológica (ENATIC); el Foro Artes y Humanidades del Círculo de Bellas Artes; el XX Foro de Seguridad y Protección de Datos de Salud, organizado por la Sociedad Española de Informática de la Salud (SEIS); el XV Foro de la Privacidad de ISMS Forum; la mesa 'Menores, tecnología y sociedad futura', organizada por la Sección de Derechos Civiles del Ateneo de Madrid; el III Curso de Derechos Humanos en la Policía Nacional; el II Congreso sobre el Derecho a la Autonomía Personal 'La tecnología en la vida cotidiana de las personas mayores', organizado por la Unión Democrática de Pensionistas y Jubilados y la Fundación Telefónica; el programa Aulas Digitales de la Fundación Coca-Cola; la Jornada sobre Protección de Datos e Investigación Sanitaria o el IX Congreso Internacional de Privacidad de la Asociación Profesional Española de Privacidad.

Además, participó en el III Congreso de Familia en Málaga; el 41 Symposium de la Asociación Española de Farmacéuticos de la Industria (AEFI); el webinario ENATIC Privacy 2023; la II Jornada sobre Seguridad y Privacidad: Derechos y obligaciones de las Fuerzas y Cuerpos de Seguridad en materia de protección de datos, organizada por ECIJA y la International Police Association (IPA) Madrid; una sesión informativa con alumnos de la facultad de Derecho de Stetson University de Florida; la sesión 'Nuevo marco para la realización de transferencias internacionales a Estados Unidos', organizada por la Fundación para la Investigación sobre el Derecho y la Empresa (FIDE); la jornada sobre 'Prevención temprana de la ciberviolencia de género en jóvenes', organizada por la Fundación Diagrama y la IV edición de la Jornada Ciudadanía Conectada, organizada por Pantallas Amigas.

La sesión de trabajo 'Generación XXX. Por un control efectivo del acceso de los menores a la pornografía', organizado por la Asociación Dale una Vuelta; el Foro 'Directivos Innovación y Gobierno en Sanidad Privada', organizado por Pfizer; la conferencia 'Conectados y ¿protegidos?' del grupo Previsión Sanitaria Nacional; la Jornada Internacional de Seguridad de la Información de

ISMS Forum; las III Jornadas 'Contra el Maltrato, Tolerancia Cero' de la Fundación Mutua Madrileña y Atresmedia; el evento Tendencias 2023, organizado por el diario El País y el acto de inauguración de la nueva Sección de Infancia y Adolescencia del Ilustre Colegio de Abogados de Madrid (ICAM) fueron otros actos en los que también participó la Agencia.

La AEPD también mantuvo reuniones con representantes de las operadoras de telecomunicaciones; de la fundación Pro-Bono España; de la Asociación Española de Abogados de Familia (AEAFA); de la Asociación Española de Banca; de Secuware; de Women4Cyber Spain (W4C Spain); de UPS y UNO (patronal de logística y transporte); de UNESPA; con una representación de los sectores relacionados con la actividad publicitaria, así como con Google, Meta y Orange.

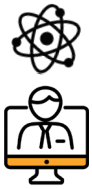
En este marco, la Agencia también se reunió con representantes de fundaciones y asociaciones, como la Asociación de la Industria de la Computación y las Comunicaciones (CCIA, por sus siglas en inglés); la European Association for Digital Transition; la Asociación Canal Sénior y la Asociación EMANCIPATIC.

Por otro lado, la Agencia exploró las implicaciones que plantean los avances científicos en torno a los neurodatos para la protección de datos personales, mediante un encuentro con el neurobiólogo Rafael Yuste.

La Agencia siguió organizando su 'Espacio de estudio sobre Inteligencia Artificial', un encuentro periódico de debate que congrega a un grupo multidisciplinar de expertos en la materia con el objetivo de fomentar un entorno de diálogo donde abordar ideas sobre los retos actuales que se plantean en el marco de la Inteligencia Artificial (IA), así como nuevos desafíos, perspectivas, desarrollos, inquietudes y posibles iniciativas, para facilitar el desarrollo de una IA que respete los principios éticos y de protección de datos. En 2023 celebró su tercer y cuarto encuentro. A estos eventos hay que añadir la celebración de "DATA SPACES IN EU: Synergies between data protection and data spaces, EU challenges and experiences of Spain", organizado por la AEPD y la Agencia de la Unión Europea para la Ciberseguridad (ENISA), con el objetivo de abordar las Iniciativas Europeas de Espacios de Datos desde la perspectiva de la privacidad.

Igualmente, la Agencia organizó jornadas sobre distintas materias, como el Encuentro 'Mayores en el entorno digital', organizado conjuntamente con la Plataforma de Mayores y Pensionistas (PMP); una jornada de calidad normativa en protección de da tos; el Ciclo de Foros Virtuales sobre 'Retos para la protección de datos ante los avances tecnológicos', organizado junto con la Agencia Española de Cooperación Internacional para el Desarrollo (AECID); y moderó el webinario organizado por la Agencia Española de Cooperación Internacional para el Desarrollo (AECID) sobre digitalización y menores, en el que también participaron representantes de UNICEF España, el INTEF, del Ministerio de Educación y Formación Profesional, y la Asociación Europea para la Transición Digital.

La Agencia organizó en 2023 un nuevo ciclo de webinarios sobre 'Innovación y Protección de datos. Mujer y Ciencia', con cuatro sesiones de debate digitales para analizar diversos aspectos relacionados con la ciencia y la tecnología.



Asimismo, cabe destacar la firma de Protocolos Generales de Actuación con la Plataforma de Mayores y Pensionistas (PMP), la Fundación Instituto Internacional de Tecnología y Derecho Digital y el Consejo General de Colegios Oficiales de Médicos, respectivamente, para establecer un marco de cooperación y colaboración en beneficio de los derechos y libertades de las personas en el tratamiento de sus datos personales. Dentro de este marco, la Agencia también suscribió un Protocolo General de Actuación con el Consejo General de Colegios Oficiales de Psicólogos dirigido a incrementar la eficacia de las medidas de atención a las personas afectadas por la violencia digital, especialmente mujeres, menores y miembros de colectivos vulnerables, cuando sus datos se hayan obtenido y difundido ilegítimamente a través de Internet.

En el ámbito internacional, la Agencia siguió participando en las reuniones plenarias y los subgrupos del Comité Europeo de Protección de Datos (CEPD), y celebró encuentros con otros reguladores a escala internacional, como la reunión virtual con la Autoridad de Protección de Datos del Reino Unido (el ICO, por sus siglas en inglés) o el XIII Encuentro Ibérico de Autoridades de Protección de Datos, celebrado entre las Autoridades de Protección de Datos de España y Portugal.

En el marco de la Red Iberoamericana de Protección de Datos Personales (RIPD), la AEPD participó en el XX Encuentro de la RIPD celebrado en Santa Cruz de la Sierra (Bolivia); en el encuentro conmemorativo del XX aniversario de esta Red, celebrado en La Antigua (Guatemala), así como en la sesión informativa online sobre ChatGPT celebrada en el marco de la acción común coordinada por la RIPD.

Dentro del capítulo de citas internacionales en el campo de la protección de datos y la privacidad, la Agencia asistió y participó en la 45th Global Privacy Assembly, celebrada en Bermudas; el Privacy Symposium, celebrado en Venecia, o la Conferencia de Primavera, organizada por la Autoridad Húngara de Protección de Datos y celebrada en Budapest.

Dentro de este contexto, la AEPD recibió a una delegación del Defensor del Pueblo ucraniano, que visitó la Agencia para realizar un período de prácticas en el marco del proyecto 'Refuerzo de EU4DigitalUA: fortalecimiento institucional, comunicación y protección de datos', financiado por la Unión Europea y gestionado por la Fundación Internacional y para Iberoamérica de Administración y Políticas Públicas (FIIAPP). A esta visita se une la recibida por una delegación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación de Bolivia (AGETIC), para conocer el marco normativo sobre protección de datos, las funciones de la Agencia como autoridad encargada de velar por el cumplimiento de dicha normativa, así como las herramientas y guías desarrolladas por la Agencia para facilitar el cumplimiento.

Hay que señalar, asimismo, que la AEPD y el Supervisor Europeo de Protección de Datos (EDPS) firmaron un Memorando de Entendimiento (MOU) con el objetivo de promover la cooperación entre ambas autoridades para difundir el derecho a la protección de datos y proporcionar un marco para el intercambio de conocimientos técnicos y mejores prácticas.

Finalmente, el Consejo Consultivo de la Agencia de Protección de Datos -órgano colegiado de asesoramiento a la dirección de la Agencia – mantuvo reuniones el 11 de julio y el 11 de diciembre de 2023 para exponer y analizar la actividad de la institución.

3.4 Infografías

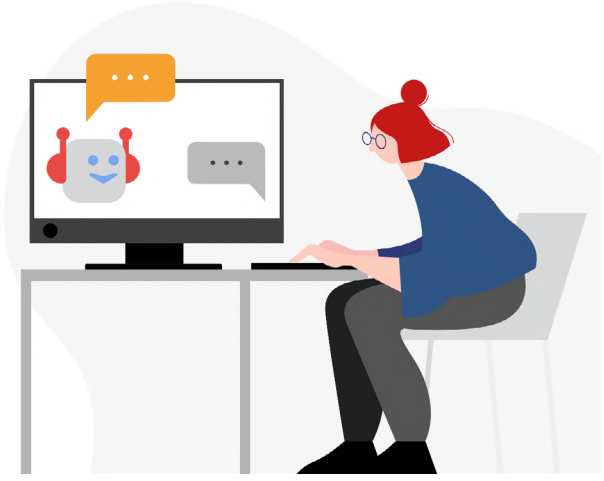
La AEPD publicó en 2023 varias infografías como complemento a la información facilitada a través de sus canales. Todas ellas están disponibles en una sección específica de la página web de la Agencia y, aunque varias de ellas abordan temas que ya han sido tratados en formatos como guías u otros documentos más extensos, desde la Agencia se considera que este tipo de información puede ayudar tanto a los ciudadanos como a los responsables a abordar diferentes materias relacionadas con la protección de datos de una forma simplificada.

En 2023 se han publicado o actualizado las siguientes **infografías**:

Responsabilidad de los y las menores (y de sus padres y madres) por los actos cometidos en Internet

- Recomendaciones para familias del Plan Digital Familiar
- Cómo afectan las pantallas a la salud
- Criterios para el tratamiento de datos personales en centros educativos
- Consejos básicos para familias sobre La guía que no viene con el móvil

- Recomendaciones para usuarios en la utilización de chatbots con Inteligencia Artificial



- Derecho a no recibir llamadas comerciales no solicitadas

3.5 Presentaciones

La AEPD continuó en 2023 con su compromiso de fomentar la cultura de protección de datos entre los ciudadanos y organizaciones a través de diferentes acciones de divulgación.

A continuación, se recogen las presentaciones organizadas por la Agencia o en colaboración con otras entidades que contaron con la presencia de medios de comunicación:

- **Presentación de los criterios de verificación de edad de la Agencia para acceder a páginas web con contenidos inadecuados para menores y celebración del 30 aniversario de la Agencia (14 de diciembre)**

La directora de la Agencia Española de Protección de Datos (AEPD), Mar España; la presidenta en funciones de la Sala de Supervisión Regulatoria de la Comisión Nacional de los Mercados y la Competencia (CNMC), Pilar Sánchez; y la presidenta-directora de la Fábrica Nacional de Moneda y Timbre (FNMT), Isabel Valldecabres, mantuvieron un encuentro con la prensa en el que se presentaron los criterios de verificación de edad elaborados por la Agencia y los siguientes pasos que se van a dar para evitar el acceso por parte de los menores a contenidos inadecuados en Internet. En el encuentro la Agencia presentó una propuesta práctica y efectiva de sistema de verificación de edad y protección de las personas menores de edad en Internet ante el acceso a contenidos para adultos.

Con la presentación de este sistema -compuesto de un **Decálogo que recoge los principios que debe cumplir un sistema de verificación de edad**, **una nota técnica con los detalles del proyecto** y **tres vídeos prácticos sobre el funcionamiento del sistema en diferentes dispositivos**- se demostró que es técnicamente posible proteger a los menores del acceso a contenidos inadecuados a la vez que se garantiza el anonimato de los adultos en su navegación por internet. Tras la rueda de prensa tuvo lugar el acto de celebración del 30 aniversario de la creación de la AEPD.

El evento comenzó con una intervención de la directora de la Agencia en la que repasó los 30 años de experiencia de la AEPD, tras la cual, la presidenta del Comité Europeo de Protección de Datos (CEPD), Anu Talus, llevó a cabo una ponencia donde compartió la experiencia del Comité Europeo. A continuación, se celebró una mesa redonda dedicada al 'Pacto de Estado para la protección a la infancia y adolescencia en el entorno digital y la incidencia de los dispositivos electrónicos en la salud y privacidad de los menores ', en la que participaron la vicepresidenta de la Asociación Europea para la Transición Digital, Ana Caballero; la fiscal de la Unidad de Menores (Fiscalía General del Estado), Rosa María Henar Hernando García; la fiscal de Criminalidad Informática, Patricia Rodríguez Lastras; el director del Instituto Nacional de Tecnologías Educativas y de Formación de Profesorado (INTEF), Julio Albalad Gimeno; y el presidente de la Asociación Española de Pediatría, Luis Carlos Blesa Baviera.

Posteriormente, se inició la mesa dirigida a analizar los 'Criterios para la protección de los menores en el acceso a contenidos de adultos', que contó con la participación del director de la División de Innovación Tecnológica de la AEPD, Luis de Salvador Carrasco; el presidente del Consejo General de Colegios de Ingeniería en Informática, Fernando Suarez Lorenzo; la directora de Telecomunicaciones y del sector Audiovisual de la CNMC, Alejandra de Iturriaga Gandini; el comisario y DPD de la Dirección General de la Policía, Félix Jodra Abuelo; la subdirectora general de Ordenación de los Servicios de Comunicación Audiovisual (SETELECO), Cristina Morales Puerta, y la directora de Servicios Digitales e Innovación de la FNMT, Raquel Poncela González.

Finalmente, el fiscal general del Estado, Álvaro García Ortiz, y el ministro de la Presidencia, Justicia y Relaciones con las Cortes, Félix Bolaños García, fueron los encargados de clausurar el acto.

Convocatoria de la Agencia Española de Protección de Datos, Fiscalía General del Estado –Sala del Menor– y la Asociación Europea para la Transición Digital con motivo del Día Mundial de la Infancia (20 de noviembre)

La directora de la Agencia; el Fiscal de Sala Coordinador de Menores en la Fiscalía General del Estado, Eduardo Esteban, y la vicepresidenta de la Asociación Europea para la Transición Digital (AETD), Ana Caballero, mantuvieron un encuentro con la prensa con motivo del Día Mundial de la Infancia.

Durante el mismo se expuso la experiencia práctica de la AEPD y las diferentes acciones que se están llevando a cabo para concienciar a las familias del importante impacto que puede tener en los menores el uso prematuro y sin control de Internet y las redes sociales; los delitos más frecuentes que sufren los menores en el ámbito digital por parte de la Fiscalía de Menores y las novedades respecto a la propuesta de **Pacto de Estado para la protección de los menores de edad en internet y las redes sociales**, liderada por la AETD y consensuada con Fundación ANAR, Save The Children, Dale una Vuelta, iCMedia y Unicef, y que cuenta con el apoyo institucional tanto de la AEPD como de la Fiscalía General del Estado.

Presentación Plan Digital Familiar (14 de septiembre)

La Agencia colaboró con la Asociación Española de Pediatría (AEP) en la presentación del **Plan Digital Familiar**, que contó con la participación de los doctores Guillermo Martín Carballo, vicepresidente de Atención Primaria de la AEP, y María Salmerón Ruíz, coordinadora del grupo de trabajo de Salud Digital del Comité de Promoción de la Salud de la AEP, y Mar España Martí, directora de la AEPD.

El Plan Digital de la AEP, que cuenta con el respaldo de la Agencia Española de Protección de Datos, se materializa en una plataforma con información útil sobre el uso adecuado de internet por parte de los menores para familias y pediatras. Incluye, además, un documento que las familias pueden personalizar y adaptar a sus circunstancias particulares con recomendaciones científicas en función de la edad de sus hijos y otras generales para todos los miembros. La colaboración establecida para la difusión específica del Plan Digital Familiar se detalla en el apartado 'Iniciativas de colaboración' de esta Memoria.

Curso Universidad Internacional Menéndez Pelayo 2023 (5-7 de julio)

La Agencia impartió del 5 al 7 de julio el seminario **'Retos para la protección de datos en el momento actual'**. El seminario, organizado por la Agencia Española de Protección de Datos (AEPD) y la Universidad Internacional Menéndez Pelayo (UIMP) en el marco de los Cursos de Verano de Santander, está dirigido por la directora de la AEPD, que compareció ante los medios de comunicación para dar a conocer los principales retos a los que se enfrenta la AEPD y la importancia de este derecho fundamental, entre otros, el tratamiento de datos personales de menores y el impacto de la Inteligencia Artificial.

Presentación del Pacto de Estado para proteger a los menores de edad en internet y las redes sociales (22 de junio)

Seis entidades de la sociedad civil -la Asociación Europea para la Transición Digital, Save The Children, Fundación ANAR, iCMedia, Dale Una Vuelta y Unicef- presentaron el 22 de junio en el Ateneo de Madrid una propuesta de **Pacto de Estado acerca de la protección de los menores de edad en internet y las redes sociales**. Esta propuesta, cuenta con el apoyo institucional de la Agencia Española de Protección de Datos.

Premios Protección de Datos 2022 (26 de enero)

El 26 de enero la AEPD realizó la entrega de los 'Premios Protección de Datos 2022'. 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. Los premios entregados corresponden a las categorías de Comunicación; Proactividad y buenas prácticas en el cumplimiento del Reglamento y la LOPDGDD; Buenas prácticas educativas; Investigación 'Emilio Aced'; Emprendimiento 'Ángela Ruiz Robles' y Buenas prácticas para una mayor protección de las mujeres frente a la violencia digital. El detalle de las iniciativas premiadas se recogen en un apartado específico posterior de esta Memoria.

- **Acto de presentación 'Los códigos de conducta como instrumento para fomentar la resolución ágil de controversias' (17 de enero)**

Con motivo de la aprobación de la modificación del **Código de conducta de AUTOCONTROL 'Tratamiento de datos en la actividad publicitaria'**, que recoge una vía para resolver de forma más ágil las reclamaciones en materia de protección de datos y publicidad que puedan plantear los ciudadanos, la Agencia organizó un acto de presentación del mismo. El evento fue inaugurado por la directora de la AEPD, Mar España, y contó con la presencia del director general de AUTOCONTROL, José Domingo Gómez Castallo, y de las operadoras de telefonía Másmóvil, Orange, Telefónica y Vodafone, que suscribieron su adhesión al mismo.

3.6 Iniciativas de colaboración y difusión

3.6.1 Apoyo a la propuesta de Pacto de Estado "Protegiendo a la infancia y adolescencia en el entorno digital"

La AEPD apoya la propuesta de **Pacto de Estado para la protección de los menores de edad en internet y las redes sociales** lanzada por la Asociación Europea para la Transición Digital, promotora de la iniciativa, Save The Children, Fundación ANAR, iCMedia, Dale la Vuelta y UNICEF.

El punto de partida de esta iniciativa, la primera de este calado en la que participan las organizaciones más representativas de protección a la infancia, ha sido la preocupación compartida sobre los riesgos que afrontan niños, niñas y adolescentes en estos entornos, al utilizar servicios diseñados para adultos, que pueden afectar a su socialización y potenciar posibles problemas de salud mental, como la ansiedad y la depresión, además de facilitar situaciones de violencia como el acoso escolar y sexual. Además, los dispositivos móviles se han convertido en una puerta a contenidos pornográficos, lo que genera una banalización de las relaciones sexuales, sexualización precoz y exposición a contenidos inapropiados. Por último, los firmantes también advierten sobre la captación masiva de datos de los menores, con vistas a su perfilado para la venta a terceros con fines publicitarios.

Las medidas propuestas inciden en la necesidad de asumir el problema, formar a profesionales para afrontarlo, y desarrollar la legislación vigente para que todos los actores implicados asuman su responsabilidad ante una población vulnerable como son los niños, niñas y adolescentes. Las propuestas atañen a varios niveles de la Administración Pública.

3.6.2 Actualización de los vídeos Protege tu privacidad: Whatsapp, Instagram, TikTok

La AEPD actualizó en 2023 sus vídeos de configuración de la privacidad y seguridad de **Instagram**, **TikTok** y **Whatsapp**. Los vídeos se inician con una breve introducción explicando qué es y para qué se utiliza cada servicio. A continuación, realizan un tutorial que guía a los usuarios paso a paso a través de las opciones de configuración de privacidad y seguridad de cada uno de estos servicios, ofreciendo recomendaciones para optar por el mayor grado de privacidad posible.

3.6.3 Difusión especifica del Canal prioritario y de las responsabilidades en las que se puede incurrir al difundir contenido sensible, y de las que pueden tener que responder solidariamente sus padres y madres

A finales de septiembre de 2023, se conoció un caso de las fotos manipuladas con inteligencia artificial que mostraban niñas desnudas, utilizando la cara real de las jóvenes y cuerpos falsos generados con Inteligencia Artificial. Es lo que se ha dado en denominar como deepfakes sexuales; una práctica que se ha popularizado gracias a nuevas herramientas tecnológicas al alcance de cualquiera y que puede suponer una infracción de la normativa de protección de datos e incluso un delito.

La repercusión que este caso tuvo en medios y las consultas de prensa planteadas ante la Agencia llevó a la difusión específica del Canal prioritario (para solicitar la retirada urgente de las imágenes si estas se hubieran publicado en páginas de Internet) y a las responsabilidades administrativas, civiles y penales en las que podían haber incurrido los menores autores de esas imágenes y de su difusión. Además, la Agencia anunció que iniciaba una investigación de oficio.

En este contexto, la visibilidad de la AEPD se situó en un total de 452 noticias. El impacto en audiencia superó los 92 millones, con un retorno económico de más de 2,8 millones de euros.

3.6.4 Colaboración con el Ministerio de Función Pública

En marzo de 2023 la Agencia **realizó un vídeo para promocionar el talento público** con la participación de varias personas trabajadoras en la Agencia.

3.6.5 Divulgación de proyectos con FIIAPP

Las divisiones de Innovación Tecnológica e Internacional participaron en 2023 en sendos proyectos junto con la FIIAPP. La primera lidera el componente de protección de datos del proyecto EU4DigitalUA que la FIIAPP implementa en Ucrania. La segunda participa en la alianza digital entre la UE y América Latina y Caribe, en la que se enmarca el proyecto europeo Diálogos Políticas y regulaciones digitales, que cuenta con participación de personal de la AEPD. Esta colaboración se ha plasmado en varias iniciativas de difusión online conjunta y coordinada.

3.6.6 Fomento del Canal prioritario - 8 marzo

Con motivo del día internacional de la mujer, la Agencia publicó los datos correspondientes a 2022 del Canal prioritario, haciendo un llamamiento a denunciar la publicación de contenido sexual o violento publicado sin consentimiento. Las cifras revelaron que **un amplio porcentaje de las intervenciones realizadas en 2022 se trataba de violencia digital contra mujeres y niñas, aglutinando un 70% de los casos** que se denuncian en el Canal prioritario.

3.6.7 Colaboración con Eurochild

En marzo de 2023 la Agencia adaptó al inglés dos de las infografías del Canal prioritario a petición de Eurochild, que quería difundir la información de este Canal en el grupo de trabajo que mantienen con 26 organizaciones en 21 países europeos para trabajar en seguridad de niños y adolescentes online. El objetivo, además de difundirlo como buena práctica, es que esas organizaciones puedan abogar por el establecimiento de algún mecanismo similar a nivel nacional.

3.6.8 Convenio con RTVE

La Agencia y RTVE firmaron un convenio que posibilita la cooperación de servicio público entre las dos instituciones. Mediante el mismo, RTVE colabora en la difusión de las actividades organizadas por la AEPD que sean consideradas de especial relevancia e interés, además de producir en sus instalaciones, con sus propios medios técnicos, el espacio semanal 'Protegemos tu privacidad' que se emite en Radio 5. Asimismo, los espacios se alojan en la plataforma digital RTVE Play Radio.

3.6.9 Cuarta edición del curso online 'Menores y seguridad en la Red', organizado por la AEPD, INCIBE e INTEF

La Agencia, el Instituto Nacional de Ciberseguridad (INCIBE) y el Instituto Nacional de Tecnologías Educativas y de Formación de Profesorado (INTEF) lanzaron la **4ª edición del curso online gratuito 'Menores y seguridad en la Red'**, que tuvo lugar del 7 al 16 de junio. La Agencia contribuyó a la difusión del mismo, tanto a través de su web de menores, sus redes sociales y su blog.

3.6.10 MOOC 'Educar en seguridad y privacidad digital' 2023

La Agencia, en colaboración con el Instituto Nacional de Ciberseguridad (INCIBE), dependiente del Ministerio de Asuntos Económicos y Transformación Digital, y el Ministerio de Educación y Formación Profesional, a través del Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF), realizaron un curso de formación gratuito en formato MOOC, dirigido a los docentes, durante diciembre de 2023. Al igual que con el mencionado anteriormente, la Agencia colaboró también con la difusión del mismo, tanto a través de su web de menores, sus redes sociales y su blog.

3.7 Campañas de difusión

Presentación de los criterios de verificación de edad

La Agencia presentó en diciembre de 2023 una propuesta efectiva de sistema de verificación de edad y protección de las personas menores de edad en Internet ante el acceso a contenidos para adultos, demostrando que es técnicamente posible proteger a los menores del acceso a contenidos inadecuados a la vez que se garantiza el anonimato de los adultos en su navegación por internet.

La visibilidad de la AEPD en el contexto del desarrollo de un sistema de verificación de edad para acceder contenido online para adultos fue inmediata (periodo 16-19 de diciembre), situándose en más de 300 noticias.

El impacto conseguido superó los 66 millones, con un retorno económico de más de 2,2 millones de euros.

Campaña 'Cambia el plan'

La Agencia Española de Protección de Datos y la Asociación Española de Pediatría (AEP) lanzaron en octubre de 2023 su campaña 'Cambia el plan', una iniciativa para promover la salud digital de los menores a través de la concienciación de sus padres y madres, reduciendo los riesgos que supone a nivel físico, mental, sexual y social el uso intensivo y sin control de las pantallas. La campaña promueve la utilización del **Plan Digital Familiar**, una plataforma con información útil sobre el uso adecuado de los medios digitales por parte de los menores para familias y pediatras.

'Cambia el plan' **contó con el apoyo de la Fundación Atresmedia, Mediaset España y RTVE**, entidades adheridas al **Pacto Digital para la Protección de las Personas** de la AEPD que difundieron el spot a través de sus respectivos

canales, y que reforzaron con su participación su compromiso con los derechos de niños, niñas y adolescentes en el entorno digital. La campaña en televisión contó con 66 pases y casi 34 millones de impactos. La colaboración con la AEP, además de la campaña en televisión y redes sociales, también se plasmó en una serie de materiales que aparecen recogidos en el apartado Infografías de esta Memoria.

Además, la campaña **'En Plan' se remitió a las siguientes organizaciones**, de forma que pudieran contribuir a su difusión:

- Consejerías de Educación de las CC.AA, Consejerías de Familias y/o Derechos Sociales de las CCAA, incluidas Ceuta y Melilla, INTEF, Instituto Andaluz de la Mujer, Comisión General de Educación, Consejo Escolar del Estado, Delegados de Protección de Datos de Educación.
- Asociaciones de Padres y Madres: Asociación Estatal de Acogimiento Familiar, Fundación ATENEA, Asociación de Familias por la Convivencia, Asociación de Familias Homoparentales, Asociación de Familias Lesbianas y Gays, Federación de Asociaciones de Madres solteras, Fundación de Familias Monoparentales Isadora Duncan, Unión de Asociaciones familiares, Fundación Mujeres, Observatorio de la Violencia de Género.

Campaña 'Más que un móvil' + La guía que no viene con el móvil con UNICEF España

La Agencia y UNICEF España lanzaron en noviembre de 2022 su campaña **'Más que un móvil'**, dirigida a ofrecer a las familias las claves que deben tener en cuenta antes de entregar a sus hijos e hijas un teléfono móvil. La web Más que un móvil ha recibido más de 130.000 consultas desde su lanzamiento. Por su parte, La guía que no viene con el móvil, el material más destacado de la campaña, ha obtenido **más de 350.000 descargas**.

La campaña contó en su lanzamiento con la colaboración de Movistar, Orange, Vodafone, Yoigo, Fundación Atresmedia, Mediaset España, RTVE, JC Decaux, Metro de Madrid y EMT Madrid, que la difundieron de forma gratuita a través de sus respectivos canales para que todas las familias tengan acceso a unos consejos básicos sobre cómo pueden preparar a sus hijos e hijas para el acceso a estas tecnologías.

La repercusión acumulada de la campaña fue de **más de 300 millones de impactos**, a lo que hay que sumar el apoyo prestado por META a través de sus redes sociales (Instagram y Facebook) para difundir la campaña. Esta inversión realizada por Meta se materializó en créditos publicitarios asignados a UNICEF para gastarlos en la promoción de 'Más que un móvil', llevando a los usuarios a La guía que no viene con el móvil publicada en la página web de la Agencia.

Se establecieron **tres momentos principales** para el uso de esos créditos: la semana del **9 de enero** de 2023, tras la llegada de los reyes magos ante el previsible regalo de un teléfono móvil, los días

colindantes con el **28 de enero**, día internacional de la protección de datos, y los días colindantes con el **7 de febrero**, día de internet segura.

Según los datos facilitados por UNICEF, se consiguó un **alcance total de 9.090.771 y 821.355 interacciones** totales.

Colaboración en la campaña A un click de ayudarles

La Agencia colaboró en la campaña **'A un click de ayudarles'** de la Asociación Europea para la Transición Digital, una iniciativa en la que también colaboran la Fundación Atresmedia y la Fundación Anar).

'A un click de ayudarles' trata de incentivar un papel más activo de padres y madres ante la actividad online de los y las menores de edad, alertando de riesgos como el ciberbullying, la incomunicación o los problemas de autoestima y también de las peculiaridades de algunos modelos de negocio de las plataformas y las redes sociales, basados en el perfilado de los datos de los menores.

El spot de la campaña difundió desde el 24 de mayo de manera gratuita a través de todos los canales televisivos (**Antena 3, laSexta, Nova, Neox, Mega, Atreseries**) y radiofónicos (**Onda Cero, Europa FM, Melodía FM**) del Grupo Atresmedia.

En **televisión** se realizaron 328 pases, alcanzando a **108 millones espectadores** adultos y en **radio 172 pases** de la cuña.

3.8 Premios

Premios concedidos por la AEPD

La Agencia entregó el 26 de enero de 2023 los 'Premios Protección de Datos 2022' en las categorías de Comunicación; Proactividad y buenas prácticas en el cumplimiento del Reglamento y la LOPDGDD; Buenas prácticas educativas; Investigación 'Emilio Aced'; Emprendimiento 'Ángela Ruiz Robles' y Buenas prácticas para una mayor protección de las mujeres frente a la violencia digital.

En la categoría de **Comunicación**, la AEPD concedió el premio al **Área de Ciencia y Tecnología de la Agencia EFE** por sus trabajos sobre los riesgos de publicar imágenes de menores en redes sociales por parte de sus padres; las implicaciones de tecnologías como la inteligencia artificial (IA) o la biometría para la protección de datos, y las precauciones que deben adoptarse antes de escanear códigos QR potencialmente maliciosos, entre otros temas.

El jurado otorgó un accésit en esta misma categoría a **Maldita.es**, por los programas emitidos en su canal 'Maldita Twitchería', donde se analizaron materias como los patrones oscuros y la manipulación online; la identificación y abordaje del acoso online o la importancia del cifrado.

Respecto al **Premio a la Proactividad y Buenas Prácticas en el cumplimiento del Reglamento Europeo de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos Personales y Garantía de los derechos digitales (LOPDGDD)**, en la modalidad de empresas, asociaciones y fundaciones, el jurado concedió el premio a la **Fundación Pro Bono España**, por su programa formativo 'Modo dataprotectiON' para entidades sin ánimo de lucro. El proyecto, eminentemente práctico, contribuye a facilitar la comprensión de la protección de datos y ofrece plantillas, formularios y herramientas prácticas para cumplir con las obligaciones recogidas en la normativa.

En la modalidad de entidades del sector público se otorgó el premio a la **División de Atención al Ciudadano, Transparencia y Publicaciones**

(DIVATP) del Ministerio de Ciencia e Innovación, por su proyecto de vídeos formativos en materia de protección de datos de carácter personal. Éstos abordan, entre otros temas, la normativa, el concepto de dato personal y tratamiento de datos, las figuras del responsable, encargado de tratamiento y delegado de protección de datos, y los derechos de los interesados.

En la categoría de **Buenas prácticas educativas en privacidad y protección de datos personales para un uso seguro de internet por los menores**, el jurado concedió el premio en la modalidad dirigida a centros de enseñanza de Educación Primaria, ESO, Bachillerato y Formación Profesional, a **Humanitas Bilingual School Tres Cantos** (Madrid) por su trabajo 'Mentores digitales. 1º Bachillerato', un proyecto a través del que 70 jóvenes recibieron formación sobre el uso responsable y seguro de Internet para trabajar posteriormente con alumnos y alumnas del mismo centro, desde 5º de Primaria a 3º de Secundaria.

En la modalidad de compromiso de personas, instituciones, organismos, entidades, organizaciones y asociaciones, públicas y privadas, se otorgó el premio a **Orange España** por 'Un uso seguro y responsable de las tecnologías', un proyecto que ofrece cursos formativos online relacionados con la educación en nuevas tecnologías y seguridad, dirigidos a educadores, progenitores, alumnado y AMPAS, incluyendo iniciativas formativas para alumnado con necesidades educativas especiales.

En la categoría de **Investigación en protección de datos personales Emilio Aced** el jurado concedió el premio a **Guillermo Lazcoz Moratinos**, por su trabajo 'Sistemas de AI en la asistencia sanitaria. Cómo garantizar la supervisión humana desde la normativa de protección de datos', que destaca el valor de la Inteligencia Artificial (IA) en el sector de la sanidad teniendo en cuenta la supervisión humana en las decisiones y en el ciclo de vida del sistema de IA.

Asimismo, el jurado otorgó un accésit a **José González Cabañas, Ángel Cuevas, Rubén Cuevas, Juan López Fernández y David García**, por su trabajo 'Único en Facebook: Formulación y evidencia de la publicidad (NANO) dirigida a usuarios con datos NO-PII', donde los autores analizan el nivel de identificación del usuario en la red social con un número de datos que no lo identifican directamente.

Respecto a la categoría de **Emprendimiento en protección de datos personales Ángela Ruiz Robles**, el jurado premió a **Acuratio Europe**, por su 'Plataforma de Inteligencia Artificial para entrenar redes neuronales manteniendo la privacidad de los datos', una ejecución práctica del planteamiento del MIT (Massachusetts Institute of Technology) denominado vertical federated learning, que plantea la desconcentración de información en tratamientos de IA en el entrenamiento de redes neuronales.

Finalmente, en la categoría de **Iniciativas y buenas prácticas para una mayor protección de las mujeres frente a la violencia digital**, el jurado reconoció el trabajo a la **Fundación Cibervoluntarios**, por su trabajo 'Para, Piensa, Conéctate contra la Violencia de Género', un programa de formación en el uso seguro de internet enfocado a la sensibilización y prevención de distintas formas de violencia digital por razón de género en menores entre 10 y 17 años y su entorno docente y familiar cercano, mediante ciberformaciones guiadas en centros educativos de toda España.

Premios recibidos por la AEPD

En 2023 la Agencia Española de Protección de Datos fue galardonada con un total de siete premios, que forman parte de los 29 que la Agencia ha recibido en los últimos años por las acciones realizadas para proteger a las personas en un mundo digital.

1. **Premio Justicia Sostenible de la 4ª edición de los Premios WLW (Women in a Legal World)**, que reconocen la labor tanto de personas como de empresas e instituciones. La AEPD ha recibido este reconocimiento por su labor en la lucha contra la violencia de género, así como por impulsar la constitución de un grupo de trabajo –del que forma parte el Consejo General del Poder Judicial– en esta materia.

2. **Premio de Internet 2023 a la Trayectoria Personal.** El coordinador de la Unidad de Apoyo y Relaciones Institucionales de la AEPD, Jesús Rubí, fue galardonado por la Asociación de Usuarios de Internet (AUI) con el premio de Internet 2023 a la Trayectoria Personal. El Jurado tuvo en cuenta el trabajo desarrollado por Rubí principalmente en la AEPD en el marco de un constante proceso de evolución de las actividades económicas y de las innovaciones tecnológicas con el foco puesto en el derecho fundamental a la protección de datos. Asimismo, destacó que "su actividad profesional se ha centrado en la búsqueda de soluciones realistas que han contribuido a una constante mejora del derecho a la privacidad con transparencia y con garantías para los ciudadanos".

3. **'Premio Seguridad y Protección del dato' de la Revista Sociedad de la Información Digital.** La AEPD fue premiada por la Revista Sociedad de la Información Digital con el galardón de la candidatura 'Seguridad y Protección del dato' de los Premios Socinfo Digital 'AGE TIC', organizados por la revista con el objetivo de divulgar proyectos de desarrollo de las TIC en las AAPP aplicadas en los servicios al ciudadano y reconocer la labor de los profesionales del sector. El Jurado destacó que el proyecto presentado por la Agencia otorga una visión extensiva del tratamiento de datos y resaltó su valor para el crecimiento y preparación en temas de seguridad de datos e información, así como su beneficio para la sociedad.

4. **Premio Responsabilidad Social de la 3ª edición de los Premios PantallasAmigas.** La Agencia Española de Protección de Datos fue galardonada en la categoría de Responsabilidad Social de la 3ª edición de los Premios PantallasAmigas, por las acciones realizadas en materia de protección y promoción del bienestar de la infancia en el ámbito digital.

5. **Premio 'Resolución de conflictos & Aplicación de la Ley' de los Global Privacy and Data Protection Awards 2023.** El **Canal prioritario** de la Agencia Española de Protección de Datos (AEPD) fue galardonado en la categoría de 'Resolución de conflictos & Aplicación de la Ley' de la 6ª edición de los Global Privacy and Data Protection Awards 2023, concedidos en el marco de la 45ª Asamblea Global de Privacidad, que reúne a más de 140 autoridades de protección de datos y privacidad a nivel mundial. El galardón reconoce el valor del Canal prioritario de la AEPD como un instrumento eficaz en situaciones en las que la integridad física y psicológica de las personas afectadas se pone en grave riesgo por la difusión de contenidos publicados online y que constituye violencia digital, especialmente contra mujeres, niños y personas vulnerables.

6. **Premio en la categoría de 'Innovación' de los VI Premios Confilegal:** La directora de la Agencia Española de Protección de Datos (AEPD), Mar España, fue galardonada en los VI Premios Confilegalen la categoría de 'Innovación'. El jurado valoró "el trabajo realizado en el campo de la protección de datos y la privacidad, abogando por soluciones legales y tecnológicas para minimizar el impacto negativo del mal uso de Internet y las redes sociales, especialmente en el contexto de contenidos sensibles y la protección de menores".

7. **Premio QIA a la 'Innovación en el sector público'.** La Agencia Española de Protección de Datos fue galardonada en los Quality Innovation Award, QIA 2023 -que otorga la Asociación Nacional de Centros Promotores de la Excelencia (CEX)-, en la categoría de 'Innovación en el sector público', por su proyecto 'Iniciativas prácticas para proteger a los menores en internet con entornos saludables, positivos y seguros'. El comité organizador de los QIA consideró el proyecto de la Agencia como una quality innovation, una innovación que cumple con cinco características: novedad, utilidad, aprendizaje, orientación al cliente y efectividad.

El histórico completo de premios recibidos por la AEPD puede consultarse en este enlace.

3.9 Acceso a la información pública y transparencia

La transparencia es uno de los principales valores de esta Agencia, como requisito necesario para garantizar su independencia en el desarrollo de las funciones que tiene encomendadas.

En cuanto a la transparencia activa, la AEPD cumple con sus obligaciones a través de su propia web y aplica los criterios del Consejo de Transparencia y Buen Gobierno. En 2023 se ha constatado un aumento de un 36% en el número de accesos al apartado Transparencia de nuestra página web. Respecto al acceso a la información pública, se ha producido una disminución en el número de solicitudes, respecto a 2022. No obstante, el porcentaje de concesiones totales aumenta ligeramente.

La mayor parte de las peticiones se refieren a expedientes y resoluciones sancionadoras, pero también se ha solicitado, y se ha facilitado, el acceso a informes jurídicos de la AEPD, información sobre el número y tipo de Delegados de Protección de Datos comunicados a esta Agencia, el presupuesto invertido en publicidad institucional, o sobre el personal que presta sus servicios en la Agencia.

Al igual que en 2022, el 100% de las resoluciones de acceso adoptadas por la AEPD se han emitido en el plazo legalmente establecido para resolver. A lo largo de 2023, 10 resoluciones de la AEPD fueron recurridas ante el Consejo de Transparencia y Buen Gobierno (CTBG), lo que supone menos del 9% de las resoluciones, y todas ellas han sido desestimadas por el CTBG, confirmando así las resoluciones de la Agencia.

De especial interés resulta la resolución del CTBG en la que confirma que, en un procedimiento sancionador en curso, con la comunicación de la fecha de apertura del procedimiento sancionador, la duración máxima del mismo, y la información de que en el momento en que se dicte resolución que ponga fin al procedimiento se remitirá al demandante una nueva comunicación; se considera atendido el derecho a conocer el estado del procedimiento. Sin que proceda reconocer su derecho de acceso al resto de la información generada en el marco de un procedimiento sancionador en curso en el que el solicitante (denunciante) no tiene la condición de interesado.

Asimismo, también ha respaldado que no cabe reclamación ante el CTBG frente a una Resolución de acceso a la información pública cuando dicha información haya sido proporcionada por el mismo organismo en un procedimiento de derecho de acceso posterior al reclamado.

Destacable resulta también, el pronunciamiento del CTBG respecto a la inadmisibilidad de una reclamación cuando se haya interpuesto recurso de reposición contra la misma, dado que el artículo 23.1 de la LTAIBG configura la reclamación ante el Consejo como sustitutiva de los recursos administrativos, de lo que se desprende la imposibilidad de simultanear ambas vías.

La Unidad de Información y Transparencia (UIT) de la AEPD participa en el grupo de trabajo del Comité Europeo de Protección de Datos preparando el estudio europeo comparado sobre el acceso a documentos de expedientes sancionadores

y actuaciones de investigación transfronteriza. Igualmente, la UIT de la AEPD participa en el grupo de trabajo que aglutina a todas las UITs de la Administración General del Estado (AGE) para coordinación de criterios, que es convocado y dirigido por la DG de Gobernanza. En aplicación de su compromiso de actuación transparente, la AEPD **publica en su web** las resoluciones firmes denegatorias, o parcialmente denegatorias, para el conocimiento general de los razonamientos y motivación de su actuación.

4. Ayuda efectiva a las entidades

4.1 Sujetos obligados y delegados de protección de datos (DPD): funcionamiento del Canal del DPD y valoración de las consultas de los DPD

Los sujetos obligados, responsables y encargados del tratamiento, deben cumplir con el principio de responsabilidad proactiva que se complementa con la obligación, en unos casos o la posibilidad, en otros, de designar un DPD, a través del cual se pueden formular consultas a la AEPD.

En virtud del artículo 39.1.e) del RGPD y conforme a los requisitos que se exponen en la norma 4 de la Instrucción 1/2021, la AEPD puede ser consultada por los DPD, bajo ciertos requisitos coherentes con el principio de responsabilidad proactiva, y por las organizaciones y asociaciones representativas de responsables y encargados del tratamiento que presten servicio de asesoramiento en materia de protección de datos a sus asociados, especialmente cuando se trate de pequeñas y micro empresas, en las mismas condiciones que se establecen para los DPD.

Las **consultas recibidas** ascienden a un total de **850**, lo que supone un **incremento de 22,3%** respecto del año anterior.

En cuanto a su contenido, se pueden resaltar como más relevantes, las siguientes:

- **En el ámbito de la seguridad pública:** Las cuestiones relacionadas con la videovigilancia y con la interpretación de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, han generado importantes dudas respecto de la normativa aplicable a la instalación de videocámaras fijas en la vía pública por las Fuerzas y Cuerpos de Seguridad del Estado. En estas cuestiones la AEPD junto al resto de autoridades autonómicas ha interpretado que la exigencia de autorización para la instalación de videocámaras fijas establecida por la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos y su normativa de desarrollo continúa vigente, no habiendo sido derogada por la Ley Orgánica 7/2021.

Siguen siendo numerosas las consultas planteadas por las Policías Locales en las que se solicita la autorización de la AEPD para la instalación de cámaras en las vías públicas de sus Municipios. Se señala en cualquier caso que la AEPD no tiene entre sus competencias la de autorizar la instalación de este tipo de dispositivos, más allá de señalar las consideraciones que deben tener en

cuenta a la hora de su instalación y que pueden consultarse en la web de la Agencia en al apartado dedicado a la **videovigilancia**.

- **En el ámbito laboral**, la implantación de sistemas de reconocimiento facial y huella como medida para el control horario de los trabajadores y el control de acceso sigue siendo un tema recurrente. Sobre estas cuestiones ha tenido especial incidencia la publicación de las "Directrices 05/2022 del CEPD sobre el uso de técnicas de reconocimiento facial en el ámbito de aplicación de la ley", poniendo de manifiesto que con la evolución tecnológica resulta necesario establecer mayores controles tanto para la autentificación como para la identificación en base a elementos biométricos de la persona, y plantearse los límites al tratamiento de datos biométricos y las medidas que han de establecerse para que un tratamiento de datos personales que decida utilizar sistemas biométricos garantice el cumplimiento RGPD. Sobre estas cuestiones la AEPD ha publicado una **Guía sobre tratamientos de control de presencia mediante sistemas biométricos** estableciendo los criterios para la utilización de la biometría en el registro de la jornada laboral o el control de acceso con fines laborales y no laborales.

- **En relación con la publicidad no deseada**: Con la entrada en vigor de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones, también se han planteado numerosas consultas relativas a la interpretación que debía darse a su artículo 66.1.b), en relación con la legitimación para el tratamiento de datos en llamadas no deseadas con fines de comunicación comercial sobre todo en lo referido al posible interés legítimo admitido por dicho precepto. Sobre esta cuestión la Agencia ha aprobado **la Circular 1/2023, de 26 de junio, sobre la aplicación del artículo 66.1.b) de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones**.

- **En cuanto a lucha contra la corrupción**: La publicación de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción también está siendo objeto de consultas porque de su aplicación se derivan tratamientos de datos personales. Principalmente, se trata de cuestiones relacionadas con la puesta en marcha de los sistemas de denuncias internas en el entorno de las Administraciones Publicas y relacionados con la posición jurídica de cada uno intervinientes (asignaciones de roles de responsable del tratamiento, encargados o corresponsables). Sobre los principios generales del Sistema interno de información y defensa del informante, y el procedimiento de gestión de informaciones previsto en la Ley 2/2023, la AEPD ha aprobado y publicado los **Principios del Sistema interno de Información y defensa del informante** y el **Procedimiento para la gestión de informaciones de la Ley 2/2023**.

4.2. Inscripción de Delegados de Protección de Datos

La importancia de la función de delegado de protección de datos (DPD) como elemento fundamental para el cumplimiento del RGPD resulta evidente tal y como se desprende de las funciones, posición y características que le atribuye tanto el RGPD como la LOPDGDD.

La AEPD ha continuado impulsando la puesta a disposición de las personas que desempeñan esta función de las herramientas, recursos y canales de comunicación con el fin de que puedan desempeñar su función con las garantías de solvencia e independencia. Al mismo tiempo, la AEPD ha continuado también con la labor de concienciación a los responsables obligados a la designación de DPD, así como los que consideren su designación de forma voluntaria, a dotar a esta figura de recursos suficientes para el desarrollo de las tareas que el RGPD les atribuye.

También ha participado en la acción europea coordinada para analizar la designación y situación de los delegados de protección de datos en entidades públicas y privadas, dentro del marco de actuaciones coordinadas del CEPD. Dicha acción ha dado como resultado un informe que ofrece una visión tanto del sector público como privado con el fin de contribuir a elevar el nivel de cumplimiento y la protección de los datos personales de los ciudadanos en el conjunto de la UE.

En ejecución de esta acción coordinada, la AEPD ha analizado la práctica de más de 10.000 entidades del sector público y privado.

Estas entidades respondieron al cuestionario remitido y que incluía cuestiones sobre la designación, conocimiento y experiencia de los DPD, sus tareas y recursos o su papel y posición en sus respectivas organizaciones.

Las recomendaciones recogidas han señalado la necesidad de continuar promoviendo la concienciación entre las organizaciones para que adopten la necesaria diligencia en la designación del DPD; de que los responsables verifiquen los medios puestos a disposición de los DPD para que puedan desempeñar con eficacia las funciones que tienen encomendadas; de proporcionar la capacitación y la formación de los DPD a través de diversos mecanismos, así como fomentar el uso de la certificación; de dotar al DPD de la debida independencia en el ejercicio de sus funciones con el fin de evitar los conflictos de interés , así como promover la visibilidad de esta función dentro de la organización; la importancia de promover los mecanismos internos para que el DPD reporte al más alto nivel de la organización; a continuar con la labor desarrollada hasta ahora por las autoridades de control con el fin de proporcionar directrices y herramientas que contribuyan al eficaz desempeño de dichas funciones.

4.3. Encuentro con los DPD de las Administraciones Públicas

Como continuación de los encuentros mantenidos con los DPD de diferentes Administraciones Públicas y sectores de actividad en el año 2022, y en el marco de la función consultiva prevista en la Instrucción 1/2021, el 28 de marzo de 2023, se celebró el encuentro con los DPD de las entidades locales pertenecientes a capitales de provincia y ciudades de 100.000 habitantes y de las Diputaciones, Cabildos y Consejos Insulares del ámbito competencial de la AEPD.

Este 6º Encuentro, celebrado después de la pandemia, con el objetivo de mantener un espacio de diálogo continuo con los DPD, como elementos clave del ecosistema de protección de datos del sector público, así como conocer a través de los propios DPD cuál es la situación actual con respecto al ejercicio de sus funciones e intercambiar experiencias y buenas prácticas desarrolladas en el sector. Además, es de suma importancia apoyar la labor de los DPD y reforzar su independencia frente a los responsables del tratamiento.

En dicho Encuentro se abordaron los resultados de la encuesta sobre el estado de situación de los DPD en las Entidades Locales, entre cuyos resultados destacan su actuación tanto como DPD de responsable como de encargado, en el caso de los DPD de las Diputaciones, su designación sobre la base de sus conocimientos y experiencia, y desempeñan su tarea a tiempo parcial el 58%, compaginándola con otras labores de distinta naturaleza, la ausencia de previsión de informe anual (38%) y el interés en recibir materiales de la autoridad de control para el mejor desempeños de sus funciones.

Asimismo, tuvo lugar la presentación del área temática dedicada al Sector público habilitada en la web de la AEPD, las brechas de datos personales, los procedimientos sancionadores más relevantes en el ámbito de las entidades locales y del **Canal Prioritario**.

Finalmente, se trataron las consultas planteadas por los asistentes con carácter previo a la celebración del Encuentro, así como las que surgieron a lo largo del mismo. Entre estas cuestiones se abordaron consideraciones generales sobre el acceso a los datos del Padrón, así como dudas respecto al tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales; el uso de las denominadas cámaras onboard por parte de la policía local, así como el uso de los teléfonos móviles no corporativos por parte también de la policía local; uso del Padrón Municipal de habitantes por parte del Ayuntamiento para llevar a cabo una consulta sobre proyectos de inversiones municipales; difusión de imágenes de asociaciones de personas mayores o grupo de menores que visitan el Ayuntamiento; acceso a los datos padronales de su hijo menor de edad del que ostenta la patria potestad en caso de progenitores separados.

Acción coordinada del Comité Europeo del Protección de Datos sobre la designación y situación de los DPD

Durante 2023, la Agencia Española de Protección de Datos ha participado en la segunda acción coordinada del Comité Europeo de Protección de Datos, que tuvo por objeto analizar la designación y situación de los DPD en las organizaciones, si ocupan la posición que exige el RGPD y si disponen de los recursos necesarios para llevar a cabo sus tareas.

En el desarrollo de esta acción la AEPD analizó las prácticas de las más de 10.000 entidades del sector público y privado que respondieron al cuestionario remitido y que incluía, entre otras, cuestiones relacionadas con la designación, conocimiento y experiencia de los DPD, sus tareas y recursos o su papel y posición en sus respectivas organizaciones.

En el marco del sector privado, el cuestionario se dirigió a distintos sectores de actividad: educación, entidades bancarias y financieras, sanidad, sector energético, seguridad, servicios de telecomunicaciones, solvencia patrimonial y crédito, y actividades relacionadas con los juegos de azar y apuestas.
Acción en la que ha colaborado el Consejo de Transparencia y Protección de Datos de Andalucía en su ámbito de actuación.

El informe final del CEPD (adoptado a principios de 2024) recoge una serie de **recomendaciones y puntos de atención** dirigidos a las organizaciones, a los DPD y a las autoridades de control, tales como:

- Continuar promoviendo la concienciación entre las organizaciones para que la designación del DPD se ajuste a los que prevé el RGPD.
- La necesidad de que los responsables del tratamiento verifiquen que los medios puestos a disposición de los DPD les permiten desempeñar con eficacia las funciones que tienen encomendadas.
- Proporcionar capacitación y formación de los DPD a través de diversos mecanismos, y el fomento del uso de la certificación.
- La necesidad de garantizar la independencia del DPD para el ejercicio de sus funciones con el fin de evitar los conflictos de interés, así como promover la necesaria visibilidad del delegado dentro de la organización.
- La importancia de promover los mecanismos y procesos internos para que el DPD reporte al más alto nivel de la organización.
- Proporcionar las autoridades de control, como hasta ahora, directrices y herramientas y recursos que contribuyan al eficaz desempeño de las funciones de DPD.

4.4. Certificación de DPD conforme al Esquema AEPD-DPD

El artículo 37 del RGPD establece la figura del delegado de protección de datos (DPD) como aquella que, entre otras actividades, ha de asesorar a los responsables del tratamiento en el cumplimiento de la legislación de protección de datos, además de incluir los requisitos que ha de cumplir dicho DPD, pues establece que "será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos".

La AEPD, con la finalidad de facilitar a los responsables del tratamiento la designación de DPD cualificados, con ahorro de tiempo y de recursos, elaboró en julio de 2007 un Esquema de Certificación en línea con lo que dispone el artículo 35 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

En 2023, las principales magnitudes del Esquema tienen que ver con el número de DPD certificados, que han sido 169, el 42% de los 404 candidatos a obtenerlo en un total de 62 pruebas.

Con ellos, el número total de DPD que han obtenido la certificación con arreglo al Esquema de la AEPD a 31 de diciembre asciende a 1.100, dato que contrasta con el número de DPD personas físicas que han sido comunicados a la AEPD (10.459), si bien se muestra que el porcentaje de DPD certificados sobre el total de DPD continúa aumentando, llegando a 10,52% (9,67% el año anterior).

Tras el fuerte impacto de la pandemia, que produjo una tendencia a la baja en el número de DPD certificados esos años, 2023 ha supuesto una inversión de la tendencia y se observa que es la primera vez que el número de DPD certificados durante el año supera al del anterior.

Otro aspecto relevante ha sido la retirada del Esquema de una de las entidades de certificación, por lo que actualmente son 7 el número de entidades certificadoras acreditadas por ENAC. En cuanto a las entidades de formación, la AEPD ha reconocido como tal a la Universidad del País Vasco por su Máster en "Protección de Datos Personales, Ciberseguridad y derecho de las TIC's" que se suma a las dos Universidades previamente reconocidas.

4.5. Códigos de conducta

En el año 2023, conforme a lo dispuesto en el RGPD, se ha seguido impulsando la elaboración de los códigos de conducta con la finalidad de contribuir a su correcta aplicación, teniendo en cuenta las características de los tratamientos de datos que se realicen según los sectores de actividad. Asimismo, y en cumplimiento de lo establecido en la Disposición transitoria segunda LOPDPGDD se continua con el proceso de adaptación de los códigos tipo.

Para ello, se han mantenido numerosas reuniones y contactos con los promotores de códigos de conducta cuyos proyectos se encuentran en tramitación con la finalidad de ajustar su contenido a las exigencias del RGPD, las Directrices 1/2019 del CEPD y los criterios de acreditación de los organismos de supervisión adoptados por la Agencia, lo que implica el estudio y valoración de los proyectos presentados y de sus sucesivas versiones y, en su caso, efectuar las recomendaciones y sugerencias de mejora. En algunos supuestos, y como en ejercicios anteriores, se ha solicitado la colaboración de otras unidades de la AEPD en aquellos apartados que tratan materias que conforman su trabajo diario.

Es importante destacar el impulso de la Agencia para la elaboración de códigos de conducta que regulen procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento, sin perjuicio de los derechos de los interesados en virtud de los artículos 77 y 79 (art. 40.2.k RGPD).

Códigos nacionales

El total de códigos aprobados por la AEPD hasta el momento son los que se relacionan a continuación:

- **"Código de conducta de tratamiento de datos en la actividad publicitaria"** promovido por AUTOCONTROL y que ha sido modificado en el año 2023 debido fundamentalmente a la necesidad de adecuarlo a los cambios normativos de la Ley 11/2022, General de Telecomunicaciones y de la LOPDPGDD, así como a lo dispuesto en la Circular de la AEPD 1/2023.

- **"Código de conducta regulador del tratamiento de datos personales en el ámbito de los ensayos clínicos y otras investigaciones clínicas y de la farmacovigilancia"** promovido por FARMAINDUSTRIA.

- **"Código de conducta regulador del tratamiento de datos personales en los sistemas comunes del sector asegurador"** promovido por UNESPA.

Respecto de estos tres códigos, el punto 6.1 de los Criterios de acreditación para los organismos de supervisión de códigos de conducta establece que *"El organismo de supervisión informará anualmente a la AEPD de las actividades realizadas, que incluya tanto las medidas y diligencias realizadas para verificar el cumplimiento del código, y de sus resultados, como las reclamaciones recibidas y sus resultados".*

Conforme a dicho criterio, se han recibido los informes de actividades correspondientes a los códigos aprobados, habiéndose procedido a su análisis para verificación del cumplimiento de lo establecido en los mismos.

Actualmente se encuentran en distintas fases de tramitación 16 proyectos de códigos de conducta, 9 referidos a adaptación de códigos tipo y 7 a nuevos proyectos.

En el momento de cierre de esta Memoria se encuentran muy avanzada la tramitación del "Código de conducta para la resolución de controversias de protección de datos en el sector de las comunicaciones electrónicas" promovido por las siguientes teleoperadoras: Orange Espagne, S.A.U., Orange España Virtual, S.L., Telefónica de España, S.A.U., Telefónica Móviles España, S.A.U., Vodafone España, S.A.U., Vodafone ONO, S.A.U., Xfera Móviles, S.A.U. y Pepemobile, S.L.

Códigos de Conducta Transnacionales

Además, la AEPD ha participado en la tramitación de 5 proyectos de códigos de conducta liderados por autoridades de protección de datos de otros Estados miembro en el marco del procedimiento coordinado.

En el ejercicio 2023, la AEPD actúa como autoridad correvisora en el proyecto de CÓDIGO DE CONDUCTA DE LA UE SOBRE INVESTIGACIÓN CIENTÍFICA, promovido por la Federación Europea de Industrias Farmacéuticas (EFPIA, por sus siglas en inglés).

Asimismo, la AEPD ha revisado la última versión del código de conducta EUCROF, liderado por la Autoridad francesa, y ha efectuados observaciones a la consulta formulada por la Autoridad de Austria en relación con el código para Marketing transfronterizo por correo postal.

4.6. Promoción del derecho fundamental a la protección de datos

La AEPD, dentro de su función de promoción, realiza actuaciones de sensibilización dirigidas, por una parte, a responsables y encargados del tratamiento acerca de las obligaciones que les incumben en virtud del RGPD y la LOPDPGDD y, por otra, al público, que incluye la comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento de sus datos, que se desarrollan a través de cursos, jornadas y participación en eventos que tienen por objeto las finalidades descritas.

La AEPD ofrece dos modalidades de cursos:

- Curso de 20 horas configurado en **8 videoconferencias en formato online**.

- **Curso de 6 módulos en formato Moodle**. Se ha incorporado la realización de una videoconferencia en directo en cada uno de los módulos, para una mayor interacción entre alumnos y profesor.

Además, se imparten cursos más específicos, adaptados a las características de las actividades de tratamiento de datos de los organismos y entidades en concreto, sujetos a la disponibilidad de la AEPD.

La formación impartida durante 2023 **se ha dirigido a:**

- **La Administración General del Estado.**

- **Ministerios**: Sanidad; Derechos Sociales y Agenda 2030; Transportes, Movilidad y Agenda Urbana; Interior; Educación y Formación Profesional; Trabajo y Economía Social; Inclusión, Seguridad Social y Migraciones; Política Territorial; Justicia; Defensa; Ministerio para la Transición Ecológica y el Reto Demográfico.

- **Otros organismos públicos**: Tribunal de Cuentas, Universidad de Las Palmas de Gran Canaria y Principado de Asturias.

- **Cursos dirigidos a los empleados públicos**. Los Organiza el Instituto Nacional de Administración Pública (INAP), sobre la "Aplicación del Reglamento General de Protección de Datos en las Administraciones Públicas", y que se imparten por representantes de la AEPD, que han contado con 600 alumnos.

Hay que destacar el "Programa especializado para delegados de protección de datos de las Administraciones Públicas.", curso específico para formar a los futuros DPD y cuya primera edición tuvo una nueva metodología, estructura, etc.

El **"Programa especializado para delegados de protección de datos en las Administraciones Públicas"** se impartió a **80 alumnos** durante el primer semestre del año.

Un aspecto importante de las actividades de promoción son las dirigidas a la difusión de las medidas adoptadas por la AEPD para la protección de colectivos vulnerables frente a situaciones de violencia digital, en particular del Canal Prioritario. En 2023 **se ha participado en diversas Jornadas organizadas por**:

- Fundación Diagrama
- Unidad de Violencia sobre la Mujer, Subdelegación del Gobierno en Segovia
- Ministerio de Justicia

Además, se ha celebrado una Jornada de Calidad normativa en protección de datos, donde se abordaron temas como la función asesora de la Agencia en la elaboración de normas y la Memoria de Análisis de Impacto Normativo (MAIN); el análisis de riesgos y evaluaciones de impacto en protección de datos en la producción normativa, y la incidencia del Reglamento General de Protección de Datos en el contenido de las normas garantías a incorporar en la norma.

4.7. Transferencias Internacionales

Durante 2023, una vez que el Comité Europeo de Protección de Datos emitió su opinión favorable, la AEPD ha aprobado las normas corporativas vinculantes (BCR, por siglas en inglés) de responsable del grupo multinacional Prosegur.

En este período el grupo Align Technology ha solicitado que la AEPD actuase como autoridad líder con respecto a sus BCR (responsable y encargado). Aunque estas BCR ya fueron adoptadas en su momento por la autoridad de los Países Bajos, se ha solicitado el cambio de autoridad líder debido a la designación como entidad principal del grupo a una entidad establecida en España.

El total de BCR adoptadas por la AEPD a finales de este período es de 10 normas corporativas vinculantes.

Actualmente se encuentran en distintas fases de tramitación 12 proyectos de BCR en el marco del procedimiento coordinado y consistencia previsto en el RGPD. En el momento de cierre de esta Memoria se encuentran en la fase final de tramitación las BCR de Mapfre y Telefónica.

Además, la AEPD ha participado como autoridad correvisora en la tramitación de 4 proyectos de BCR lideradas por autoridades de protección de datos de otros Estados miembro en el marco también del procedimiento coordinado.

5. La potestad de supervisión

5.1 Resultados

La mayor presencia y alcance de los tratamientos de datos personales en la sociedad y la consiguiente preocupación de los ciudadanos por el tratamiento de sus datos vuelve a encontrar reflejo en el registro de reclamaciones ante la Agencia, que alcanza un año más un volumen sin precedentes.

En 2023 se registraron 21.590 reclamaciones, un 43% más que el año inmediatamente anterior. En los tres años de esta década, se han duplicado las reclamaciones que tiene que tramitar la Subdirección General de Inspección de Datos (SGID).

Durante el año 2023 se han resuelto más reclamaciones que ningún año anterior, siendo un 37% más que durante el año 2022. A pesar de ello, el gran aumento de entradas ha tenido su repercusión en la tasa de resolución de reclamaciones -que compara el número de reclamaciones recibidas con el número de reclamaciones resueltas en el mismo año- que ha descendido a un 94% frente al 99% del año anterior.

En cuanto a las actividades que realiza la SGID se puede destacar que el RGPD establece entre las funciones de la Agencia la de tratar las reclamaciones presentadas e investigarlas en la medida oportuna, informando al reclamante sobre el curso y el resultado. Esto se realiza en la SGID a través de las actuaciones y procedimientos que se regulan en el Título VIII de la LOPDGDD y, supletoriamente, en la regulación del procedimiento administrativo común que establece la LPACAP. La tramitación de las reclamaciones se inicia con una evaluación de la admisibilidad que incluye una primera fase de análisis previo de admisibilidad, para posteriormente desarrollar la fase de traslado de la reclamación al responsable o encargado y decidir sobre su admisión a trámite. Una vez admitida a trámite, si se estima necesario

para determinar las circunstancias de la infracción y completar la identificación del responsable, se realizan las actuaciones previas de investigación, para finalmente, plantearse la conveniencia de iniciar el procedimiento sancionador o el procedimiento de apercibimiento. En el caso de que la reclamación esté relacionada exclusivamente con los derechos establecidos en los artículos del 15 al 22 del RGPD, con la admisión a trámite de la reclamación se puede iniciar un procedimiento específico de ejercicio de derechos.

Cabe destacar que en los últimos dos años se han revisado los criterios que aconsejan la apertura de actuaciones de investigación previa al inicio de procedimiento que ha llevado a una reducción del número de investigaciones desde entonces, permitiendo así a los inspectores dedicar más tiempo a las investigaciones que tienen un mayor impacto. Esta tendencia prosigue en 2023, mejorando la eficacia del trabajo que realiza la SGID dado que de las investigaciones llevadas a cabo: el 55% culmina en la apertura de procedimiento, frente al 39% del año 2022, y el 28% de 2021.

A través de las actuaciones y procedimientos indicados se tramitan también otro tipo de entradas, distintas de las propias reclamaciones presentadas ante la Agencia, y que no existían con anterioridad a la aplicación del RGPD: casos procedentes de otras autoridades de control del Espacio Económico Europeo (EEE) y notificaciones de brechas de datos personales en las que procede la investigación de la SGID. También nace en años recientes el canal prioritario para la retirada de contenidos sensibles, como pueden ser fotografías, vídeos o audios de contenido sexual o violento que estén publicados en Internet, que puedan causar un daño irreparable en los derechos y libertades de los afectados. Este canal también incluye un acceso específico para los menores de 14 a 18 años. Todo ello, junto a las actuaciones realizadas por propia iniciativa, suman en 2023 más de 1.250 entradas adicionales a las reclamaciones que también originan las actuaciones descritas.

Además de las competencias que tiene la Agencia derivadas del RGPD y de la LOPDGDD, la Ley 11/2022 General de Telecomunicaciones (en adelante, LGTel) y la Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico (en adelante, LSSI), como leyes especiales, también otorgan competencias a la SGID para aplicar los procedimientos dispuestos en el Título VIII. Al margen de estas dos normas, se han aprobado en esta década diversas leyes que también facultan a la Agencia y, en particular, a la SGID, para intervenir controlando y supervisando la aplicación de determinadas disposiciones. Entre ellas, se encuentran la Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del Registro de Nombres de Pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, la Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia, que tienen un impacto directo en la actividades de la SGID, la Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual, o la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual, por citar las más significativas. Estas nuevas asignaciones redundan en un incremento de la entrada, con reclamaciones que vienen de ámbitos normativos diferentes con peculiaridades propias que conviene distinguir a la hora de realizar los procedimientos.

En definitiva, todo ello contribuye a una **tendencia de aumento de las reclamaciones y del trabajo de la Agencia**, que previsiblemente se continuará produciendo en los próximos años por la persistencia de las causas que lo producen.

También hay que mencionar el aumento del 6% de los recursos de reposición interpuestos contra resoluciones de los procedimientos, después de haber aumentado también en los años anteriores de forma importante (un 13% y un 18% en 2022 y 2021 respectivamente), lo que supone un incremento de más del 40% en tres años.

Analizando ahora los actos que ponen fin a las actuaciones de la SGID, casi el 70% de las reclamaciones recibidas finalizan tras el análisis previo de admisibilidad y, por lo tanto, no prosiguen a fases posteriores.

Hay que destacar la excepcionalidad del procedimiento sancionador, por lo que, cuando es posible, se opta por mecanismos alternativos amparados por la normativa, tal y como ocurre con la remisión de la reclamación al DPD o al responsable o encargado, según dispone el artículo 65.4 de la LOPDGDD. Tomando como referencia las reclamaciones que superan el análisis previo de reclamación, es decir, el 30% de las reclamaciones, se observa que solo el 8% de las resoluciones se producen en el procedimiento sancionador, frente al 86% que se producen tras el traslado de la reclamación. Así, la principal vía de resolución de reclamaciones pasa por su remisión al responsable o encargado del tratamiento, que analiza la reclamación y proporciona una respuesta a la Agencia que, en un número significativo de casos, permite concluir que no existe infracción o que esta ha sido corregida, y que no se estima necesario la apertura de nuevas actuaciones, con independencia de las potestades de investigación y sancionadoras que siempre puede iniciar la AEPD.

Estos mecanismos también tienen reflejo sobre los tiempos en que los ciudadanos obtienen respuesta a sus reclamaciones, en descenso desde que se comenzaron a aplicar. No obstante, en este último año, tras varios años de sucesivas reducciones, el tiempo medio de resolución de las reclamaciones que superan el análisis previo de admisibilidad se ha visto incrementado en un 3%, por el gran aumento de reclamaciones recibidas y por la consolidación de los procesos desde que se aplica el RGPD y la LOPDGDD. Sin embargo, los tiempos siguen siendo bajos y los ciudadanos han visto atendida su reclamación plazos menores a los que hubieran tenido que esperar si se hubiera tenido que iniciar uno de los procedimientos establecidos en la LOPDGDD.

Del análisis de los datos por grupos de clasificación, se observa un año más cómo las reclamaciones más frecuentes se repiten con las del año anterior (aunque en un orden distinto): las relacionadas con publicidad, servicios de internet y videovigilancia, sumando entre las tres un 46% del total de reclamaciones. Destaca principalmente el aumento de reclamaciones relacionadas con publicidad, con un incremento del 114% con respecto al anterior. En relación con ello, a final de 2022 se trabajó en la modificación del código de conducta publicitario de Autocontrol, al que se han podido adherir al comienzo ya de 2023 los principales operadores de telecomunicación, para la intermediación y rápida resolución de las reclamaciones sobre publicidad no deseada.

Siguiendo con los grupos de clasificación, se ha producido un importante aumento de las reclamaciones recibidas sobre comercio, transporte y hostelería (+66%) y, dentro de este ámbito, el aumento de infracciones reclamadas relacionadas con el uso de datos personales por parte de empresas de reparto y paquetería, algo que ya sucedió durante el año anterior: en su mayor parte se trata de reclamaciones asociadas a la entrega de paquetería a terceros (vecinos o tiendas cercanas) sin haberse informado de ello, y revelando así datos personales de los destinatarios que se encuentran anotados en la etiqueta del paquete. Por último, cabe reseñar un aumento también relevante (+73%) en reclamaciones relacionadas con entidades financieras o acreedoras, principalmente relacionadas con el ejercicio de derechos.

En relación con los procedimientos sancionadores y las multas, el ámbito más frecuente de los primeros es la videovigilancia (164 procedimientos), aunque, el mayor volumen de multas corresponde a los casos relacionados con quiebras de datos personales. Esto se explica por la, generalmente, menor entidad de los casos de videovigilancia, tanto por su gravedad como por el tipo de responsable (personas físicas) y su relación con la eficacia de las multas (en términos de proporcionalidad y capacidad de disuasión), frente a la gran repercusión de las infracciones con la presencia de grandes compañías en el ámbito de las brechas de datos personales que afectan a gran número de clientes o ciudadanos.

La mayor multa impuesta en el año se corresponde con un procedimiento del sector de las entidades financieras, en el que se impone a Caixabank S.A., por infracción de los artículos 5.1.f, 25 y 32 del RGPD, una multa de 5 millones de euros,

además de ordenar las medidas necesarias para corregir la infracción e impedir su reproducción en el futuro.
Observando los grupos de clasificación en términos del volumen de multas impuestos, también destaca un descenso (-91%) en el importe de las multas del grupo de servicios de internet, lo que se explica por el procedimiento del año previo contra Google LLC que supuso por sí solo una multa de 10 millones de euros.

En el ámbito europeo, dentro de los mecanismos de cooperación entre las autoridades de control de los Estados del Espacio Económico Europeo (EEE) para la gestión de los casos transfronterizos, se puede destacar el incremento tanto de casos en los que España actúa como autoridad principal, por estar el responsable establecido en terreno nacional, como los casos de cooperación en los que España actúa como autoridad interesada. En total, los casos han aumentado un 51%.

En cuanto a las entradas procedentes de otros estados del EEE, se estabilizan con un ligero incremento del 1%. Aumentan la entrada de nuevos casos transfronterizos y las consultas procedentes de otras autoridades, pero se reducen los proyectos de decisión de casos en los que la AEPD participa. Dado que en este último supuesto se trata de un proceso complejo que puede durar varios años, el descenso de decisiones en el año depende del inicio de casos en años previos.
En el ámbito europeo, la SGID ha participado en varios grupos de trabajo para cohesionar criterios y cooperar en diversas materias, como se detalla en el apartado de La Agencia en cifras de esta Memoria. Es destacable la participación que la SGID ha tenido en la elaboración del borrador de ajuste fino del RGPD destinado a los casos transfronterizos.

Asimismo, hay que citar también las obligaciones que tiene la SGID en relación con la supervisión de la protección de datos personales de las diversas agencias de la Unión Europea y de sus grandes sistemas de información, que sirven a las finalidades de cooperación entre los Estados Miembro, en particular en el ámbito judicial, policial, y de control de aduanas y fronteras. Las normas de protección de datos propias de cada uno de ellos se encuentran primariamente en sus respectivas normas de establecimiento, que normalmente tienen la forma de Reglamento UE, sin perjuicio de que sean también de aplicación, dependiendo del ámbito material en que opera la agencia o sistema, el Reglamento General de Protección de Datos (RGPD) y la Directiva de Ámbito Penal (DAP). Las auditorías a estos grandes sistemas se están implantando gradualmente y, aunque el plazo de cada una puede diferir entre tres o cuatros años para finalizarlas, su evaluación se realiza de manera continua.

En el marco de las evaluaciones Schengen 2021-2025, se han llevado a cabo auditorías sobre grandes sistemas de información de la UE como son el Sistema de Información de Visados (VIS), el Sistema de Información Schengen (SIS II) y el EURODAC. De este modo, sobre el VIS, se han realizado entre otras inspecciones en la Sección Consular de la Embajada de España en Emiratos Árabes Unidos, en la Comisaría General de Extranjería y Fronteras, o en el Consulado General de España en Nueva York. En relación con el SIS II, se han inspeccionado, entre otros, la Jefatura de Servicios Técnicos de la Guardia Civil, la Oficina de Enlace del Sistema de Información Schengen o el Centro Tecnológico de Seguridad, de la Secretaría de Estado de Seguridad del Ministerio del Interior. Por último, este año 2023 se ha incluido al listado un nuevo gran sistema de las infraestructuras europeas: EURODAC.

La mayor actividad del año se ha dedicado a la preparación de las auditorías, estudiando el sistema y su reglamentación específica, y a finales de año se produjo la primera inspección a la Comisaria General de Policía Científica de la Policía Nacional, responsables del Punto de Acceso Nacional a EURODAC.

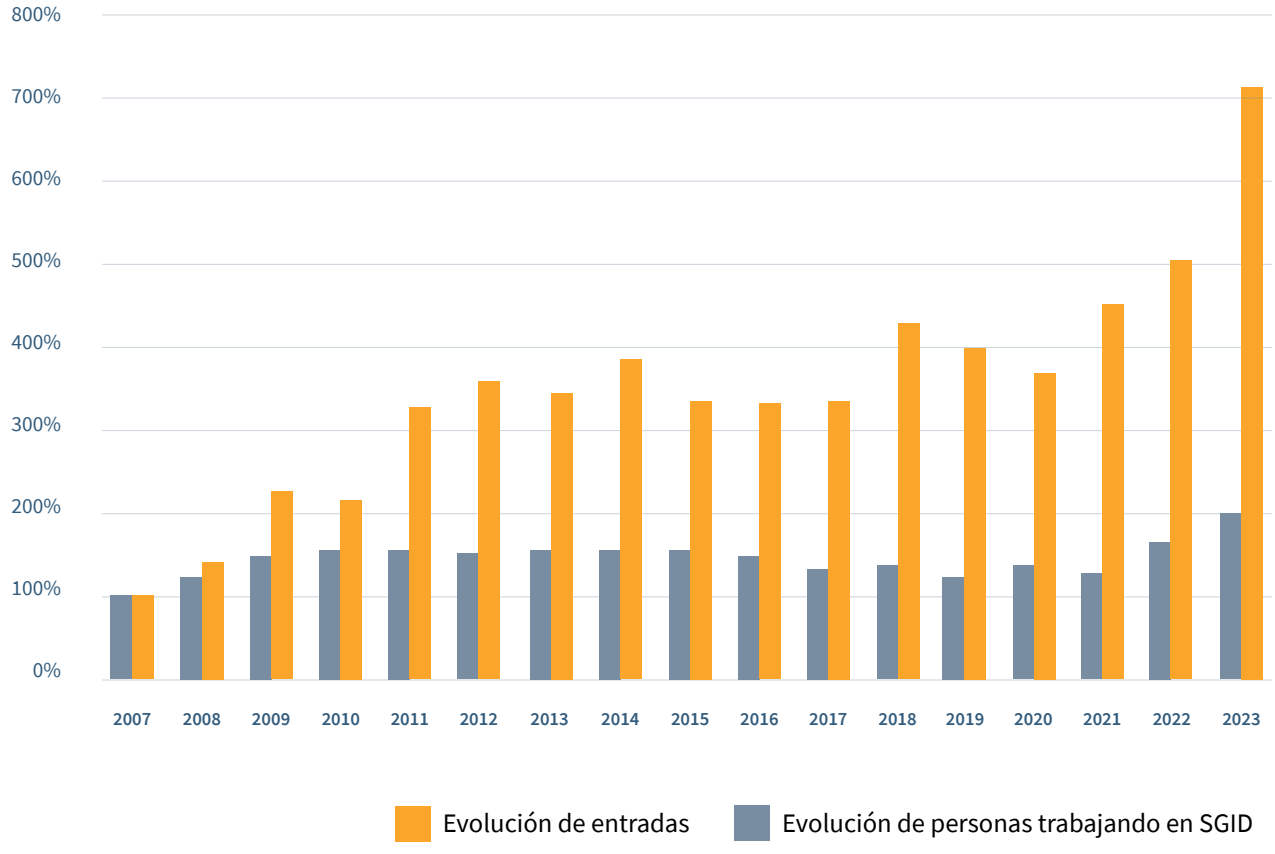
Finalmente, entre los resultados anuales se debe hacer referencia al **Canal prioritario de la Agencia para solicitar la retirada urgente de contenidos sexuales o violentos publicados en Internet sin consentimiento**.

El número de entradas recibidas por este canal se ha incrementado en un 36%.

Sin embargo, si se tiene en cuenta el análisis previo que realiza la Agencia sobre estos casos, las entradas que efectivamente han sido tramitadas como urgentes ha sido un 32% inferior a las del año previo. La tasa de eficacia de las intervenciones, medida por la proporción de retiradas de contenido requeridas y las efectivamente cumplidas en el año ha sido de un 94%. Las medidas cautelares que no han resultado eficaces en el año se firmaron durante los últimos días de 2023, por ello a final de año figuran pendientes de cumplimiento, destacándose que el resto de las medidas emitidas durante el año han resultado eficaces en un 100%. No obstante, durante los primeros días del año 2024 esas medidas se cumplieron, por lo que se puede decir que la eficacia en el cumplimiento de las medidas de retirada urgente de contenidos efectuadas durante 2023 ha tenido un 100% de cumplimiento.

El detalle completo del volumen de trámites realizados por la Subdirección General de Inspección de Datos y su valoración se ha incluido en el apartado de esta Memoria denominado La Agencia en cifras.

Evolución compatariva del nº de entradas y del personal de la SGID, 2007- 2023



Para evitar el desbordamiento y el consiguiente colapso que puede producir toda la carga de trabajo que se ha reflejado en los párrafos anteriores, entre los que se destaca un aumento del 43% en las reclamaciones en un solo año, la Agencia está desarrollando desde hace algunos años varias estrategias para hacer frente al trabajo. Se basan en tres pilares fundamentales: adecuación de la plantilla, simplificación y automatización y modificaciones normativas.

El primero, pasa por la adecuación del personal. En este caso, la creación de nuevas plazas es un aspecto fundamental: en el año 2022 se incorporaron 14 personas y durante este último año 2023 lo han hecho otras 17.

De esta manera, hoy esta subdirección cuenta con el doble de trabajadores que había en 2007. Pero las reclamaciones recibidas crecen a un ritmo muy superior, siendo siete veces las que se recibían en ese año.

En el gráfico anterior se compara el ritmo de crecimiento del personal, frente al de las entradas que generan nuevos expedientes (mayoritariamente reclamaciones ante la AEPD, pero también casos recibidos de otras autoridades del espacio europeo, canal prioritario de menores, notificaciones de brechas de seguridad en las que se abre investigación, y otros casos de propia iniciativa).

Además, del incremento en el número de las reclamaciones hay que tener en cuenta otra tendencia que viene siendo habitual que es una mayor extensión del ámbito de las reclamaciones e infracciones investigadas, con una menor presencia de casos individuales y una mayor presencia de casos que afectan a una generalidad de afectados, de forma real o potencial, por deficiencias de los procedimientos de tratamiento de datos personales. Este mayor alcance se refleja también en la amplitud de las actuaciones que la SGID desarrolla en respuesta a estos casos, que ya no precisan la investigación y corrección de un caso particular, sino el análisis y adecuación de los procedimientos del responsable a lo que exige la normativa. Lo que implica que las actuaciones previas de investigación que se han realizado tienen una complejidad mucho mayor, dado que no es lo mismo analizar un caso particular que un caso en el que puede haber un mal diseño, que puede afectar a multitud de personas.

Por ello es importante adecuar la plantilla a la carga de trabajo. A la hora de incorporar nuevo personal a la Agencia hay que tener en cuenta que la protección de datos personales es un tema muy específico y es muy difícil encontrar personal especializado. **Todas las nuevas incorporaciones han recibido una formación introductoria de dos meses para el desarrollo de su trabajo**, además del propio plan de formación anual de la Agencia, que incluye algunos cursos especializados.

En paralelo a la incorporación de nuevo personal, ha sido necesario **reorganizar la subdirección** dotando de más efectivos en las áreas de evaluación de la admisibilidad de la reclamación para evitar el colapso en la entrada debido al alto volumen de reclamaciones, permitiendo tratar de manera adecuada las reclamaciones y poder decidir en el plazo de tres meses sobre su admisión a trámite.

Sin embargo, esta reestructuración ha originado que las áreas que llevan los procedimientos, entre ellos los sancionadores, se hayan visto mermadas de efectivos lo que provoca un **problema en el medio plazo que está pendiente de solucionar con la incorporación de nuevas personas durante el año 2024**.

En el segundo eje en el que se ha trabajado para adecuar la carga de trabajo ha sido el de la **automatización**. Durante 2023 se ha añadido automatización en diversos pasos de los procedimientos de la SGID, tanto basada en sistemas de información, como en modelado de documentos dinámicos, con el objeto de reducir los tiempos de tramitación.

Se han puesto en práctica los primeros procesos de robotización para tareas repetitivas y mecánicas que se venían haciendo durante la tramitación de

ciertos expedientes. Estos cambios no suponen una reducción importante de la carga de trabajo, pero sirven para descargar al personal de tareas mecánicas, permitiendo que puedan dedicarse a otras actividades en las que es necesario la intervención de los profesionales. Adicionalmente se siguen evaluado otras técnicas para su futura incorporación en distintas tareas auxiliares a los procedimientos.

Por último, relacionado con la simplificación y automatización, durante este año 2023 se ha trabajado en el **diseño de un nuevo buzón de reclamaciones en la sede electrónica de la AEPD**. Este buzón tiene como objetivo facilitar la presentación de las reclamaciones a los ciudadanos, ya que los guía indicando los distintos documentos que tienen que presentar y formulando las preguntas necesarias para que la reclamación quede completa. El buzón, además de ser una de las recomendaciones de la normativa, permite una mejor clasificación de las reclamaciones recibidas y cataloga los documentos aportados, lo que redunda en una mejora en el trabajo que debe realizar la SGID. Se puso en marcha en los últimos días del año, comenzando con las reclamaciones de publicidad no deseada, uno de los ámbitos donde año tras año se producen mayor número de reclamaciones, en aumento en 2023 desde la aplicación de las obligaciones de la nueva Ley General de Telecomunicaciones para las llamadas comerciales.

El tercer gran eje en el que se venía trabajando es el de la modificación normativa. Durante 2023, se han aprobado las modificaciones a la LOPDGDD, que dan mejor cobertura a los procedimientos de respuestas a las reclamaciones. Entre las modificaciones cabe destacar la **creación del procedimiento de apercibimiento**, la regularización de la posibilidad de realizar investigaciones en remoto o la posibilidad de establecer modelos de presentación de reclamaciones de uso obligatorio. El procedimiento de apercibimiento es un procedimiento novedoso y totalmente diferenciado del sancionador, que permite, además de apercibir al responsable, en caso necesario, incluir medidas correctivas, como en el resto de los procedimientos que define la LOPDGG.

La LOPDGDD prevé, en su Disposición Adicional vigésima tercera, que la AEPD podrá establecer modelos de presentación de reclamaciones en todos los ámbitos en los que tenga competencia, que serán de uso obligatorio para los interesados con independencia de que estén obligados o no a relacionarse electrónicamente con las administraciones públicas. En virtud de esta potestad, la Agencia ha establecido en 2023 un modelo general de presentación de reclamaciones y seis modelos específicos referidos a distintos tratamientos de datos personales, aprobados por **resolución** de la directora el 29 de junio de 2023. Entre los modelos específicos se encuentra el destinado a casos de desatención por el responsable del tratamiento de una solicitud de ejercicio de los derechos; así como aquellos reservados a casos de recepción de publicidad directa no deseada; instalación de dispositivos de videovigilancia; incumplimientos en el tratamiento de datos vinculados a deudas; canal prioritario y brechas de datos personales. Con esta resolución, se facilita al ciudadano la información que tiene que incorporar a su reclamación para sea eficaz.

5.2 Reclamaciones y procedimientos más relevantes

En 2023, **destaca** especialmente el **aumento de las reclamaciones** recibidas en relación con la recepción de **publicidad no deseada**, que se **incrementaron un 114% respecto a 2022** y se sitúan en primer lugar en cuanto al grupo principal de actividad con un **20% de las reclamaciones recibidas**.

De estas, la mayoría hace referencia a **llamadas telefónicas comerciales no deseadas**, como es el caso del **procedimiento PS/00040/2023 contra BOX 24 2050 S.L.** Este expediente se inicia a través de una reclamación por la recepción de llamadas comerciales de ROMBOC S.L., entidad que dispone de los datos de consumo energético del reclamante, y a la que no ha otorgado su consentimiento. A raíz de las actuaciones previas de investigación

se evidencia que esta empresa utiliza la base de datos de CONCENTRA CENTRAL DE COMPRAS Y SERVICIOS, S.L., que a su vez la obtenía de ATRATO MEDIA, S.L. y ésta, a su vez, de BOX 24 2050 SL. Se imputa una infracción del artículo 6.1 del RGPD con una **sanción de 2.000 euros**.

También se dan casos de recepción de publicidad a través de **SMS**, como el **procedimiento PS/00136/2022 contra AD735 DATA MEDIA ADVERTISING S.L**. El origen del procedimiento es una reclamación presentada por el afectado que, tras ejercer sus derechos de acceso, oposición y limitación del tratamiento, recibe una comunicación comercial por SMS en su teléfono sin que lo hubiera solicitado ni autorizado. Se sanciona por la infracción del artículo 7.1 del RGPD, con una **multa de 5.000 euros**, al no poder acreditar el responsable del tratamiento que estos habían sido obtenidos con el consentimiento del reclamante.

También por la **obtención de datos personales sin consentimiento** encontramos el **PS/00352/2023 contra SUMINISTRADOR IBÉRICO DE ENERGÍA**. En este caso, los datos personales se utilizaron para la formalización de un contrato de suministro de electricidad, sin que haya existido consentimiento previo ni el reclamante haya facilitado dichos datos, procediendo a realizar cargos en su cuenta bancaria en virtud de dicha contratación no consentida. Se impone una sanción de 50.000 euros por una infracción del artículo 6.1. del RGPD. En el mismo sector de la energía y por contratación fraudulenta se resolvió el PS/00546/2022 contra IBERDROLA CLIENTES, S.A.U. Esta entidad gestionó un cambio de comercializadora y un cambio de titular para un número de CUPS que no es el de la vivienda de su cliente sino de la del reclamante. Se sanciona por infracción del artículo 5.1.d) del RGPD con una **multa de 70.000 euros**.

También por **contratación fraudulenta**, encontramos el **PS/00677/2022 contra BANCO BILBAO VIZCAYA ARGENTARIA**. El origen del expediente es una reclamación, en la que la reclamante ponía de manifiesto el robo de su bolso, donde se encontraba su teléfono móvil, su DNI y otros documentos que contenían los datos personales de aquella, la comunicación de este robo al banco, la suplantación de su identidad y la contratación de diversos productos financieros, así como la inclusión de la reclamante en un fichero de morosos. En este procedimiento sancionador se han incluido cuestiones relativas a este caso puntual y otras al protocolo establecido, que afectaban a la reclamante y al resto de clientes de la entidad. **La multa total es de 1.640.000 euros** por infracciones de los artículos 6.1, 32 y 25 del RGPD.

Esta sanción corresponde a **tres infracciones relacionadas** con el caso concreto denunciado por la reclamante:

- una infracción del artículo 6.1 del RGPD, en relación con la **contratación no autorizada de productos (70.000 euros)**,
- una infracción del artículo 32 del RGPD, por la **falta de medidas de seguridad** en relación con los procedimientos de comunicación, inclusión y mantenimiento en los sistemas de información crediticia de datos personales (**500.000 euros**)
- y otra infracción del artículo 6.1 del RGPD, en relación con la **incorporación de datos personales en los sistemas de información crediticia (70.000 euros)**;
- y otras dos infracciones relacionadas con la forma en la que se establecieron los **protocolos implantados por el BBVA** y que fueron revelados a través de la información aportada por la entidad financiera durante las actuaciones de investigación:
  - una infracción del artículo 25 del RGPD (500.000 euros) en relación con los protocolos establecidos para la detección del fraude
  - y una infracción del artículo 32 del RGPD, por la falta de medidas de seguridad en relación con los procedimientos de contratación de productos financieros (500.000 euros).

El procedimiento sancionador **PS/00456/2022 también contra BANCO BILBAO VIZCAYA ARGENTARIA**, se inició igualmente como consecuencia de una reclamación en la que la afectada señala que, tras extraviar su DNI y cursar la correspondiente denuncia, un tercero acudió a una sucursal de la reclamada suplantando su identidad siéndole facilitada información bancaria, además de entregarle la totalidad del dinero que se encontraba depositado en la cuenta. Se imputan dos infracciones de los artículos 6.1 y 32.1 del RGPD con **sanciones respectivas de 50.000 y 20.000 euros**.

En el sector financiero, por infracción los artículos 25 y 32 del RGPD se sanciona a **OPEN BANK, S.A. en el procedimiento PS/00331/2022**, iniciado por una reclamación presentada por un interesado ante la Autoridad de Protección de Datos de Baviera (Alemania), debido a que no se le ha facilitado por parte de la empresa ningún medio de comunicación seguro para aportar documentación con datos personales de carácter financiero. En este caso se concluye que OPENBANK no había previsto la actividad de tratamiento consistente en la recogida de datos financieros de los clientes para la prevención del blanqueo de capitales. Al no preverse esta actividad por OPENBANK, no se habían identificado y evaluado los riesgos en los derechos y libertades de los clientes presentes en tal tratamiento y, por lo tanto, no se han establecido ni aplicado las medidas técnicas y organizativas apropiadas para aplicar de forma efectiva los principios de protección de datos (entre otros, la confidencialidad) y cumplir los requisitos del RGPD y proteger los derechos de los interesados (de todos sus clientes).

Todo lo anterior pone de manifiesto que **OPENBANK no cumplió con su obligación de aplicar el artículo 25 del RGPD, la privacidad desde el diseño**, ni antes ni durante la realización del tratamiento. En cuanto a la infracción del artículo 32 del RGPD, OPENBANK no facilitó a su cliente un medio apropiado para aportar la documentación ni siquiera pese a las advertencias de la parte reclamante en este sentido, por lo que el envío se hizo sin las medidas de seguridad adecuadas (ni siquiera preveía un mero cifrado). Por todo ello, se impone una **sanción de 2.500.000 euros**.

En el mismo sector destaca el procedimiento **PS/00020/2023 contra CAIXABANK** que ha finalizado con una **multa de 5.000.000 euros** por infracción de los artículos 5.1.f, 25 y 32 del RGPD. Este procedimiento se inició por una brecha de datos personales en la que un cliente de la entidad ha tenido acceso, durante un prolongado periodo de tiempo, al resguardo de una transferencia efectuada por otro cliente y no ha tenido a su disposición el comprobante de la actualización de datos que había realizado. Durante la investigación **se detectaron fallos en el diseño del sistema informático, así como fallos en las medidas de seguridad**.

Otro procedimiento relevante en materia de brechas de datos personales es el **PS/00002/2023 contra ENDESA ENERGÍA S.A.U**. Endesa tuvo conocimiento de la brecha con motivo de la publicación de anuncios en Facebook ofertando la venta de credenciales para acceder a la plataforma de Endesa. Tras este primer anuncio continuaron publicándose en Facebook anuncios sobre la venta de credenciales. Se sancionó a Endesa con 6.100.000 euros por diversas infracciones:

- artículo 5.1. f) del RGPD por **accesos indebidos a datos** de millones de clientes y no clientes y por no garantizar la integridad de datos de 760 afectados (**2.500.000 euros**);
- artículo 32 del RGPD por **no contar con medidas apropiadas** antes del incidente y por no haber adoptado las medidas apropiadas después de identificar los anuncios en FB (**1.500.000 euros**);
- artículo 33 del RGPD por haber **notificado la brecha meses después** de detectar los anuncios en FB (**800.000 euros**);
- artículo 34 del RGPD por haber dado **información incompleta en la comunicación a los afectados** (a pesar de haber sido ordenada por la Agencia) (**800.000 euros**)
- y artículo 44 del RGPD por **realizar transferencias internacionales a los proveedores** en Colombia y Perú (**500.000 euros**).

También por **falta de medidas de seguridad adecuadas** y de otras medidas se inició el **PS/00062/2022 contra AVALIA ARAGÓN SOCIEDAD DE GARANTÍA RECÍPROCA**, estableciéndose en la resolución infracciones del artículo 5.1.f) del RGPD (los datos personales están en la deep web) y el artículo 32 del RGPD. Se impone u**na sanción de 40.000 euros y otra de 20.000 euros** respectivamente.

En el **PS/00084/2022 contra AFIANZA ASESORES**, también hay una **brecha de datos personales** que se produjo por el robo de un dispositivo USB por un desconocido (persona externa a la organización), conteniendo documentos de las diligencias previas de un juzgado de la Audiencia Nacional, con datos básicos, económicos, de contacto, y de infracciones penales o condenas de 100 afectados. Se **impusieron dos sanciones: de 90.000 euros** por la infracción del artículo 5.1.f) del RGPD **y de 55.000 euros** por la infracción del 32 del RGPD.

Por **otra brecha de datos personales**, en este caso **en el ámbito sanitario**, en el **PS/00085/2022 se sancionó a la CONSEJERÍA DE SANIDAD DE LA COMUNIDAD DE MADRID** con apercibimiento por una infracción del Artículo 5.1.f) del RGPD y otra infracción del Artículo 32 del RGPD debido a una brecha de confidencialidad sufrida en el portal web de la Consejería de Sanidad de la Comunidad Madrid para la obtención del Certificado COVID Digital. Esta brecha de datos trascendió a prensa puesto que se pudo acceder a los datos de altas personalidades del Estado. La Consejería alegó estado de necesidad y un supuesto error humano en la puesta en producción de la aplicación que permitió accesos indebidos a datos personales. No cabe apreciar en el presente caso estado de necesidad que justifique la puesta en producción de una aplicación de forma defectuosa o con errores, que permita el acceso ilegítimo a datos personales -entre ellos, de salud- de un elevado número de ciudadanos, sin realizar previamente las comprobaciones necesarias para determinar su correcto funcionamiento, en especial, el cumplimiento de todas las obligaciones impuestas por el RGPD y demás normativa de aplicación.

También en el ámbito de las **brechas de datos personales** en el **sector sanitario**, en este caso por un ciberincidente de tipo ransomware, encontramos el **PS/00529/2022 contra INSTITUT MARQUÉS OBSTETRICIA I GINECOLOGIA, SL.P**. Tras la investigación realizada por la AEPD se deduce que las medidas que tenía la clínica no eran las más adecuadas por lo que se imputan infracciones de los artículos 5.1.f), 32 y 34 del RGPD, a los que correspondería **una sanción de multa administrativa de 50.000, 20.000 y 10.000 euros**, respectivamente.

Relacionado con una **brecha de datos personales** y por la persistente falta de respuesta a un requerimiento de información se resolvió el **PS/00686/2022 contra PREICO JURÍDICOS, S.L.** con una **sanción de 6.000 euros**.

Para terminar con las **brechas que afectan a datos personales**, el **PS/00045/2023 contra EMAILING NETWORK SARL** se inició por la denuncia de un particular en Francia que, al intentar darse de baja en la web clicplan.com, únicamente introduciendo el dato de correo electrónico con el que se suscribió, se le ofrecían sus datos personales, sin necesidad de contraseña. La autoridad de protección de datos francesa, CNIL, realizó investigaciones relacionadas con EMAILING NETWORK SARL (empresa francesa) perteneciente al grupo empresarial REWORLD MEDIA y constató que los empleados y el delegado de protección de datos de EMAILING NETWORK se encontraban en España. Se declaró una infracción del artículo 25 del RGPD, por cuanto no se realizó un análisis de riesgos adecuado ni se establecieron medidas para garantizar el cumplimiento del principio de confidencialidad con u**na sanción de multa de 10.000 euros**.

Por otro lado, los casos procedentes de otras autoridades de control del EEE han aumentado en 2023 un 51%.

Procedente de reclamación ante la **autoridad de protección de datos de Sajonia (Alemania)**, Saxon Data Protection Commissioner, se tramitó el **PS/00328/2022, contra la empresa española THE MAIL TRACK COMPANY, S.L.** La compañía ofrece un software gratuito para rastreo de correos electrónicos de forma que el emisor de un

correo es informado a través del programa de que el receptor lo ha abierto y cuándo. Además, tales correos proporcionan un enlace al home page de mailtrack.io. Si el receptor reenvía el correo, se insertan elementos dentro del mail y esto podría transferir sus datos a terceros. Se imputan a MAIL TRACK infracciones del artículo 13 Y 14 del RGPD, por no informar de que ella es la responsable del tratamiento (sanción 20.000 euros); del artículo 6 del RGPD, por los tratamientos posteriores como la mejora del servicio (sanción 30.000 euros) y del artículo 5.1.a) del RGPD, por incumplir el principio de lealtad y transparencia, dado que informan de la posibilidad de excluirse del seguimiento a través de un procedimiento engañoso (**sanción 50.000 euros**).

En el **PS/00014/2023 contra VACACIONES EDREAMS, S.L.** se interpuso una reclamación ante la autoridad de protección de datos de **Hamburgo por un derecho de acceso**. Este acceso fue denegado indicando que deberían dirigirse al servicio telefónico correspondiente para obtener el acceso a la información. Posteriormente, el representante de la parte reclamante insistió en recibir la respuesta por escrito, pero no recibió ninguna contestación a esta petición. Se impone a VACACIONES EDREAMS por una infracción del Artículo 15 del RGPD una **multa de 10.000 euros**.

También procedente de otra autoridad de control, encontramos el **PS/00209/2022 contra GLOVOAPP23, S.L.** El expediente se inició con motivo de la información facilitada por la autoridad de protección de datos de **Italia** que había realizado una investigación, en la que se descubrió que las actividades involucradas en la entrega de comida u otros artículos por los repartidores, con la ayuda de una plataforma técnica específica, propiedad de GLOVOAPP23, S.L., **entrañaba el tratamiento de una amplia gama de datos personales**, como ubicación geográfica (en tiempo real); monitorización de cada paso de la entrega; valoraciones de los repartidores por los clientes o vendedores; puntuaciones de reputación, etc. Se imputaron a GLOVOAPP23, S.L las infracciones de los artículos 13, 25 y 32 del RGPD. La resolución sanciona a la empresa con apercibimiento por la infracción del artículo 13 del RGPD y con **multa de 550.000 euros** por las infracciones de los artículos 25 y 32 del RGPD.

Otro caso procedente de otra autoridad es el **PS/00173/2023,** iniciado por una reclamación ante Urząd Ochrony Danych Osobowych, autoridad de protección de datos de **Polonia**, contra **YUDAYA, S.L.**, cadena propietaria del hotel HD Acuario Lifestyle (ubicado en Las Palmas de Gran Canaria) por la realización de una **copia de su documento de identidad sin proporcionarle la información requerida** por el artículo 13 del RGPD. Se resolvió con la imposición de **multa administrativa de 20.000 euros** por infracción de los artículos 13 y 15 del RGPD.

Muy similar, por la realización de la **copia del DNI** en un establecimiento hotelero, se realizó el **PS/00499/2022 contra MARKETING ACCOMMODATION SOLUTIONS FZ**. Esta empresa exigía para hacer el check-in online la imagen del DNI, por los dos lados y carecía de una política de privacidad completa. Se impuso una **multa de 50.000 euros** por la infracción del artículo 13 del RGPD.

También en el sector del ocio encontramos el **PS/00349/2022 contra VACACIONES EDREAMS, S.L.** La web de esta empresa fue denunciada por el uso de la cookie Google Analytics que **transfiere datos a Google LLC** con sede en EE.UU. después de que el TJUE declarara nulo el escudo de privacidad (sentencia del asunto C-311/18 "Schrems II"). **La cookie transfiere datos a Google LLC que se consideran datos personales.** Por ello se considera a VACACIONES EDREAMS exportador de datos y a Google LLC importador.

Las transferencias se realizan incumpliendo el artículo 44 del RGPD., puesto que el escudo de privacidad fue anulado y la nueva decisión de adecuación de la Comisión, de fecha 10 de julio de 2023, no es de aplicación automática pues requiere que las entidades se adhieran a los principios. En la resolución, **no se impone a VACACIONES EDREAMS, S.L. sanción de multa**, pero se le ordena, por una infracción del Artículo 44 del RGPD, que en el plazo de un mes acredite ante esta Agencia que ha adaptado la actividad de tratamiento de datos al servicio de Google Analytics a lo dispuesto en los artículos 44 y siguientes del RGPD, en particular mediante el cese de la transferencia internacional de datos hasta que se acredite que el servicio de Google

Analytics cumple con las citadas disposiciones del Reglamento.

Otro caso relacionado con **cookies** es el **PS/00051/2023 contra el GRUPO MASSIMO DUTTI, S.A** por la **utilización de las cookies y la obtención del consentimiento** del usuario en su página web. Se tramita el procedimiento sancionador por la comisión de una infracción del artículo 22.2 de la LSSI, por la ausencia de información suficiente en la primera capa acerca de las finalidades de la instalación de las cookies con **sanción de 5.000 euros**.

También por infracción del artículo 22.2 de la LSSI, por las **deficiencias detectadas en su página web** respecto de la "Política de Cookies", se impone una **sanción de 5.000 euros** en el **PS/00080/2023 contra CHATWITH.IO WORLDWIDE, S.L.**, titular de la página web a web www.iurisnow.com. En este procedimiento, además, se constata que la política de privacidad no facilita información sobre los fines, los intereses legítimos y sobre las transferencias internacionales por lo que se impone una **multa de 2.000 euros** por Infracción del artículo 13 del RGPD. Se comprueba que existe una lista de unas 130 empresas, de las cuales, más de la mitad tienen marcada por defecto la casilla de "aceptar tratamiento de datos por Interés legítimo", lo que obliga, en el caso de querer mostrar la oposición al tratamiento, a marcar una a una las opciones de la lista, sin que exista la opción de poder oponerse a todo o rechazar todo. Por esto se impone una **multa de 5.000 euros** por Infracción del artículo 5.1.a) del RGPD.

Para finalizar con los casos relacionados con **cookies**, en el **PS/00345/2022 contra el COLEGIO OFICIAL DE ARQUITECTOS DE GRANADA** se sanciona también por una infracción del artículo 22.2 de la LSSI, respecto a **la utilización de cookies de terceros de carácter no exceptuado**, sin el consentimiento del usuario con **1.000 euros**. Además, se sanciona por infracción del artículo 13 del RGPD, por la falta de información suministrada en las hojas de reclamaciones sobre el tratamiento de los datos personales obtenidos, con una sanción de 8.000 euros, y por infracción del artículo 38.6 del RGPD, por el conflicto de intereses detectado en el nombramiento del Secretario del Colegio como delegado de protección de datos una **sanción de 5.000 euros**.

También relacionado con la figura del **delegado de protección de datos**, encontramos el procedimiento **PS/00253/2023 contra APOLLONIA TOPCO, S.L.** Este **caso es novedoso** porque, por primera vez, se imputa al responsable una infracción del artículo 38.4 del RGPD, que reconoce el derecho de los interesados a ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del RGPD. La exposición de motivos de la LOPDGDD destaca respecto de la figura del delegado de protección de datos que "permite configurar un medio para la resolución amistosa de reclamaciones, pues el interesado podrá reproducir ante él la reclamación que no sea atendida por el responsable o encargado del tratamiento", lo que se plasma en el artículo 37.1 de la LOPDGDD. Además, **se sanciona** a la reclamada por infracción del artículo 5.1.c) del RGPD, por importe de **20.000 euros** y por la infracción del artículo 38 del RGPD por **importe de 10.000 euros**.

También se sanciona por **deficiencias relacionadas con el delegado de protección de datos** en el **PS/00308/2023 contra RAMONA FILMS, S.L.** Además de otras infracciones, se imputa que **no consta el DPD suministrado** de la reclamada en los sistemas de esta Agencia y que este actuaba como responsable de algunos de los tratamientos. Por otra parte, la reclamada es responsable de varios portales web en los que, aunque tienen un mecanismo para declarar la edad de quien accede a la página, no funciona correctamente, al ser fácilmente fácil de eludir, y que además no sirve para verificar la edad de quien accede. Se detectan además deficiencias en contratos de tratamiento suscritos y una necesidad de adecuación de la política de privacidad. Se resuelve imponer a RAMONA FILMS, S.L. **multa administrativa de 486.600 euros** por las infracciones de los artículos 6.1.a), 13, 28.3,32,37.38.6 del RGPD y del artículo 22.2 de la LSSI.

Además de la multa administrativa, cabe destacar las medidas impuestas para asegurar la protección de los datos de los usuarios, entre las que destaca el establecimiento de las medidas de seguridad adecuadas para adaptar los sistemas o mecanismos de verificación de la edad a las exigencias legales y asegurar que no se produce tratamiento de datos personales de menores. En el caso de las webs dedicadas a la pornografía existe un riesgo cierto de que los menores de edad accedan directamente y sin limitaciones a un contenido perjudicial para ellos:

el **acceso indiscriminado de los menores a la pornografía** en internet constituye un **alto riesgo en sus derechos y libertades**.

En relación con esta temática, se ha realizado el seguimiento de las medidas correctivas dictadas en el 2022 en la resolución del **PS/00555/2021 contra TECHPUMP SOLUTIONS S.L.** Estas medidas estaban dirigidas a la **adecuación del tratamiento de sus datos personales** al RGPD, adoptando medidas de seguridad apropiadas mediante las que se verificase la edad de los usuarios, registrados o no, que accedan a las páginas web referenciadas, garantizando que son mayores de edad, impidiendo incidencias similares en un futuro.

Relacionados con menores se han tramitado varios procedimientos. El **PS/00601/2022** que se inicia por el traslado por parte el Juzgado de Instrucción Num. 9, de Alicante, a la AEPD, de las diligencias seguidas con motivo de la agresión sufrida por un menor que fueron sobreseídas al no constituir los hechos ilícito penal. **La agresión fue grabada por el investigado**, como confirma el Fiscal, y por tal motivo se trasladan a la AEPD por si existiera infracción.

Se impone una **sanción de 10.000 euros al investigado**, que es mayor de edad, por infracción del artículo 6.1 del RGPD. También se adopta la medida consistente en la suspensión total de todo tratamiento de datos personales del menor de edad.

Asimismo, se ha requerido la retirada de varios contenidos que afectan a menores en el AI/00442/2022.

También relacionado con menores, en el **RR/00851/2022** se desestima el recurso presentado **por FACUA contra la Resolución de Archivo del AI/00410/2022**. El archivo se produjo porque, tras un procedimiento iniciado de oficio (derivado de denuncias recibidas en relación con la publicación en Twitter y Facebook de unos audios en relación con el caso Arandina, grabados por la menor objeto de abusos) y tras tres años de investigaciones no fue posible determinar a quien pertenecían las cuentas desde las que se publican los audios (no se pudo determinar la autoría). **Las publicaciones denunciadas que contenían el audio al que se hacía referencia en las denuncias fueron eliminadas** de las direcciones informadas. Facua presenta recurso que se desestimó, porque la denuncia no acredita que el tuit estuviera publicado, y los hechos estaban ya prescritos por datar de diciembre de 2019.

En cuanto a los **procedimientos sancionadores**, el área de actividad con mayor número de procedimientos resueltos en el año 2023 es la **videovigilancia**.

Es el caso del procedimiento **PS/00450/2022**, que no es un supuesto ordinario de videovigilancia, sino que se trata de la **instalación de una videocámara dentro de una vivienda** alquilada a varios inquilinos. Dicha videocámara enfoca a distintas zonas del propio chalet sin base jurídica legitimadora para este tratamiento. Hay que destacar que se trata del domicilio de terceros (de los inquilinos) dado que el ámbito "personal y doméstico" en la captación de imágenes de las zonas comunes (artículo 22.5 LOPDGDD) desaparece al ceder el uso y disfrute temporal de la vivienda a un tercero. Pasando a convertirse en un ámbito reservado a la más estricta intimidad personal. Por esta falta de base jurídica que legitime el tratamiento de datos personales de la parte reclamante (su imagen), se declara una infracción del artículo 6.1 del RGPD

con una sanción de **multa administrativa de 5.000 euros**.

Muy similar es el **PS/00496/2022 contra ROMESTONE, S.L** por la colocación de una **cámara de videovigilancia en el hall de una vivienda** de alquiler por habitaciones individuales a estudiantes. Además, la cámara tiene un control de sonido para ver si se superan determinados decibelios (en caso de fiestas). Se imputa una infracción del artículo 6.1 del RGPD con una **multa de 6.000 euros** y se ordena la retirada de la cámara.

También por tratar datos de carácter personal de los reclamantes sin legitimación alguna de las contempladas en el artículo 6.1 del RGPD se han resuelto varias reclamaciones realizadas contra **QUALITY-PROVIDER S.A.**, **entidad que comercializa una base de datos**. El **PS/00030/2023**, en el que se le impone una **multa de 20.000 euros**, así como acreditar haber procedido al cumplimiento del derecho de supresión ejercido por el reclamante y adopción de medidas adecuadas y proporcionar la información requerida por la AEPD, y el PS/00517/2022, en el que se impone también una **multa de 20.000 euros**. En este segundo procedimiento además se intentó llevar a cabo una inspección presencial, pero QUALITY la obstaculizó. Esta actuación se sancionó en un procedimiento sancionador independiente, el **PS/00204/2023**, en el que se impone a QUALITY-PROVIDER S.A., por obstaculización la potestad de investigación que el artículo 58.1 del RGPD confiere a las autoridades de control, en este caso, la AEPD, una **multa de 20.000 euros**.

Relacionados con estos casos están el **PS/00509/2022 contra ESTUDIO INMOBILIARIO SAN ISIDRO, S.L.U** y el procedimiento **PS/00525/2022 contra la inmobiliario ESTUDIO VILLALBA ANTIQUE, SL** por la **consulta a dicha base de datos** sin base de legitimación y por utilizar la información para contactar a los reclamantes. En ambos casos, la **multa fue de 5.000 euros** por infracción del art. 6.1 del RGPD.

Por la puesta a disposición de datos personales sin tener legitimación para ello se ha resuelto el **PS/00058/2023 contra TECNOLOGÍA SISTEMAS Y APLICACIONES, (TECSISA)**.

En este procedimiento, la CNMC facilitó un informe realizado como consecuencia de sus propias investigaciones, en la que se observaba una **posible utilización fraudulenta del Sistema de Información de los Puntos de Suministro (SIPS)**, indicando que se habían identificado un conjunto de escenarios que sugerían posibles usos fraudulentos del SIPS.

En las actuaciones de investigación se constató que TECSISA había creado la plataforma Kommodo SIPS, a través de la cual sus clientes obtenían una copia del SIPS. Para el acceso al SIPS, TECSISA utilizaba las claves de la comercializadora NCE con la que había suscrito un contrato de encargado del tratamiento y ponía la información a disposición de sus clientes, comercializadoras de electricidad autorizadas y no autorizadas por la CNMC para su acceso a los datos del SIPS, incluso en situación de baja. TECSISA manifestó fundamentalmente que no accede a datos personales. No obstante, si bien es cierto que según el artículo 7 del Real Decreto 1435/2002, las empresas comercializadoras no pueden acceder a los datos identificativos y de domicilio del usuario, las comercializadoras sí acceden al número de CUPS y este número permite identificar al titular del suministro de manera univoca, por lo que es un dato personal. **Se sanciona a TECSISA** por infracción del artículo 6.1 del RGPD por la descarga de la base de datos del SIPS sin tener legitimación para ello (**sanción de 45.000 euros**) y por poner a disposición de los clientes del reclamado, empresas comercializadoras autorizadas y no autorizadas para el acceso al SIPS, la información de la base de datos sin tener legitimación para ello (**sanción de 45.000 euros**) y por la infracción del artículo 25 del RGPD **una sanción de 25.000 euros.**

En el sector de las **telecomunicaciones**, se han tramitado los procedimientos **PS/00266/2023 y PS/00665/2022** en los que se sanciona a **VODAFONE ESPAÑA** con **100.000 euros y 140.000 euros respectivamente** por la **generación de duplicados de tarjeta SIM sin legitimación**. La conducta infractora consistió en un tratamiento de datos personales sin legitimación -duplicado SIM fraudulento- por no actuar diligentemente en la identificación de los solicitantes del duplicado.

También por una infracción del artículo 6.1 del RGPD tenemos el **PS/00271/2022 contra DIGI SPAIN TELECOM**, por la realización de una **portabilidad de la línea del reclamante por un tercero suplantador**, con una total ausencia de medidas válidas encaminadas a garantizar la identidad de la persona que otorga el consentimiento. Se impuso una **sanción de 70.000 euros**.

Continuando con el sector de las telecomunicaciones, en este caso en relación con el ejercicio de derechos encontramos el procedimiento de derechos **PD/00133/2023 contra VODAFONE ESPAÑA, S.A.U**, en el que la parte reclamante solicitó a Vodafone el acceso a una amplia información, entre la que se incluía el acceso al uso de TV y a los datos de tráfico, facturación y localización.

Vodafone facilitó el acceso a sus datos salvo a los datos citados de uso de TV y de tráfico, facturación y localización. En cuanto a los datos de uso de la TV, considera esta petición excesiva y que ha justificado la negativa a facilitarla. En lo relativo a los datos de tráfico necesarios para la facturación, la resolución tiene en cuenta el artículo 66.2 de la LGT el que dispone que el operador podrá tratarlos durante los plazos de impugnación de la factura, por lo que nada impide que la parte reclamante pueda tener acceso a los mismos durante este plazo. En cuanto a los datos de tráfico y localización que se conservan en cumplimiento de la Ley 25/2007, como en anteriores ocasiones se considera que la parte reclamante tiene derecho de acceso a tales datos al no establecerse ninguna limitación a este respecto en el artículo 9 de la Ley.

También en relación con el derecho de acceso, contra **VODAFONE ESPAÑA, S.A.U. se instruyó el PD/00033/2023**. El reclamante solicitó a Vodafone, acceso a los **datos de geolocalización** de cada una de las líneas contratadas con dicha empresa. A esta petición, dio respuesta Vodafone, facilitando el acceso a los datos personales obrantes en sus sistemas en relación con el reclamante e indicando los motivos por lo que no era posible facilitarle el histórico de los datos de ubicación y localización de todas sus líneas telefónicas. Motiva su negativa a facilitar datos de ubicación de las líneas de titularidad de la parte reclamante en que Vodafone conserva los datos de ubicación y localización exclusivamente al amparo de lo dispuesto en la Ley 25/2007, de 18 de octubre.

En la resolución se indica, en relación con el derecho de acceso del interesado a los datos de tráfico y localización conservados por los operadores en virtud de la ley 25/2007, que los operadores deben distinguir entre el titular del contrato y el usuario de cada línea, facilitando el acceso solo a este último.

También con el ejercicio de derechos, en este caso de **supresión**, encontramos el **PD/00140/2023 contra ROBOTSTXT, S.L.** El reclamante expone que el sitio web durcal.net publica un Boletín Oficial de Granada en el que figuran sus datos personales. Añade que solicitó la supresión de sus datos al responsable ROBOTSTXT, S.L. y que su solicitud fue denegada motivándola en que publican en su web una copia de un documento público procedente de un boletín oficial.

Se estima la reclamación, toda vez que el responsable no acredita la existencia de una base jurídica que legitime el tratamiento de los datos del reclamante.

El PS/00281/2022 contra SECURITAS DIRECT ESPAÑA, S.A. se inicia por **incumplimiento de un procedimiento de ejercicio de derechos**, al no proporcionar el derecho de acceso al interesado. El acceso se refiere a los logs que genera el dispositivo de alarma instalado en domicilio del afectado, que sufrió un robo y, según manifiesta, no fue avisado por la Compañía.

La SAN 3091/2019, de 23 de julio de 2019, define a los logs como “registros y señales captadas y enviada por el equipo de alarma instalado en un domicilio privado”.

Securitas Direct no suministra todos los logs al interesado, sino sólo aquellos que considera que son datos de carácter personal, y respecto de estos, se suministran en bruto y sin adjuntar documentación complementaria para su completa comprensión (desconocimiento del significado de las claves que figuran en el cuadro suministrado). La parte reclamada considera que los que

denomina logs técnicos no son datos de carácter personal, entre otras cuestiones porque no existe influencia o interactuación por parte del interesado. Además, aduce el secreto comercial para no suministrar todos los logs al interesado.

Este procedimiento sancionador dilucida si los logs técnicos son datos de carácter personal en este caso concreto y si el derecho de acceso resulta afectado por el derecho de secreto comercial aducido de contrario.

En la resolución, se considera que "todos los logs, incluyendo aquellos generados y almacenados en los que no interviene el titular-usuario, sea operado por empleados de Securitas en procesos en que no interactúe el titular, sea en operaciones técnicas de carácter interno que revelan información sobre la eficacia y funcionamiento, al tratarse de la alarma instalada en su vivienda, ligada al contrato de prestación de servicios suscrito, establecen una conexión entre el objeto (la alarma) y el afectado, puesto que la alarma está identificada con un identificador único (una numeración específica para cada dispositivo de alarma) para ese servicio que liga indefectiblemente al interesado con el dispositivo y todo lo que se genera y registra en relación con el mismo.

Se sancionó con 50.000 euros por infracción del artículo 58.2 del RGPD y, además, se imponen medidas para que suministre al reclamante el acceso en los términos explicitados en la resolución.

Pero no todos los procedimientos iniciados acaban en sanción. Un 11% de ellos se han resuelto con archivo.

En el **PS/00253/2022 contra PYRAMID CONSULTING, S.L.** durante la instrucción del procedimiento se constató una **falta de acreditación en los hechos** atribuidos a PYRAMID CONSULTING, en cuanto a la incorrecta identificación de la parte reclamante como autora de una infracción de tráfico, frente a la certeza y concreción exigida en estos supuestos para poder calificar la conducta como sancionable, concluyendo que no existe prueba de cargo suficiente contra la citada entidad, por lo que se procedió a acordar el archivo del procedimiento.

También finalizaron en archivo **el AI/00363/2022 contra OIZ RIDESHARING, el AI/00365/2022 contra TUCYCLE BIKESHARING, el AI/00362/2022 contra AVANT FULLSTEP, S.L., y el AI/00361/2022 contra ECO-LÓGICA TURISMO SOSTENIBLE, S.L.** En todos los casos se denuncia una reclamación en la que **se denuncia la comunicación de datos de usuarios entre distintas empresas** que prestan servicio de bikesharing, en las que no se informa a sus usuarios de tales comunicaciones, y no se recaba el consentimiento. Se realizan actuaciones previas de investigación y como consecuencia de ellas, se comprueba que las incidencias habían sido subsanadas antes de la admisión a trámite de las reclamaciones por lo que se archivan.

También se desestima la reclamación en el procedimiento **PD/00191/2023 contra la Consejería de Educación de Castilla y León**. La parte reclamante solicita el **derecho de acceso presencialmente** ante un registro de la Administración Autonómica de Castilla y León requiriendo la copia de los datos personales mediante medios electrónicos. La parte reclamada se lo deja a su disposición en la secretaría del centro donde cursa estudios la reclamante o alternativamente en la Dirección Provincial de Educación.

El debate se centra, por tanto, en el medio de entrega de la copia de los datos personales objeto del derecho, puesto que mientras la parte reclamante asevera que tiene derecho a que se los envíen por correo electrónico, la parte reclamada indica que la copia de los datos personales está a disposición de la parte reclamante, a los efectos de que elija el que más le convenga, en la Secretaría de los centros educativos, o alternativamente en la Dirección provincial de Educación de León.

La normativa relaciona la entrega de la copia de datos personales por medios electrónicos a supuestos en los que el interesado haya ejercido de dicha forma su derecho de acceso, y sin perjuicio de que se limite la entrega en dicho formato a supuestos en los que esto sea posible,

especialmente cuando hayan de aplicarse medidas de seguridad, en particular si hay categorías especiales de datos personales implicados. Cada responsable de tratamiento tendrá que determinar, respecto de la modalidad de copia de datos personales, el medio a través del cual va a facilitar el derecho de acceso, atendiendo a las características de su propia organización, a la tipología de los datos personales afectados, a las medidas de seguridad precisas o las circunstancias del interesado, entre otras. Y siempre que no suponga una carga excesiva o un impedimento para el interesado (frustrando el derecho mismo).

La **Administración Pública también es objeto de investigaciones y procedimientos**, que culminan con la declaración de infracción y la imposición de medidas, y que deben comunicarse al Defensor del Pueblo.

Durante el 2023 se han instruido varios procedimientos como el **PS/00476/2022 contra el Ayuntamiento de Ourense** por no adoptar medidas adecuadas para evitar la publicación de datos personales del reclamante en relación con una sentencia, ni para impedir que la información continuara siendo accesible tras su retirada de la web. **Se sanciona al Ayuntamiento por una infracción del Artículo 5.1.f) con apercibimiento**.

En el **PS/00031/2023 se sanciona a DIRECCIÓN GENERAL DE TRÁFICO**. En este caso, las actuaciones se iniciaron de oficio como consecuencia de la documentación trasladada por la DGT al Gabinete jurídico para la emisión de informe sobre el **proyecto "Libro Taller",** que es un servicio a través del cual los talleres de reparación de vehículos comunican a al DGT las reparaciones realizadas en un vehículo con la finalidad de que pueda ser consultada la información por cualquier ciudadano, mediante la obtención de un informe del vehículo.

Se considera que **no existe base de legitimación pues los talleres no obtienen un consentimiento informado, específico y libre**. No se facilita la información necesaria sobre los fines y no existe un procedimiento para que los interesados puedan retirar el consentimiento. Tampoco puede ampararse el tratamiento en el interés público, por cuanto se recogen datos que no constan en la normativa que regula el Registro de Vehículos y no existe una norma que declare el interés público de este nuevo tratamiento, lo que constituye una infracción del artículo 6.1. del RGPD. Además, no se ha realizado un análisis de riesgos ni previsto medidas para cumplir con los principios de licitud, exactitud y transparencia, con lo que se infringe el artículo 25.1. También se considera una infracción del artículo 32, puesto que los talleres pueden acceder a la información del Libro taller de los vehículos que van a reparar, pero no existen medidas que eviten que se consulte información que esté relacionada con otros vehículos y del artículo 30, ya que según la DGT este nuevo tratamiento se integra en las operaciones de tratamiento del Registro de vehículos, pero no se ha incluido en el RAT.

También es destacable el caso del **servicio de salud de Castilla-La Mancha en Talavera de la Reina**, por el que se inició el procedimiento sancionador **PS/00168/2022**. El procedimiento sancionador se inicia por los **accesos indebidos a historias clínicas por profesionales del Servicio de Salud** de Castilla-La Mancha (SESCAM). Se imponen **sanciones de apercibimiento** por las infracciones de los artículos 5.1.f), 32, 33 y 35 del RGPD. Asimismo, se propone al Servicio de Salud de Castilla-La Mancha la iniciación de actuaciones disciplinarias contra las personas responsables de los accesos indebidos y se da traslado de la reclamación a la Fiscalía General del Estado para que analice la posible comisión de un ilícito penal.

El **PS/00547/2022 contra la MANCOMUNIDAD DE LA COMARCA DE PAMPLONA** se inicia a consecuencia de una reclamación interpuesta contra los Servicios de la Comarca de Pamplona S.A., que ha implantado desde otoño de 2021 un sistema de apertura de contenedores de residuos a través de una **tarjeta electrónica vinculada a una determinada dirección postal**. Esta empresa pública buzoneó en el término municipal de Pamplona un sobre que contenía un folleto con dos tarjetas electrónicas adheridas, así como una hoja con datos de "usuario" y una contraseña para una aplicación móvil. En cada tarjeta constaba una dirección, que es la del inmueble a cuyo ocupante (sea quien sea, sin petición de identificación) se

entregaba el sobre. En la información facilitada por los interesados se indica que los datos de apertura de los contenedores, por cada una de las tarjetas, son tratados para analizar la utilización de los contenedores.

Si bien las tarjetas electrónicas para la apertura de contenedores de residuos en un primer momento fueron buzoneadas, con posterioridad las personas han podido solicitar una nueva tarjeta (en casos de pérdida, avería, rotura, cambio de domicilio), solicitar la activación de la tarjeta de transporte para la apertura de contenedores de residuos o solicitar credenciales para poder activar la aplicación móvil de apertura de contenedores de residuos.

En estos casos, además de tratar el dato personal del domicilio postal, se han tratado nuevos datos personales derivados de la recogida y registro de la presentación de las mencionadas solicitudes: DNI, nombre y apellidos, dirección de correo electrónico, número de teléfono, dirección postal, IDE tarjeta transporte, firma.

La implantación de un sistema de apertura de contenedores de residuos equipados con cerraduras electrónicas que se corresponden con Equipos de Control de Acceso (ECA) a tales contenedores, accionados mediante tarjeta vinculada a una determinada dirección postal, tarjeta de transporte activada para la apertura de contenedores o aplicación móvil vinculada a una determinada dirección postal supone, de conformidad con las definiciones del artículo 4 del RGPD, el tratamiento de un conjunto de datos personales.

Se sanciona a la Mancomunidad de la Comarca de Pamplona con apercibimiento por las siguientes infracciones: artículo 6.1 del RGPD, artículos 12.1, 13 y 14 del RGPD, artículo 30.1 del RGPD y artículo 35 del RGPD.

Además, se impone a la Mancomunidad de la Comarca de Pamplona, a que, en virtud del artículo 58.2.f) del RGPD, en el plazo de 10 días, acredite haber procedido al cese de dicho tratamiento de datos personales.

Por otra parte, en el **RR/00027/2023** se desestima el recurso de la **Consejería de Sanidad de la Junta de Comunidades de Castilla-La Mancha** de suspensión de la medida cautelar que impone limitar o suspender el tratamiento impuesta en el marco del **PS/00441/2021**. Se **sancionaba** a la Consejería de Sanidad de la Junta de Comunidades de Castilla-La Mancha por una infracción del artículo 35 del RGPD.

Esta medida cautelar consistía en la limitación temporal o definitiva del tratamiento del sistema de control horario mediante la huella dactilar, en tanto no disponga de una evaluación de impacto de protección de datos del tratamiento válida, que tenga en cuenta los riesgos para los derechos y libertades de los empleados y las medidas y garantías adecuadas para su tratamiento, o incluso si se realizara, precisara efectuar la previsión de consulta que se establece en el artículo 36 del RGPD.

Se desestima el recurso y se deniega la suspensión al prevalecer los derechos y libertades de los funcionarios (la suspensión vaciaría de contenido la parte citada de la resolución sancionadora), resultando que, además, disponen de alternativa por lo que no se estima que cause graves perjuicios frente a los derechos de los afectados y riesgos asociados al tratamiento.

Relacionado con el **tratamiento de datos biométricos** encontramos el **PS/00553/2021 contra GSMA LIMITED**. Este procedimiento se origina por una **reclamación de una asistente** al Congreso de Mobile Word en Barcelona 2021, contra la entidad que organiza el Congreso como titular de la web en la que se han de registrar los datos de los asistentes. Manifiesta que para registrarse en la modalidad "presencial", tiene que facilitar una **fotografía a la que aplican técnicas de reconocimiento facial** con fines de seguridad.

La entidad alega que existen dos modalidades para registro e identificación de los asistentes al evento: el llamado sistema común que no supone reconocimiento facial y el sistema de registro e identificación con reconocimiento facial, que lo basan en el consentimiento.

El uso de datos biométricos es consentido por los interesados mediante la marcación de una casilla. La reclamante no se registró en modo de uso de tecnología de reconocimiento facial.

Se inició el procedimiento a GSMA LTD por la presunta infracción del artículo 35 del RGPD. Si bien la reclamada aporto una Evaluación de Impacto relativa a la Protección de Datos, a lo largo del procedimiento se consideró que la evaluación de impacto no contiene aspectos esenciales, tales como la valoración de los riesgos y la proporcionalidad; la necesidad de la implantación del sistema, o su afectación a los derechos y libertades de los interesados y sus garantías. **Se sancionó** a GSMA LIMITED, por una infracción del artículo 35 del RGPD, **con una multa administrativa de 200.000 euros**.

También relacionado con el **tratamiento de datos biométricos** encontramos el **PS/00413/2022 contra METROPOLITAN SPAIN, S.L.** El motivo de la reclamación que lo origina es que se **exige** como requisito a los usuarios para el acceso a sus instalaciones el **uso de la huella dactilar**. El sistema se impone a los socios y quien no suministre sus datos biométricos no puede acceder al gimnasio. Sin habilitar un sistema alternativo para que sea libre.

Se impone una **sanción de 27.000 euros** por infracciones de los artículos 13, 9.1 y 6.1 del RGPD. Además, en la resolución también se imponen la necesidad de acreditar, una correcta y adecuada implantación del sistema de uso de huella dactilar para acceso a instalaciones, considerando y acreditando su necesidad y proporcionalidad atendiendo a instauración de una base de tratamiento lícita para el tratamiento de los datos, también respecto a los que ya se disponen de ese dato, y a su correlativa información del tratamiento asociada a la misma, así como proceder a: "limitar temporal o definitivamente el tratamiento" en el plazo de diez días sobre el uso del sistema de acceso al gimnasio con huella dactilar, en tanto no acomode la base legitimadora del tratamiento y su correcta información a los usuarios.

En el **ámbito educativo**, el **PS/00334/2022 se instruyó contra el Ministerio de Defensa** por la utilización de la herramienta Google Workspace for Education en el Colegio Menor Ntra. Sra. Loreto, colegio privado adscrito al Patronato de Huérfanos de la Armada del Ejército del Aire, del Ministerio de Defensa.

El reclamante manifiesta que el colegio solicitó a los padres el consentimiento para el uso de la herramienta y, aunque **no dio el consentimiento** para su uso, **dieron de alta a sus hijos en las cuentas de Google**. Se impone una **sanción de apercibimiento** por cada una de las infracciones del RGPD, de los artículos 28 y 13.

También en relación con el uso de **Google Suite en centros de enseñanza** se encuentra el **PS/00176/2022 contra Consejería De Educación, Universidades, Cultura Y Deportes Del Gobierno de Canarias**, a raíz de la reclamación recibida contra la Consejería de Educación, Universidades, Cultura y Deportes del Gobierno de Canarias-CEUCD por el uso de la aplicación Google Suite en los colegios.

El reclamante refiere que el IES en el que está matriculado su hijo menor ya implantó el uso de Google Suite durante los cursos 2019/2020 y 2020/2021, sin que solicitaran su consentimiento y dieron de alta a su hijo a pesar de haber desautorizado el tratamiento.

Se sanciona con apercibimiento a la Consejería de Educación, Universidades, Cultura y Deportes del Gobierno de Canarias-CEUCD, por las infracciones d ellos artículos 13, 32 y 6.1 del RGPD.

También en el **ámbito educativo**, podemos destacar el **PS/00516/2022 contra el Centro de Estudios Aeronáuticos S.L.** Este expediente se inició a raíz de una **reclamación por la petición de determinados datos** para poder acceder a la formación de tripulante de cabina de pasajeros. Entre los datos solicitados se encuentran el certificado COVID, un certificado de penales y determinados datos como domicilio, personas con las que se convive o número de cuenta corriente.

Se impone una **sanción de 50.000 euros** por una infracción del artículo 9.2 del RGPD por pedir los datos de salud y el certificado COVID y no existir circunstancia que levante la prohibición del artículo 9 del RGPD; una **multa de 10.000 euros** por una infracción del artículo 6.1 del RGPD por no tener legitimación para pedir datos de salud en un curso de formación y otra de **25.000 euros** por infracción del artículo 6.1 del RGPD por pedir un certificado de penales y finalmente una multa de **5.000 euros** por una infracción del artículo 5.1.c) del RGPD por pedir datos excesivos.

Similar a este caso tendríamos también el **PS/00051/2022 contra la Real Federación Española de Tenis de Mesa** por la **obligación de aportar el certificado de vacunación COVID** para entrar en las instalaciones para la realización de un examen.

La Federación alegó, entre otras cosas, que, para tratar los datos, en base al artículo 6.1 del RGPD, ejerce una misión publica puesto que colabora en las funciones de formación de técnicos que reseña la Ley del Deporte. No se considera que en este caso esté realizando una actuación pública y por eso se impone una **sanción económica** vinculada con la infracción del artículo 9.2 del RGPD con **10.000 euros**, al carecer asimismo de excepción que lo habilite.

Relacionado con **datos de salud**, en el ámbito sanitario hay varios procedimientos reseñables.

Entre ellos, está el **PS/00302/2022, en el que se sanciona al Servicio De Salud De Las Illes Balears** por una vulneración del artículo 13 del RGPD al **no informar debidamente** de las bases de legitimación del Formulario de Control Sanitario (FCS) que debían rellenar los viajeros al entrar en las Islas Baleares en agosto del 2021 con motivo de la COVID-19.

En la resolución del procedimiento, se ha considerado que la obligatoriedad de cumplir con el principio de transparencia dispuesto en el artículo 5.1.a) del RGPD requiere, necesariamente, que, cuando el tratamiento se fundamente en cualquiera de las bases jurídicas previstas en los artículos 6.1.c) y 6.1.e) del RGPD (cumplimiento de una obligación legal o cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento) se indique al ciudadano de manera clara y precisa cuál es la norma jurídica habilitante respecto de dicho tratamiento (en el sentido del artículo 8 de la LOPDGDD).

El **PS/00263/2022 se instruyó contra la Real Federación Española de Balonmano** a partir de una reclamación por la imposición de la **obligación de registrar el certificado de vacunación completo** o en su caso test de antígenos negativo en la plataforma de la Federación. La Federación exigió para poder participar en la competición a los deportistas y staff técnico la obligación de subir a su área privada el certificado oficial de vacunación o un test de antígenos con resultado negativo. **Se sanciona** a la Federación por infracción del artículo 9 del RGPD **con multa de 20.000 euros**. La reclamada basa el tratamiento de datos de salud en las circunstancias que contemplan los artículos 9.2.d), 9.2.i) y 9.2.g), pero no existe ninguna norma que recoja este tratamiento. Por otro lado, ninguna de las medidas para la vuelta a las competiciones de ámbito estatal del protocolo CSD hace referencia al certificado de vacunación, sólo indica que se realizará a los deportistas una prueba de COVID. Se sanciona también a la Federación por una infracción del artículo 13 del RGPD **con multa de 7.000 euros**, porque, aunque la reclamada corrigió las deficiencias de la cláusula informativa durante la tramitación del procedimiento sancionador, la cláusula no estaba completa cuando se recogieron los datos en la temporada 21/22, por no indicarse la finalidad del tratamiento de los datos de salud ni la base jurídica del mismo.

Se sancionó a la **Consejería de Educación de Castilla y León en el PS/00498/2022** por **proporcionar** a un centro educativo **datos de vacunación** de la reclamante y la publicación de dichos datos en un tablón de anuncios.

Las **aplicaciones y servicios de mensajería** como WhatsApp son un medio por el que **pueden difundirse datos personales de forma indebida**, como en el **PS/00270/2023 contra el Sindicato Libre de Transportes o el PS/00494/2022 contra Grupo de**

Seguridad y Control Global, S.L. En ambos se ha sancionado por infracción de los artículos 5.1.f) y 32 del RGPD, fijándose las **multas en 5.000 y 3.000 euros**, respectivamente.

Por infracciones de los mismos artículos del RGPD se resuelve el PS/00452/2022 contra Ilunion Seguridad S.A. En este caso, se sanciona por el envío de dos correos a los trabajadores sin utilizar la opción de copia oculta, CCO, a direcciones personales de los trabajadores, con **multas de 10.000 y 5.000 euros**, respectivamente al tratarse de una gran empresa.

También en el **ámbito laboral**, el PS/00211/2023 sanciona al dueño de un bar por la **publicación del parte médico de baja** de la reclamante en su estado de **WhatsApp**. Dado que los datos personales se han expuesto a terceros se le imputa una infracción del artículo 5.1.f) del RGPD y se propone una sanción de **multa de 2.500 euros** del RGPD. También se imputa una infracción del artículo 32 del RGPD y se propone una sanción de multa de 500 euros.

Por infracción de los artículos 32 y 5.1.f) del RGPD se ha sancionado a Pelayo Mutua de Seguros y Reaseguros a Prima Fija en el PS/00025/2023. En este caso, un agente **facilita a un tercero** un documento con el nombre de la entidad aseguradora en el que constan los **datos personales** de la reclamante (tomadora y asegurada de la póliza), entre ellos de su DNI, de la prima del seguro y de los siniestros que la reclamante había comunicado a la aseguradora durante la vigencia del contrato. Se declaran infracciones de los artículos 32 y 5.1.f) del RGPD con **multas de 20.000 euros y 50.000 euros**, respectivamente.

En el PS/00678/2022, contra Foro Asturias por la **filtración de un documento** en el que aparece la nómina del reclamante, conteniendo sus retribuciones y su número de cuenta corriente. Esta reclamación se recibió originariamente en 2019 pero se inadmitió por falta de pruebas sobre la responsabilidad de la brecha. No obstante, se recibió una nueva reclamación en la que el reclamante adjunta una sentencia civil a su favor, que declara la existencia de un incumplimiento de la normativa de protección de datos por parte del secretario general de un partido político. Además de la pérdida de confidencialidad, la sentencia constata la inexistencia de medidas de seguridad que hubieran impedido la filtración. En la resolución, se declaran igualmente infracciones de los artículos 32 y 5.1.f) del RGPD con **multas de 5.000 euros y 15.000 euros**, respectivamente.

La **Agencia** también ha participado como **autoridad de control** interesada en diversos **procedimientos transfronterizos** en el marco de los mecanismos de cooperación del capítulo VII del RGPD.

Cabe destacar los **procedimientos contra las grandes plataformas tecnológicas**, establecidas en Irlanda, y por tanto en los que la autoridad de este país (la Data Protection Commission, DPC) actúa como autoridad de control principal.

El primero de estos procedimientos se dirigió contra Meta Ireland, por propia iniciativa de la DPC para examinar dos cuestiones. Por una parte, si Meta Ireland actúa legalmente y, en particular, de manera compatible con el artículo 46, apartado 1, del RGPD, al efectuar transferencias de datos personales relativos a personas que se encuentran en la Unión Europea o el Espacio Económico Europeo y que visitan, acceden, utilizan o interactúan de otro modo con productos y servicios proporcionados por Meta Ireland y, por otra parte, qué poder correctivo debe aplicar la DPC, de conformidad con el artículo 58, apartado 2, del RGPD en caso de que se llegue a la conclusión de que Meta Ireland está actuando ilegalmente e infringiendo el artículo 46, apartado 1, del RGPD.

La decisión final adoptada refleja la decisión vinculante adoptada por el Comité Europeo de Protección de Datos (CEPD) de conformidad con el artículo 65, apartado 2, del RGPD, que ordena que se introduzcan cambios en algunas de las posiciones reflejadas en el proyecto de Decisión de la DPC, debido a las objeciones presentadas por varias autoridades al proyecto de decisión, incluyendo la AEPD.

En la decisión final la DPC considera que la legislación estadounidense no ofrece un nivel de protección sustancialmente equivalente al previsto por el Derecho de la UE y que ni las de cláusulas contractuales tipo (CCT) de 2010 ni las de 2021 pueden compensar la protección inadecuada que ofrece la legislación estadounidense. Además, Meta Ireland no dispone de medidas complementarias que compensen la insuficiente protección que ofrece la legislación estadounidense; y no puede acogerse a las excepciones previstas en el artículo 49, apartado 1, del RGPD, al efectuar las transferencias de datos.

En consecuencia, considera que, **al realizar las transferencias de datos, Meta Ireland infringe** el artículo 46, apartado 1, del RGPD.

Por ello, se dicta una orden para **exigir a Meta Ireland que suspenda las transferencias de datos** y para que ajuste sus operaciones de tratamiento al capítulo V del RGPD, poniendo fin al tratamiento ilícito, incluido el almacenamiento, en los Estados Unidos de datos personales de usuarios del EEE transferidos vulnerando el RGPD. Además, se impone, de conformidad con el artículo 58, apartado 2, letra i), del RGPD, una **multa administrativa por un importe de 1200 millones EUR**.

El segundo de estos casos transfronterizos es contra **TikTok Technology Limited**. La investigación en este caso se refiere a dos conjuntos distintos de operaciones de la plataforma TikTok cada una de las cuales constituye un tratamiento de datos personales. El primero estaría relacionado con el **tratamiento de los datos personales de los usuarios menores** en el contexto de la configuración de la plataforma de TikTok. El segundo tipo de tratamiento examinado se refiere al **tratamiento de los datos personales de niños menores de 13 años** en el contexto de la plataforma TikTok, tanto en aplicaciones móviles como en sitios web, en particular en lo que se refiere a la verificación de la edad.

Por último, en lo que respecta al tratamiento de datos personales de personas menores en el contexto de la plataforma TikTok (incluido cualquier tratamiento de este tipo en relación con sitios web o aplicaciones que proporcionan acceso a la plataforma TikTok), la investigación examina si la empresa ha cumplido con sus obligaciones de proporcionar información a los interesados en virtud del artículo 12, apartado 1, letra e), del artículo 13, apartado 2, letra a), del artículo 13, apartado 2, letra b), y del artículo 13, apartado 2, letra f), del RGPD.

En la decisión final adoptada la DPC declara que se han infringido los artículos 5 (1) (c), 5 (1) (f), 24 (1), 25 (1) y 25 (2) del RGPD con relación a la protección de datos desde el diseño y por defecto en lo que respecta al tratamiento de los datos personales de los usuarios menores.

Tras examinar detenidamente las infracciones detectadas en la investigación, la autoridad irlandesa ejercitó los poderes correctores de conformidad con la sección 115 de la Ley de 2018 y el artículo 58, apartado 2, del RGPD, adoptando:

- Una orden con arreglo al artículo 58, apartado 2, letra d), para que TTL ajuste las operaciones de tratamiento a las disposiciones del Reglamento

- Un apercibimiento a con arreglo al artículo 58, apartado 2, letra b), del RGPD; y

- Tres multas administrativas:

  - En relación con la infracción por de los artículos 5 (1) (c) y 25 (1) y (2), **100 millones de euros.**
  - Por lo que se refiere a la infracción de los artículos 5 (1) (f) y 25 (1), **65 millones de euros.**
  - Por lo que se refiere a las infracciones de los artículos 12 (1) y 13 (1) (e), **180 millones de euros.**

En el procedimiento seguido contra **INSTAGRAM**, el denunciante solicita que se investiguen los **mecanismos de consentimiento** de Instagram, medidas para impedir el tratamiento ilícito de datos personales y la imposición de multas.

El proyecto de decisión emitido por la DPC fue objeto de objeciones por parte de varias autoridades de control, entre ellas la AEPD. Dado que la autoridad irlandesa no atendió las objeciones, el caso fue llevado ante el CEPD que adoptó una decisión vinculante.

Tras la Decisión vinculante del Comité, la decisión final adoptada por la autoridad irlandesa incluye las **siguientes medidas correctivas**:

- Se ordena, con arreglo al artículo 58, apartado 2, letra d), del RGPD, que Meta Ireland adecue el tratamiento al RGPD en un plazo de tres meses a partir del día siguiente a la fecha de notificación de la Decisión.

- Se impone una **multa administrativa**, con arreglo a los artículos 58 (2) (i) y 83 del RGPD, a Meta Ireland, por un importe de **180 millones de euros**.

Por último, se inició un procedimiento contra **WHATSAPP INC.,** por una reclamación contra WhatsApp Ireland Ltd., presentada por «NOYB — European Center for Digital Rights» en nombre de un reclamante alemán. A partir de la entrada en vigor del RGPD, los usuarios de WhatsApp no pudieron seguir utilizando el servicio sin aceptar las condiciones de servicio de WhatsApp. La denuncia alega que se trata de un «**consentimiento forzoso**» y que el tratamiento de datos asociado al que los usuarios no podían renunciar, en particular el tratamiento de datos para facilitar la publicidad comportamental y la mejora de los servicios infringía, entre otros, los artículos 5, 6, 7 y 9 del RGPD.

El proyecto de decisión de la DPC fue objeto de varias objeciones pertinentes y motivadas por parte de varias autoridades. Dado que la DPC no siguió las objeciones, el CEPD tuvo que pronunciarse a través de la decisión vinculante.

En la decisión final de la DPC se ordena a WhatsApp que adecue el tratamiento al Reglamento en un plazo de seis meses a partir del día siguiente a la fecha de notificación de la Decisión y adopte las medidas necesarias para que su tratamiento de datos personales a efectos de mejora del servicio y medidas de seguridad (excluido el tratamiento con fines de «seguridad informática», tal como se define en el apartado 90 de la Decisión del artículo 65) («el tratamiento») sea conforme con el artículo 6, apartado 1, del RGPD. Además, se impone una multa administrativa por un importe de 5.5 millones EUR por la infracción del artículo 6, apartado 1, del RGPD.

Estas decisiones transfronterizas pueden ser consultadas en la página web del Comité Europeo de Protección de Datos.

6. Una organización resiliente y en permanente mejora

6.1. Captación de talento y compromiso con el bienestar laboral

La Agencia Española de Protección de Datos cuenta con una Secretaría General, a la que corresponde la prestación de los servicios comunes de la entidad, bajo la inmediata dirección de la Directora de la AEPD.

En 2023, la Relación de Puestos de Trabajo (RPT) de la AEPD fue objeto de varias ampliaciones para adecuar la plantilla a las nuevas funciones a desempeñar por la Agencia, creando en total 41 puestos de trabajo.

Durante 2023 se convocaron y resolvieron cuatro convocatorias de libre designación para cubrir un total de 7 puestos, así como dos concursos específicos y dos concursos generales, en los que se han convocado 28 plazas (17 adjudicadas y 11 en proceso de resolución). Asimismo, se han provisto 16 puestos de trabajo, ya sea en comisión de servicios o en adscripción provisional.

Finalmente, en relación con el resto de las plazas creadas, ya está planificada la convocatoria durante 2024 de los oportunos procesos selectivos.

En este sentido, la AEPD es consciente de la importancia de atraer y retener a los mejores profesionales, con una clara apuesta por el teletrabajo como doble instrumento, de ordenación del trabajo y de conciliación, compatibilizando la garantía del servicio a los intereses generales y el correcto ejercicio de sus competencias, con su compromiso con la igualdad y la corresponsabilidad, estableciendo medidas específicas para los trabajadores que tengan menores a su cargo para poder apoyar una maternidad y paternidad positivas.

Con ello, se alcanza un elevado grado de ocupación de los puestos de la entidad, debiendo destacarse la presencia femenina en los niveles directivos y predirectivos. Antes de la aprobación del Plan de Igualdad de la AEPD en 2020, la Agencia contaba con un 61,54% de hombres frente a un 38,46% de mujeres en dichos puestos. A 31 de diciembre de 2023, dichos porcentajes se sitúan en un 51,45% de hombres frente a un 48,55% de mujeres.

En tan solo 4 años se ha incrementado en 10 puntos la presencia femenina en los niveles directivos y pre directivos de la Agencia.

Durante 2023, la Agencia ha retomado con fuerza las acciones formativas para su personal, con especial atención a las relacionadas con funciones de la AEPD, impartidas por formadores internos en materias tan especializadas como Tecnologías de seguimiento y Cookies, Análisis de Aplicaciones Móviles o Inteligencia Artificial.

Cabe destacar asimismo la creación de un nuevo área de ciberseguridad, profundizando en la detección de riesgos, definición de instrucciones, bastionado de sistemas y segmentación de redes, campañas internas de concienciación, respuesta ante incidentes y avisos de vulnerabilidades, estudio de nuevas soluciones y adopción de las ofertadas por el Centro Criptológico Nacional y los servicios del Centro de Operaciones de Ciberseguridad de la Administración General del Estado (CoCS).

6.2. Avance en digitalización

La AEPD continúa **avanzando en la transformación digital** de sus procesos y servicios para mejorar la calidad, la eficiencia y la satisfacción en su cometido.

La Secretaría General, a través de su departamento de Tecnologías de la Información, ha completado las actuaciones de digitalización y evolución de su infraestructura tecnológica, que se describen a continuación.

En su apuesta por una administración más cercana y centrada en el ciudadano, la Agencia trabaja en **mejorar la experiencia de usuario** de ciudadanos y entidades, que les permita extraer el máximo valor de los servicios públicos digitales.

En este sentido, los aspectos más destacados sobre la sede electrónica han sido los siguientes:

- Ampliación del tamaño de los ficheros adjuntos que se pueden presentar en sede electrónica, permitiendo un máximo de 4 ficheros que alcancen, entre todos, 100 MB, en lugar de los 15 MB que marca el servicio de registro electrónico.

- Simplificación de los requerimientos para la realización de una consulta al servicio de Atención al ciudadano, en su presentación a través de la sede electrónica, con la habilitación del mecanismo de firma no criptográfica (i.e., sin certificado electrónico y previa autenticación del interesado mediante la plataforma Cl@ve), con base en el servicio horizontal de sellado (eUtils).

- Simplificación de la presentación de candidaturas a la convocatoria de los premios anuales de protección de datos, mediante un nuevo formulario específico en la propia sede electrónica.

- Puesta en marcha del Canal de protección del informante, tras la entrada en vigor de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

- Nuevo buzón guiado de reclamaciones, en la rama de Publicidad y comunicación comercial, para facilitar, mediante preguntas dirigidas, la presentación de reclamaciones con las evidencias y requisitos de admisibilidad que señalan los modelos aprobados mediante Resolución de 29 de junio de 2023, de la Dirección de la Agencia Española de Protección de Datos, por la que se aprueban los modelos de presentación de reclamaciones.

- Nueva funcionalidad para la configuración y publicación dinámica de alertas y novedades en la portada de la sede-e, con el fin de informar acerca de incidencias técnicas o intervenciones programadas.

- Automatización de un primer catálogo de pruebas de regresión, para garantizar de manera más eficiente y exhaustiva el correcto funcionamiento de una nueva versión de la sede electrónica con carácter previo a su publicación, y acelerar así la disponibilidad de correcciones y nuevas funcionalidades.

Los **portales web** constituyen por otro lado el **principal medio de información, divulgación y primer punto de contacto** para muchas personas, y que después dirigen el tráfico en su caso a la oficina virtual (o sede electrónica) para completar la comunicación con la AEPD, o los asistentes web de ayuda al cumplimiento normativo que desarrolla la División de Innovación Tecnológica.

En relación con éstos, se puede destacar lo siguiente:

- Rediseño del portal web institucional, aprovechando la actualización tecnológica a la última versión disponible del sistema de gestión de contenidos para adecuar el tema, la plantilla y

la guía de estilos a los requisitos de accesibilidad que marca la normativa y optimizarlo para la navegación desde dispositivos móviles.

- Nuevo sistema de participación en el portal web institucional, permitiendo al visitante valorar en una escala de una a cinco estrellas la calidad de los contenidos, inicialmente en la sección de preguntas frecuentes, permitiendo acompañar de comentarios las puntuaciones inferiores.

- Incorporación en el portal web institucional de un nuevo canal del servicio de atención al ciudadano mediante tecnología conversacional (un «Chatbot») por escrito, atendido por el mismo equipo que responde a las consultas telefónicas.

- Preparación del portal web institucional para habilitar el selector de idioma en todas sus páginas, siguiendo un enfoque similar al del EDPB, en el que conviven contenidos en diferentes idiomas y con una integración con el servicio de traducción automática (eTranslation) de la Comisión Europea.

- Publicación de la fecha de firma en el listado dinámico de las resoluciones de reclamaciones en el portal web institucional, en atención a la demanda percibida desde las redes sociales.

- Nuevas versiones funcionales de los asistentes «Asesora Brecha», «Comunica Brecha», «Evalúa Riesgo», «Gestiona RGPD» y «Valida Cripto», integrando estas tres últimas con la red de distribución de contenidos (o CDN, del inglés Content Delivery Network) para mejorar la escalabilidad y velocidad de carga.

En el ámbito de la **tramitación electrónica de procedimientos administrativos**, y con el objetivo de la actualización tecnológica continua, se ha sustituido la aplicación anterior ("legacy"[1]) para la gestión de las consultas de atención al ciudadano, por un nuevo sistema tramitador que provee, adicionalmente, otras capacidades funcionales encaminadas a mejorar la gestión diaria (por ejemplo, elaboración y edición de documentos desde la propia aplicación, etc.).

Por otra parte, se ha desarrollado una nueva aplicación que aglutina, en una única herramienta, todas las funciones y acciones necesarias para llevar a cabo la **revisión, anonimización y publicación de las reclamaciones e informes jurídicos en el portal web institucional**. La nueva solución ofrece, por consiguiente, mejores facilidades para la realización de esta labor, al tiempo que se introducen mayores garantías mediante controles en el flujo de publicación y mecanismos de detección de coincidencias.

En relación con la **gestión de reclamaciones en materia de protección de datos**, se ha seguido mejorando el sistema informático de tramitación, incorporando nuevas funciones o modificaciones relevantes en las ya existentes. Se ha avanzado, por ejemplo, en la automatización de tareas que pueden realizarse de forma desasistida, para una mayor eficiencia en la gestión del volumen de reclamaciones. Asimismo, la aplicación cuenta con un nuevo buscador genérico de expedientes, actuaciones y documentos con una mayor potencia de búsqueda, basada en palabras claves, que ofrece a la par una interfaz más sencilla y usable. Se ha integrado también el servicio puesto a disposición por la Plataforma de Intermediación de Datos (PID) para la consulta de la titularidad de los bienes inmuebles. Por otro lado, se ha revisado la generación de expedientes ENI para su remisión a la Audiencia Nacional, aplicando una nueva organización de la documentación más adecuada e intuitiva. Por último, se han introducido mejoras

[1] *Se consideran sistemas "legacy" o heredados aquellos que, aunque sustentados en tecnologías o software obsoleto o desactualizado, continúan en uso en la organización por su funcionalidad y cuya sustitución o actualización entraña complejidad.*

en el proceso de composición, edición y generación de los documentos que se elaboran a lo largo de la tramitación de un expediente.

Como herramienta de apoyo a la mejora continua en el ejercicio de sus funciones y la toma de decisiones, **se ha impulsado el desarrollo de un proyecto de cuadro de mandos**, de largo recorrido, que facilite la obtención y representación gráfica de los indicadores relevantes para distintas áreas funcionales y de negocio.

Se ha seguido **colaborando en las iniciativas con el Ministerio de Justicia** para la robotización y automatización de procesos, la utilización de técnicas de inteligencia artificial en la anonimización de documentos y la realización de actos de trámite en remoto.

Por último, en aras de la mejora de la calidad del software de las aplicaciones y servicios, a lo largo del año que se resume, se han dado pasos sustanciales para **adquirir una mayor madurez en los procesos de desarrollo**, con una primera propuesta del flujo de integración continua y herramientas aplicables en cada paso, incluyendo la gestión y automatización de casos de prueba.

Algunas de estas herramientas se han puesto en marcha ya y se han acometido las primeras actuaciones para su adopción en los proyectos de desarrollo.

Internamente, la Agencia ha continuado con la **ejecución de iniciativas de modernización y actualización tecnológica de su infraestructura de sistemas y comunicaciones**, abordando diversos proyectos sustantivos, que han tenido como objetivos la homogeneización, el aseguramiento de la continuidad, la mejora del servicio y el refuerzo de la seguridad.

En el marco de dichos proyectos, se han implementado **mejoras en el ámbito de la arquitectura y configuración de las redes de comunicaciones**; la administración y gestión securizada del acceso, o proyectos de migración de servidores a plataformas tecnológicamente más actualizadas y bastionadas conforme a las guías CCN-STIC. Asimismo, se han incorporado soluciones que ofrecen una monitorización extensiva de los sistemas, servicios y aplicaciones.

De igual modo, se ha puesto el **foco en la mejora de los medios técnicos para una adecuada atención presencial**, la ubicuidad del puesto de trabajo y, en general, la prestación del servicio de soporte y atención al usuario. Así por ejemplo, sobre una nueva solución de gestión ITSM[2] del servicio, se ha acometido la definición y programación de un catálogo de incidencias y peticiones tipo, flujos y automatizaciones que, ajustadas a las necesidades de la Agencia, buscan lograr una mayor eficiencia y agilidad en la resolución de las peticiones de servicio.

Asimismo, a lo largo del año objeto de esta Memoria, se ha realizado un **esfuerzo especial en el soporte audiovisual a la celebración y retransmisión de eventos en directo**, con un equipamiento mejorado, para acercar su contenido a cualquier persona interesada.

Por otra parte, en el ámbito de la **ciberseguridad**, se ha constituido una nueva área específica dedicada a este propósito, lo que ha permitido profundizar en la detección de riesgos, definición de instrucciones, o acciones de carácter preventivo frente a posibles incidentes o vulnerabilidades y, en general, con la finalidad de la mejora de la seguridad de los sistemas y servicios.

En este sentido, se ha abordado la elaboración de un **Plan de Tratamiento de Riesgos** orientado al cumplimiento de las medidas del ENS[3]. Asimismo, se han adoptado diversos servicios de prevención y detección puestos a disposición por el Centro

[2] *ITSM: IT Service Management, o gestión de servicios de Tecnologías de la Información.*

[3] *ENS, o Esquema Nacional de Seguridad, definido mediante el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.*

Criptológico Nacional (CCN) y el Centro de Operaciones de Ciberseguridad de la AGE (COCS). E implantado la política establecida por la Secretaría General de Administración Digital (SGAD) para la securización de los dispositivos móviles.

De igual modo, se ha continuado avanzando, con mayor impulso, en la aplicación de **medidas para la protección perimetral**, así como el bastionado de dispositivos y sistemas.

Finalmente, orientado al personal, se ha puesto en marcha un **programa de formación y concienciación en ciberseguridad** que, dividido en módulos y ejercicios prácticos de corta duración, los empleados pueden realizar a su ritmo y de forma interactiva.

6.3. Eficiencia en la gestión de los recursos

La gestión económica y financiera de un organismo público como la AEPD exige la planificación y la correcta administración de los recursos de la organización.

En 2023 el presupuesto inicial de gastos de la AEPD ha ascendido a 18.750.730 euros, un 11,1% superior al de 2022, para hacer frente a las necesidades de creación de nuevos puestos de trabajo para adecuar la estructura de la plantilla a las funciones de la Agencia.

Como en anteriores ejercicios, **el nivel de ejecución presupuestaria se ha mantenido alto**, por encima del 90%, concretamente, en un 93,2% para el año 2023. El remanente se ha producido fundamentalmente en el capítulo 1 "Gastos de Personal", por el decalaje existente entre la creación de las plazas y su cobertura tras los correspondientes procesos selectivos.

Por lo que respecta a la ejecución de su presupuesto de ingresos, a 31 de diciembre de 2023 **el importe de los derechos reconocidos brutos ha ascendido a 31.778.046,02 euros**, de los que un 95,3% (30.278.978,16 euros) corresponden a derechos reconocidos por sanciones. Por su parte, **el importe de los derechos reconocidos netos se ha situado en 30.110.633,52 euros**, una vez contabilizadas las insolvencias o anulaciones producidas durante el año.

La **recaudación total** en el ejercicio corriente 2023 asciende a **15.234.956,45 euros**, de los que 13.735.888,59 euros corresponden a sanciones (un 90,1%).

La **recaudación neta de sanciones**, en el ejercicio corriente 2023, ha sido de **13.656.315,03 euros**, una vez contabilizadas las devoluciones de sanciones.

Teniendo en cuenta la recaudación de derechos reconocidos de ejercicios cerrados durante el ejercicio corriente, la recaudación total de sanciones en el ejercicio de 2023 se ha situado en 14.868.210,64 euros, y la recaudación neta total de sanciones ha sido de 14.788.637,08 euros, una vez contabilizadas las devoluciones de ingresos como consecuencia de la estimación parcial o total de recursos.

Finalmente, como novedad durante 2023, **cabe destacar** que los **importes depositados** en las cuentas corrientes abiertas a nombre de la AEPD **han generado ingresos financieros por importe de 1.452.202,24 euros**.

7. La necesaria cooperación institucional

7.1. Consejo Consultivo

El Consejo Consultivo de la Agencia, órgano colegiado de asesoramiento de la Dirección, se reunió en 2023, en dos ocasiones.

En la reunión del 11 de julio se puso de manifiesto el gran incremento de actividad de la AEPD en todas sus subdirecciones y divisiones, **destacando el importante aumento en cantidad y complejidad de reclamaciones recibidas, un 33,3% que en el mismo semestre del ejercicio anterior;** así como los pasos dados por la Agencia en la protección de la privacidad de los menores en internet, iniciativa valorada muy positivamente por los miembros del Consejo.

En la reunión del 11 de diciembre, además de exponer la actividad de las distintas unidades, **se designaron los trabajos premiados** en la convocatoria de los premios de la AEPD de 2023.

Ambas reuniones se celebraron en formato mixto, aunando la presencialidad de algunos de sus miembros y facilitando la intervención telemática de los que no se desplazaron hasta nuestra sede, aprovechando las facilidades introducidas en la Ley 40/2015. de 1 de octubre, de Régimen Jurídico del Sector Público, que prevén la posibilidad de que las sesiones se celebren a distancia, las convocatorias se remitan por medios electrónicos y que se puedan grabar las sesiones.

7.2. Autoridades autonómicas

En el mes de mayo de 2023 se celebró una reunión con participación 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 en las que se trataron temas relacionados con las implicaciones en protección de datos de ChatGPT, se analizaron las implicaciones de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción desde el punto de vista de la normativa de protección de datos, el procedimiento para la procedimiento para la declaración de apercibimientos tras la reforma LOPDGDD, las iniciativas para la evaluación de impacto en protección de datos en el proceso normativo, la experiencia práctica de las autoridades de control tras la recepción de notificaciones de brecha de seguridad, las orientaciones sobre cookies y analítica web en portales de las administraciones públicas, las orientaciones preliminares para la implementación de protección de datos desde el diseño en Espacio de Datos.

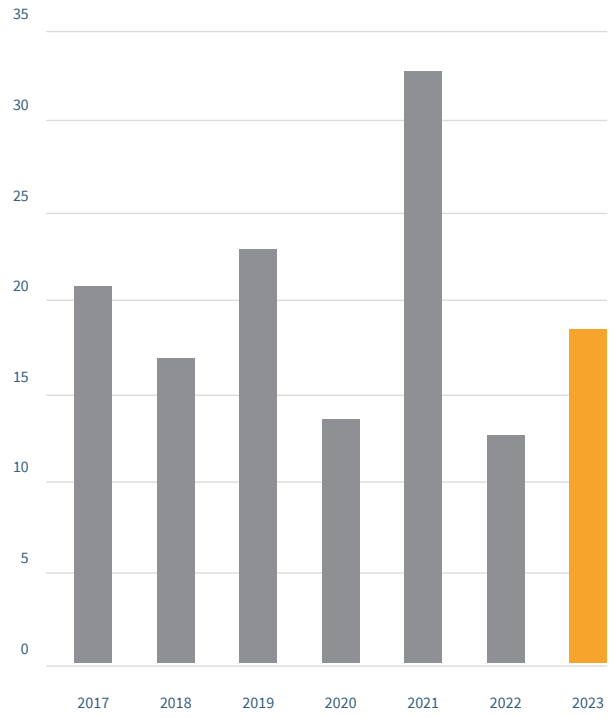
Asimismo, se informó sobre el de circular de la AEPD del artículo 66.1.b) de la LGT relativo al régimen jurídico de la publicidad telefónica y sobre las actividades del Comité Europeo de Protección de Datos.

Finalmente se intercambiaron criterios sobre las reuniones de grupo de trabajo de las Autoridades de Protección de Datos.

7.3. Relaciones con el Defensor del Pueblo

Durante el presente año 2023 **se han tramitado un total de 18 asuntos**, frente a los 12 del pasado año.

Evolución quejas DP



Respecto a los **motivos** que han llevado a los ciudadanos a dirigirse a la AEPD mediante este cauce, el principal de ellos, en siete ocasiones, ha sido el relativo a **la queja por la falta de respuesta en plazo de la resolución de las correspondientes reclamaciones o solicitudes de información formuladas ante la Agencia**. Junto a las ya mencionadas solicitudes de información sobre las medidas adoptadas por las administraciones públicas en cumplimiento de las resoluciones de la Agencia, **destaca la solicitud de información sobre las medidas adoptadas**.

En un caso, se reitera la solicitud de información del Defensor del Pueblo sobre las razones que justifican la cesión de datos por parte de la Dirección General de la Policía y de la Dirección General de Política Interior a la Tesorería General de la Seguridad Social. Y por parte de la Dirección General de la Política Interior a la Policía, indicando la fecha de remisión de la misma.

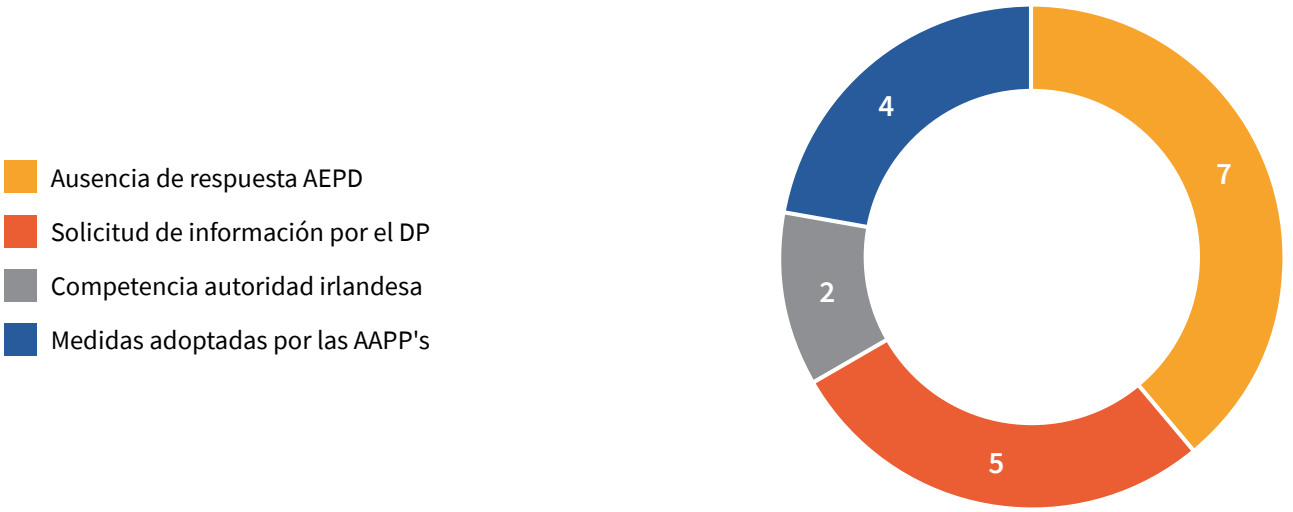
En dos casos, se ha solicitado información sobre reclamaciones respecto de las que en el marco del Reglamento (UE) 2016/679, General de Protección de Datos, la AEPD no era la autoridad competente para su tramitación, habiendo sido remitidas a la autoridad de protección de datos de Irlanda, como autoridad principal, circunstancia notificada a los reclamantes en ambos casos.

Finalmente, en un caso se ha recibido un recordatorio del Defensor del Pueblo sobre el cumplimiento de los deberes legales de resolución en plazo de las reclamaciones y recursos presentados ante la Agencia.

Este escrito fue respondido argumentando detalladamente sobre la carga de trabajo de la Agencia por el crecimiento exponencial del número de reclamaciones presentadas, la complejidad e incremento de los procedimientos transfronterizos en los que ha intervenido y los requisitos de cualificación jurídica y tecnológica de las reclamaciones planteadas que, adicionalmente, inciden en la cualificación de los profesionales que se incorporan a la Agencia, haciendo necesario un periodo de adaptación, e informando sobre cómo se han puesto de manifiesto estas circunstancias en las comparecencias de la Directora en el Congreso de los Diputados.

El escrito finaliza haciendo referencia a las medidas tecnológicas dirigidas a conseguir una mayor automatización de los procedimientos que permitan su simplificación y agilización, así como a las iniciativas de la Agencia para la modificación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que se han tramitado para obtener una mayor eficiencia y eficacia, en particular, promoviendo procedimientos de mediación para la tramitación de las reclamaciones conforme a las previsiones del Reglamento General de Protección de Datos (RGPD).

Motivos de queja



8. Una autoridad activa en el panorama internacional

8.1 Unión Europea

8.1.1 Comité Europeo de Protección de Datos (CEPD)

La actividad del Comité Europeo de Protección de Datos ha sido intensa a lo largo del año 2023. La Agencia ha participado de forma muy activa en estos trabajos. La Agencia está representada en todos los subgrupos de expertos del Comité Europeo y actúa como coordinador de uno de sus subgrupos, el denominado su subgrupo de Cumplimiento, Salud y Gobierno Electrónico ("Compliance, Health and eGovernment")

Finalmente, la AEPD ha participado como **redactor principal o corredactor** en varios de los documentos que el Comité ha publicado en 2023.

A fin de cumplir con su misión de garantizar la aplicación coherente en toda la Unión Europea del RGPD, el CEPD ha continuado con su labor de elaboración y aprobación Directrices que clarifiquen y proporcionen orientación sobre distintos aspectos de la aplicación del Reglamento. **Durante el año 2023 CEPD ha aprobado las siguientes Directrices:**

Directrices 2/2023: Sobre el alcance técnico del Art. 5(3) de la Directiva sobre la privacidad y las comunicaciones electrónicas (Directiva 2002/58/EC, ePrivacy)

El objetivo de estas directrices es realizar un análisis técnico sobre el ámbito de aplicación del artículo 5 apartado 3 de la Directiva europea

sobre la privacidad y las comunicaciones electrónicas. En concreto pretenden aclarar qué se entiende por almacenamiento o acceso a información almacenada en el equipo terminal de un suscriptor o usuario. Las directrices no abordan las circunstancias bajo las cuáles una operación de tratamiento puede estar dentro de las excepciones del requisito de consentimiento previstas por la Directiva.

La aparición de nuevos métodos de seguimiento para reemplazar las herramientas de seguimiento existentes (por ejemplo, las cookies, debido a la interrupción del soporte a las cookies de terceros) y la creación de nuevos modelos de negocio se ha convertido en una preocupación crítica en materia de protección de datos. Si bien la aplicabilidad del artículo 5 apartado 3 de la Directiva sobre privacidad electrónica está claramente establecida para algunas tecnologías de seguimiento, como por ejemplo las cookies, es necesario eliminar las ambigüedades relacionadas con la aplicación de dicha disposición a las herramientas de seguimiento emergentes, como pueden ser los píxeles y urls de seguimiento, el seguimiento basado en la dirección IP, el procesamiento local y los identificadores únicos entre otras.

Estas **directrices 2/2023** han sido sometidas a consulta pública en la versión disponible en el siguiente **enlace**, estando pendiente de publicación la versión definitiva.

Directrices 1/2023: Sobre el artículo 37 de la Directiva policial (680/2016)

Aportan garantías adicionales para Transferencias Internacionales en materia de cooperación policial y judicial a terceros estados en ausencia de una decisión de la Comisión Europea. En esta se ha llegado a un **acuerdo sobre dos puntos**:

a. En el caso del art. 37 a) que permite que el responsable evalúe las garantías concretas a implantar a una transferencia concreta, las guías sugieren que es preferible evitar esa evaluación y que el responsable acuda a las herramientas de transferencia del título V del RGPD.

b. En el caso de que el responsable evalúe las garantías que ya incorpora la transferencia en un instrumento jurídicamente vinculante son adecuadas, deberá considerar el riesgo para los derechos fundamentales del afectado en vista de la protección de datos del tercer Estado en cuestión y ponderar el interés legítimo de otras personas que puedan verse afectadas.

Estas **directrices 1/2023** han sido sometidas a consulta pública en la versión disponible en el **siguiente enlace**, estando pendiente aprobación y publicación para la versión definitiva.

Directrices 9/2022: Sobre las notificaciones de violaciones de seguridad bajo el RGPD

Debido a ciertas dudas sobre las notificaciones de brechas de seguridad, el CEPD decidió modificar las Directrices publicadas por el antiguo Grupo de Trabajo del Artículo 29. La modificación se limita al párrafo 73 y aclara que la mera presencia en algún país de la Unión Europea de un representante de un responsable que esté fuera de la Unión no significa que se pueda utilizar automáticamente el sistema de ventanilla única. En estos casos, las brechas de seguridad deberán notificarse a todas las autoridades de protección de datos afectadas.

Estas **directrices 9/2022** fueron sometidas a consulta pública tras lo cual se aprobaron en su versión definitiva disponible en el **siguiente enlace**.

Directrices 8/2022: Sobre la identificación de la autoridad principal para un responsable o encargado

Las directrices tienen por objeto clarificar el concepto de establecimiento principal en el contexto de responsables conjuntos teniendo en cuenta las Directrices 7/2020 del Comité Europeo de Protección de Datos sobre el concepto de responsable y encargado del tratamiento.

Las directrices abordan los conceptos de tratamiento transfronterizo, aportan criterios para realizar un test que permita dilucidar si dicho tratamiento "afecta sustancialmente", según la definición de tratamiento transfronterizo recogida en el artículo 4 del RGPD, a interesados en más de un Estado Miembro y analizan el concepto de establecimiento principal.

A partir de los conceptos anteriores, se proporciona un procedimiento para identificar la autoridad de supervisión principal en diferentes escenarios: establecimiento principal distinto del emplazamiento de la central administrativa en el Espacio Económico Europeo, grupo de empresas, responsables conjuntos, otros casos límites, etc., aportándose ejemplos en cada escenario para una mejor comprensión.

Estas **directrices 8/2022** fueron sometidas a consulta pública tras lo cual se aprobaron en su versión definitiva disponible en el **siguiente enlace**.

Directrices 7/2022: Sobre la certificación como una herramienta para transferencias internacionales

El RGPD exige en su artículo 46 que los exportadores de datos establezcan garantías adecuadas para las transferencias de datos personales a terceros países u organizaciones internacionales. Entre las garantías adecuadas previstas en el artículo 46 del RGPD se encuentra la certificación, tal y como la desarrolla el artículo 42.
Estas directrices proporcionan orientaciones sobre cómo debe de emplearse la certificación para que ofrezca las garantías adecuadas exigidas en las transferencias internacionales.

Para ello, las directrices se estructuran en cuatro secciones que abordan, entre otros, el proceso de certificación, la acreditación de los organismos de certificación, los criterios de valoración de la normativa del país importador, las obligaciones generales de los exportadores e importadores, las normas para las transferencias posteriores, los mecanismos de reparación y ejecución, las acciones para situaciones en las que la legislación y las prácticas nacionales impidan el cumplimiento de los compromisos asumidos como parte de la certificación y las solicitudes para el acceso a los datos por parte de las autoridades de terceros países, los compromisos vinculantes entre los responsables y encargados no sujetos al RGPD pero adheridos al certificado mediante contrato u otro instrumento vinculante para cumplir las salvaguardas apropiadas proporcionadas por el mecanismo de certificación.

Además de las citadas cuatro secciones, se incluye un anexo con ejemplos de medidas suplementarias en línea con las recogidas en el anexo II de las Recomendaciones 01/2020, sobre medidas que complementan las herramientas de transferencia para garantizar el cumplimiento del nivel de protección de datos personales de la UE.

Estas **directrices 7/2022** fueron sometidas a consulta pública tras lo cual se aprobaron en su versión definitiva disponible en el **siguiente enlace**.

Directrices 5/2022: Sobre el uso de tecnologías de reconocimiento facial en el ámbito policial

El objetivo de estas directrices es proporcionar una serie de pautas para alinear al RGPD los tratamientos de reconocimiento facial en el ámbito de la cooperación policial.

La guía señala que las autoridades policiales y judiciales usan cada vez más tecnologías de reconocimiento facial para identificar a personas a partir de fotografías o vídeos con diferentes finalidades y con el apoyo de otras tecnologías adicionales tales como la inteligencia artificial, el "machine learning" o el "big data".

Entre las finalidades, se encuentran el tratamiento de listas de sospechosos o la monitorización de los movimientos de las personas en espacios públicos. Estos tratamientos a gran escala pueden afectar a derechos fundamentales como el derecho a la privacidad y producir discriminación e incluso falso resultados.

La guía establece que toda limitación al ejercicio de los derechos y libertades fundamentales debe contar con una base legal y respetar la esencia de esos derechos y libertades. El fundamento jurídico debe ser suficientemente claro en sus términos para dar a los ciudadanos una indicación adecuada de las condiciones y circunstancias en las que las autoridades están facultadas para recurrir a cualquier medida de recopilación de datos y vigilancia secreta, por lo que, a juicio del Comité Europeo de Protección de Datos, una mera transposición al derecho nacional de la cláusula general contenida en el artículo 10 de la Directiva (UE) 2016/680 (directiva LED) no sería válida al carecer de la precisión y previsibilidad necesaria en la limitación de los derechos y libertades fundamentales.

La guía apuesta por una prohibición del uso de estas tecnologías en espacios públicos y aboga por el respeto de los principios de finalidad y proporcionalidad de los tratamientos de datos en uso de estas. Además, las medidas legislativas destinadas a implantar su uso deben ser adecuadas para alcanzar los objetivos legítimos perseguidos por la legislación en cuestión. Un objetivo de interés general, por fundamental que sea, no puede en sí mismo, justificar una limitación a un derecho fundamental. Las medidas legislativas deben diferenciar e identificar a las personas que son objeto de ellas a la luz del objetivo concreto, por ejemplo, la lucha contra delitos graves específicos.

Estas **directrices 5/2022** fueron sometidas a consulta pública tras lo cual se aprobaron en su versión definitiva disponible en el **siguiente enlace**.

Directrices 4/2022: Sobre el cálculo de multas administrativas bajo e RGPD

El objetivo de estas directrices es proporcionar una serie de pautas a las autoridades de supervisión del RGPD para el cálculo del importe de las multas relativas a infracciones al RGPD, con el fin de armonizar dichos importes.

Estas directrices complementan unas directrices anteriores del Comité (sobre la aplicación y el establecimiento de multas administrativas en el Reglamento, WP253, respaldadas por el Plenario de 25 de mayo de 2018) y cuya aplicación práctica había puesto de manifiesto sus carencias.

Las nuevas directrices pretenden además de armonizar la metodología a seguir para el cálculo de los importes de las multas, pretende incrementar la claridad y transparencia en este tipo de operaciones, así como garantizar la aplicación y cumplimiento del Reglamento.

Este documento especifica lo dispuesto por el artículo 83 del Reglamento, que establece una serie de condiciones generales para la imposición de multas. Entre otras cosas, este artículo dispone que cada autoridad garantizará que las multas sean efectivas, proporcionadas y disuasorias.

También establece una serie de criterios a tener en cuenta por las autoridades de control al decidir la imposición de multas y su cuantía en cada caso individual.

En cualquier caso, es necesario tener siempre en cuenta que las reglas generales que contienen estas directrices se entienden sin perjuicio de las circunstancias específicas y concretas de cada expediente.

Estas **directrices 4/2022** fueron sometidas a consulta pública tras lo cual se aprobaron en su versión definitiva disponible en el **siguiente enlace**.

Directrices 3/2022: Sobre los patrones engañosos en las interfaces de las redes sociales: como reconocerlos y evitarlos

El objetivo de estas directrices es ofrecer recomendaciones prácticas a los diseñadores y usuarios de las plataformas de redes sociales sobre cómo evaluar y evitar los llamados "patrones engañosos" en las interfaces de las redes sociales que infringen los requisitos del RGPD.

El documento incluye una lista de patrones engañosos y mejores prácticas, así como los casos de uso, aunque esta lista no es exhaustiva. Los proveedores de redes sociales siguen siendo responsables de garantizar el cumplimiento del RGPD de sus plataformas.

Estas **directrices 3/2022** fueron sometidas a consulta pública tras lo cual se aprobaron en su versión definitiva disponible en el **siguiente enlace**.

Directrices 1/2022: Sobre los derechos de los afectados – el derecho de acceso

Con el objetivo de realizar unas directrices sobre los derechos del afectado bajo el RGPD, se ha comenzado por el derecho de acceso abordado en estas directrices.

El objetivo general del derecho de acceso es proporcionar a las personas información suficiente, transparente y fácilmente accesible sobre el tratamiento de sus datos personales para que puedan conocer y verificar la legalidad del tratamiento y la exactitud de los datos tratados. Con ello, se facilita que el afectado pueda ejercer otros derechos como el de supresión o el de rectificación si bien el ejercicio del derecho de acceso no es un requisito previo para el ejercicio de otros derechos.

Las directrices abordan aspectos tales como la no necesidad de justificación por parte del interesado a la hora de ejercer este derecho, el ámbito del ejercicio de este derecho especialmente cuando afecta a derechos de terceros, la información adicional que debe contener la respuesta al derecho de acceso aparte de los propios datos personales del interesado, así como el formato y la vía por la que el responsable del tratamiento debe de facilitar el derecho con especial consideración cuando el volumen de información a proporcionar sea grande.

También se abordan en las directrices los casos en los que el responsable puede rechazar el ejercicio del derecho, así como aquellos supuestos en los que el responsable de tratamiento puede exigir el pago del coste de dicho ejercicio, teniendo en cuenta que, como regla general, el derecho debe ser gratuito.

Estas **directrices 1/2022** fueron sometidas a consulta pública tras lo cual se aprobaron en su versión definitiva disponible en el **siguiente enlace**.

Directrices 5/2021: Sobre la relación entre la aplicación del artículo 3 y las previsiones sobre transferencias internacionales del Capítulo V del RGPD

Estas directrices son una consecuencia de las adoptadas anteriormente sobre ámbito territorial del RGPD (Directrices 3/2018).

En el proceso de elaboración de aquellas directrices, se planteó la duda sobre la consideración que debería darse a las comunicaciones de datos desde encargados situados en la UE y responsables no establecidos en ella cuando esas comunicaciones se producían en el marco de tratamientos de datos sometidos al RGPD en virtud de su artículo 3.2. Varias delegaciones sostenían que, en la medida en que los datos abandonan la UE existiría una transferencia internacional, mientras que, para otras, el hecho de que los datos no salieran del ámbito de protección del RGPD suponía que no podía hablarse de transferencia internacional.

Esta duda, unida al hecho de que el RGPD no contiene una definición de lo que se debe entender por "transferencia internacional de datos", ha llevado a la elaboración de estas presentes directrices.

Para el Comité, **existe una transferencia internacional cuando** se dan los tres siguientes requisitos:

- El responsable o el encargado (exportador) está sujeto al RGPD para el tratamiento en cuestión.
- El exportador comunique mediante el envío o haga por cualquier otra forma que los datos personales, sujetos a este tratamiento,

pueden quedar a disposición de cualquier otro responsable, corresponsable o encargado (importador).

- El importador se encuentre en un tercer país o en una Organización Internacional, independientemente de que al importador le resulte o no de aplicación el RGPD respecto al tratamiento en cuestión de acuerdo con el art.3 del RGPD.
- Como puede observarse, en esta definición de transferencia se incluye ya la respuesta a la controversia sobre la aplicación o no del concepto de transferencia internacional para los tratamientos sujetos al RGPD en virtud del art. 3.2, ya que, según el tercero de los requisitos, el hecho de que el importador se encuentre en un tercer país determina la existencia de transferencia con independencia del régimen al que esté sujeto el tratamiento en que se enmarca.

Otros **elementos de interés** en las directrices son:

- No se considera transferencia en caso de que un responsable en un tercer país recoge datos personales directamente de un interesado en la UE, dado que no hay "exportador"
- No se considera transferencia en caso de que un empleado de un responsable en la UE viaja a un país tercero por razones profesionales y accede a los datos contenidos en los registros del responsable, dado que no existiría un "importador" distinto del propio responsable para el que el empleado trabaja.

Estas **directrices 5/2021** fueron sometidas a consulta pública tras lo cual se aprobaron en su versión definitiva disponible en el **siguiente enlace**.

Directrices 3/2021: Sobre la aplicación del artículo 65.1.a del RGPD

El Capítulo VII del RGPD recoge los mecanismos de cooperación y coherencia entre las autoridades de control que se aplican a los casos de tratamientos transfronterizos. El artículo 60 fija el procedimiento a seguir para la resolución de dichos casos, mediante una decisión final que ha de ser consensuada por unanimidad entre todas las autoridades de control participantes en el caso. Cuando la unanimidad no sea posible, el RGPD prevé el mecanismo de coherencia establecido en el artículo 65.1.a), que otorga al CEPD la capacidad de dictar una decisión de carácter vinculante para todas las autoridades de control participantes en el caso.

Al objeto de establecer un procedimiento para este mecanismo de resolución de conflictos, el Comité ha elaborado unas directrices en las que se establecen determinados conceptos y se identifican los pasos a seguir cuando se aplica este procedimiento.

Estas directrices están estrechamente relacionadas tanto con las que se están elaborando sobre el mecanismo de cooperación del artículo 60 RGPD, a las que se alude posteriormente, como con las aprobadas en 2020 sobre la noción de Objeción Relevante y Motivada.

Dentro de los criterios que se establecen en las directrices sobre el artículo 65 son especialmente destacables las secciones sobre los límites y contenidos de las decisiones que puede adoptar el Comité y sobre la implementación del "derecho a ser oído" ante el Comité para las partes interesadas que puedan verse afectadas por la decisión del Comité

Estas **directrices 3/2021** fueron sometidas a consulta pública tras lo cual se aprobaron en su versión definitiva disponible en el **siguiente enlace**.

DICTÁMENES

Dictamen 5/2023, sobre la propuesta de decisión de adecuación del marco de privacidad UE-US (DPF)

El 13 de diciembre de 2022, la Comisión Europea publicó un proyecto de Decisión de adecuación sobre el nuevo esquema acordado con el gobierno de EEUU para los intercambios transatlánticos de datos personales denominado Marco de Privacidad de Datos UE-US. (DPF, por sus siglas en inglés), que pretende sustituir al anterior esquema denominado Escudo de Privacidad o Privacy Shield invalidado por el Tribunal de Justicia de la Unión Europea (TJUE) el 16 de julio de 2020, en el asunto Schrems II.

De conformidad con el artículo 70.1.s, del RGPD, la Comisión solicitó el dictamen del Comité Europeo de Protección de Datos (CEPD) sobre el proyecto de Decisión.

El CEPD en su dictamen evaluó la adecuación del nivel de protección concedido en los EEUU, sobre la base del examen del proyecto de Decisión, cubriendo tanto los aspectos comerciales como el acceso y el uso de los datos personales transferidos desde la UE por las autoridades públicas de los Estados Unidos.

Para ello, el CEPD tuvo en cuenta el marco jurídico aplicable de la UE en materia de protección de datos establecido en el RGPD, así como los derechos fundamentales a la vida privada y a la protección de datos consagrados en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 8 del Convenio Europeo de Derechos Humanos. También examinó la aplicación del derecho a una defensa efectiva y a un juicio imparcial establecido en el Artículo 47 de la Carta, así como la jurisprudencia del TJUE en materia de protección de los derechos fundamentales.

Finalmente, el CEPD aprobó, con fecha 28 de febrero de 2023, su dictamen 5/2023. Por su parte, la Comisión Europea, tras recoger parte de las recomendaciones contenidas en el dictamen anterior, adoptó, con fecha de 10 de julio de 2023, la decisión de adecuación del nuevo marco de privacidad UE-US. Este marco va a ser monitorizado periódicamente por la Comisión en colaboración con el CEPD.

Este **dictamen 5/2023** del CEPD se encuentra disponible en el **siguiente enlace**.

Dictamen conjunto EDPB-EDPS 1/2023, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas de procedimiento adicionales relativas a la aplicación del RGPD

La Comisión Europea (CE) publicó el 04/07/23 una propuesta de Reglamento para establecer normas procedimentales adicionales relativas a la ejecución del RGPD y circunscrita a los tratamientos transfronterizos. Esta propuesta, pretende acordar reglas para la tramitación de reclamaciones, así como para la realización de investigaciones por parte de las autoridades de supervisión.

De manera conjunta, el CEPD junto con el Supervisor Europeo de Protección de Datos (EDPS, por sus siglas en inglés), aprobaron dicho dictamen en el que ambos organismos acogen favorablemente la propuesta de la Comisión, dirigida a fortalecer el cumplimiento efectivo de las disposiciones del RGPD. También señalan que su temprana adopción es de capital importancia para continuar mejorando la eficiencia y consistencia del RGPD.

Este dictamen conjunto es por tanto una referencia a tener en cuenta en las negociaciones que están teniendo lugar para aprobar este nuevo Reglamento, ya que ha sido adoptado por los organismos competentes en materia de protección de datos en el seno de la UE.

Este dictamen conjunto **EDPB-EDPS 1/2023** se encuentra disponible en el **siguiente enlace**.

Dictamen conjunto EDPB-EDPS 2/2023, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo para el establecimiento del euro digital

El Banco Central Europeo (BCE) publicó un informe sobre el euro digital el 20 de octubre de 2020, cuya posible emisión es prerrogativa exclusiva del BCE. Posteriormente, El 28 de junio de 2023, la Comisión Europea propuso un paquete legislativo sobre un euro digital, que incluía una propuesta por la que se establece el marco jurídico para un posible euro digital y consultó formalmente al SEPD y al CEPD al objeto de que emitieran una opinión conjunta sobre dicha propuesta.

El CEPD y el SEPD valoran muy positivamente determinados aspectos de la propuesta, como por ejemplo que los usuarios siempre tengan la opción de pagar en euros digitales o en efectivo, que el euro digital no sea «dinero programable» y que la propuesta tenga por objeto proporcionar un alto nivel de privacidad y protección de datos para el euro digital y, en particular, mediante la introducción de una «modalidad fuera de línea», para minimizar el tratamiento de datos personales en relación con el euro digital, así como para integrar la protección de datos desde el diseño y por defecto.

Sin embargo, el CEPD y el SEPD llaman la atención de los colegisladores sobre una serie de posibles riesgos para la protección de datos personales que, si no se abordan en la propuesta, podrían llegar socavar la confianza de los ciudadanos en el futuro euro digital y, en última instancia, su aceptación social. Entre posibles riesgos se destacan los relativos al establecimiento de identificadores únicos, los mecanismos para la detección del fraude, la seudonimización de las transacciones entre el BCE y los bancos centrales nacionales, las bases legales aplicables y las categorías de datos personales que deben tratar los diferentes agentes implicados, la relación con la lucha contra el blanqueo del dinero y la financiación del terrorismo, entre otros.

Este dictamen **conjunto EDPB-EDPS 2/2023** se encuentra disponible en el **siguiente enlace**.

Dictámenes sobre Reglas Corporativas Vinculantes (BCR)

El RGPD prevé en su artículo 46.1 que, en ausencia de decisión de adecuación según el artículo 45.3 del RGPD, un responsable o encargado puede transferir datos personales a terceros países u organizaciones internacionales solo si el responsable o encargado del tratamiento hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

Un grupo de empresas dedicadas a una actividad económica conjunta puede proporcionar tales garantías mediante el uso de BCR legalmente vinculantes, que confieren expresamente derechos exigibles a los interesados y cumplen una serie de requisitos (artículo 46 del RGPD). La implementación y adopción de BCR por parte de un grupo de empresas tiene como objetivo proporcionar garantías que se aplican de manera uniforme en todos los terceros países y, en consecuencia, independientemente del nivel de protección garantizado en cada tercer país.

Las BCR están sujetas a la aprobación de la autoridad de supervisión competente, de acuerdo con el mecanismo de consistencia establecido en el artículo 63 y 64.1 del RGPD que deben de comprobar que dichas BCR satisfacen las condiciones establecidas en el artículo 47, junto con los criterios establecidos por el CEPD en las directrices establecidas al efecto WP256 rev.01 del GT 29 y adoptadas por el CEPD)

Durante el año 2023 recibieron un dictamen favorable un total de veintisiete BCR presentadas por los siguientes países: Holanda, Dinamarca, Alemania, Francia, Rumania, Bélgica, Irlanda, España e Italia.

Estos documentos sobre **Reglas Corporativas Vinculantes** pueden ser accedidos en el **enlace**.

Dictámenes sobre los requisitos de acreditación de órganos de supervisión de códigos de conducta y entidades de certificación

El RGPD establece que los códigos de conducta deben contar con un órgano de supervisión que vigile el cumplimiento del código por parte de los responsables adheridos al mismo. Este órgano debe acreditarse por la autoridad nacional siguiendo unos requisitos de acreditación, que deben ser presentados al CEPD para su aprobación. Durante 2023, se presentaron un total de cuatro requisitos de acreditación presentados por las autoridades de Suecia, Croacia, Rumania y Letonia que han recibido un dictamen favorable.

De manera similar, antes de aprobar un mecanismo de certificación de acuerdo con el art. 42 del RGPD, es necesario establecer los requisitos de acreditación de las entidades de certificación que se dedicarán a emitir los certificados. Estos requisitos pueden ser elaborados por la propia autoridad o, si el organismo que se encarga de acreditar es el órgano de acreditación nacional (NAB), se deberán establecer requisitos adicionales a la norma ISO 17065. En cualquier caso, los requisitos deben aprobarse por el CEPD mediante dictamen. Durante 2023, se presentaron un total de cinco requisitos de acreditación presentados por las autoridades de Eslovenia, Luxemburgo, Croacia, Chipre y Malta que recibieron un dictamen favorable.

Puede **acceder a estos documentos** a través del **enlace**.

Dictámenes sobre esquemas de certificación

El RGPD prevé que algunos tratamientos puedan someterse a certificación para ayudar a demostrar que se realizan con seguridad y cumpliendo con el derecho fundamental a la protección de datos. Las entidades pueden elaborar esquemas de certificación que se someten al escrutinio y aprobación del CEPD.

Durante el año 2023 se aprobó el dictamen 15/2023 sobre los criterios de certificación denominados "Brand Compliance certification standard" presentado por la entidad Brand Compliance B.V. a través de la autoridad de Holanda, y que recibió un dictamen favorable. Estos **criterios de certificación** tienen por objeto asegurar una aplicación consistente del RGPD excepto para las transferencias internacionales.

Puede **acceder a estos dictámenes** sobre esquemas de certificación a través del **enlace**.

RECOMENDACIONES

Recomendaciones 1/2022 sobre la Solicitud de Aprobación y sobre los elementos y principios que se encuentran en las Normas Corporativas Vinculantes del Responsable (BCR) (Art. 47 RGPD)

Tienen por objetivo clarificar los requisitos que han de reunir las BCR en relación con las obligaciones de los responsables y los encargados de BCR (BCR-C Y BCR-P) con el fin de garantizar unas mismas condiciones de igualdad para todos los solicitantes de BCR.

Las recomendaciones se han realizado al objeto de actualizar recomendaciones previas sobre BCR contenidas recogidas en los documentos WP 256 rev.01 para BCR-C, y WP 257 rev.01 para BCR-P así como incluir los formularios de solicitud normalizados que deben utilizar los solicitantes de las BCR y contenidos en el documento WP264 del Grupo de Trabajo del Artículo 29 para BCR-C y al WP265 para BCR-P, respectivamente.

La recomendación también incorpora los requisitos señalados por el TJUE en su Sentencia Schrems II, en relación con los elementos principales contenidos en las nuevas Cláusulas Contractuales Tipo de la Comisión Europea para realizar transferencias internacionales de datos personales a terceros países. Además, estas recomendaciones incorporan la experiencia acumulada por las autoridades de protección de datos en el curso de los procedimientos de aprobación de solicitudes concretas de BCR desde la entrada en vigor del RGPD. **La aprobación de las BCR es una tarea que deben desempeñar todas las Autoridades de Supervisión miembros del CEPD trabajando de la misma forma**, y por ello es muy importante alcanzar un entendimiento común, entre todas las Autoridades de Supervisión, sobre los requisitos que deben incluirse en las BCR y en su formulario de solicitud.

Tras ser sometidas a consulta pública, **las recomendaciones** fueron aprobadas estando disponibles en el siguiente **enlace**.

DECISIONES VINCULANTES

A tenor del artículo 65 del RGPD, el CEPD tiene potestad para adoptar decisiones vinculantes cuando entre las autoridades principales y las interesadas no se llega a acuerdos por unanimidad en relación con las propuestas de decisión en los casos transfronterizos. **Este es el denominado mecanismo de resolución de disputas.** En el año 2023, el CEPD ha adoptado dos decisiones vinculantes relativas al artículo 65 del RGPD así como una decisión vinculante urgente relativa al artículo 66 del RGPD que se detallan a continuación:

Decisión vinculante 1/2023 sobre el litigio presentado por la Autoridad de Supervisión de Irlanda sobre las transferencias de datos realizadas por Meta Platforms Ireland Limited para su servicio Facebook (Art. 65 RGPD)

En el presente caso, la autoridad de control principal fue la de Irlanda (Data Protection Commission - DPC) y el responsable del tratamiento investigado fue META Platforms Ireland Limited (antes Facebook Ireland Limited).

Este caso gira en torno a la licitud de las transferencias que ha estado realizando este responsable a META US. Estas eran sistemáticas, masivas, repetitivas y constantes (esto es, no ocasionales o esporádicas).

En su borrador de decisión de 06/07/22, DPC consideró que ese responsable cometió infracción al artículo 46.1 del Reglamento. Esa autoridad ordenó suspender las transferencias a ese país, sobre la base de que la legislación americana no proporcionaba un nivel de protección equivalente al de la Unión Europea/Espacio Económico Europeo.

La resolución de la disputa giró en torno a la necesidad de imponer dos medidas coercitivas adicionales por haber cometido esta infracción. Por un lado, una multa que deberá ser efectiva, proporcional y disuasoria. Por otro lado, y con

relación a los datos ya transferidos a EEUU, una orden a META para que cumpla el capítulo V del Reglamento, debiendo cesar el tratamiento ilícito de estos datos en ese país (incluido su conservación). La decisión vinculante del Comité incluyó ambas medidas adicionales.

Esta **decisión vinculante 1/2023** puede ser consultada en el **siguiente enlace**.

Decisión vinculante 2/2023 sobre el litigio presentado por la Autoridad de Supervisión de Irlanda respecto de TikTok Technology Limited (Art. 65 RGPD)

En el presente caso, la autoridad de control principal fue la de Irlanda (Data Protection Commission - DPC) y el responsable del tratamiento investigado fue TikTok Technology Limited (TTL).

Este caso gira principalmente en torno a la eficacia de las medidas técnicas y organizativas de verificación de edad adoptadas por TTL durante el período de referencia (desde el 31/07/20 hasta el 31/12/20), así como sobre una posible infracción adicional al principio de lealtad.

El CEPD decidió que no tiene en este caso suficiente información como para valorar de forma concluyente el cumplimiento por TTL del artículo 25.1 RGPD (protección de datos desde el diseño), pese a sus serias dudas sobre la eficacia de estas medidas. El CEPD admitió la infracción adicional al principio de lealtad, y ordenó a DPC que la tenga en cuenta en su decisión final. El CEPD ordenó que la decisión final irlandesa incluya la eliminación de los patrones engañosos (deceptive design patterns) identificados en esta decisión vinculante, en el plazo que determine DPC.

Esta **decisión vinculante 2/2023** puede ser consultada en el siguiente **enlace**.

Decisión Urgente Vinculante 01/2023 solicitada por Autoridad de Supervisión de Noruega para ordenar medidas definitivas respecto de Meta Platforms Ireland Ltd (Art. 66(2) RGPD)

El Plenario del Comité adoptó el 27/10/23 la decisión vinculante urgente (UBD) 01/2023, sobre FACEBOOK e INSTAGRAM. La Autoridad de Supervisión de Noruega fue quien solicitó esta decisión, en aplicación del artículo 66 del RGPD. META Irlanda (META) es el responsable del tratamiento en cuestión siendo la autoridad principal del caso la de Irlanda (DPC) y el resto de autoridades del Espacio Económico Europeo interesadas en el caso.

Noruega presentó este caso porque las decisiones vinculantes del CEDP 03/2022 (sobre FACEBOOK) y 04/2022 (sobre INSTAGRAM), ambas de 05/12/22, señalaron a DPC que META se apoyó inapropiadamente en el artículo 6.1.b) RGPD para tratar datos de un reclamante para realizar publicidad comportamental o “behavioral advertising” (BA, por sus siglas en inglés), y que no se apoyó en ninguna otra base legal para realizar BA, por lo que carecía de base legal legitimadora para tratar esos datos con esa finalidad, infringiendo por tanto el artículo 6.1, por lo que debía de recibir una orden de cumplimiento de DPC para acatar esa disposición en el plazo de 3 meses.

En aplicación de esas decisiones vinculantes, DPC adoptó el 31/12/22 sus resoluciones IN-18-5-5 (sobre FACEBOOK) e IN-18-5-7 (sobre INSTAGRAM), que reprodujeron lo señalado anteriormente por el Comité.

El Plenario del CEPD de 27/10/23 ordenó a DPC que disponga la prohibición de realizar BA por parte de META, con base en el 6.1.b) y en el 6.1.f) RGPD. Tuvo en cuenta que, más de 6 meses después de la expiración del plazo que tenía META para adaptarse a esta disposición, ese responsable seguía sin cumplir este artículo.

Esta **decisión vinculante 01/2023** puede ser consultada en el **siguiente enlace**.

INFORMES

Contribución del CEPD al informe sobre la aplicación del RGPD según el artículo 97

A tenor del artículo 97 del RGPD, la Comisión debe presentar en 2024 un informe de carácter público al Parlamento Europeo y al Consejo que evalúe su aplicación.

El CEPD ha adoptado en su plenario de diciembre la presente contribución para que sea tenida en cuenta por la Comisión en el citado informe.

En su informe, el CEPD estima que, solo cinco años y medio después de la entrada en vigor del RGPD, es prematuro abrir su proceso de revisión, considerando que es conveniente esperar a tener más elementos que nos permitan apreciar los aspectos que esta importante regulación necesita mejorar. Una vez que se disponga de más perspectiva, podrá lanzarse ese proceso.

El CEPD hace un llamamiento a los legisladores europeos y a la Comisión para que trabajen hacia una mayor claridad y homogeneidad por lo que respecta a las nuevas funciones y competencias de las autoridades de control. También les solicita que garanticen que tanto el CEPD, como las autoridades de control que lo forman, dispongan de los recursos suficientes tanto humanos, como técnicos y financieros.

Este **documento** se encuentra en el **siguiente enlace**.

Sobre la designación y situación de los Delegados de Protección de Datos (DPD)

Dentro del Marco de Supervisión Coordinado (CEF, por sus siglas en inglés), el CEPD promueve anualmente una acción de supervisión común a desarrollar de forma voluntaria entre las autoridades que lo componen. La acción promovida para el ejercicio de 2023 fue dedicada a conocer la situación de los Delegados de Protección de Datos o DPDs y la AEPD participó de forma activa en dicha acción.

Como resultado del trabajo anterior, el CEPD adoptó su informe final de conclusiones. Este informe contiene un resumen ejecutivo, una serie de recomendaciones sobre este tema, un primer anexo con estadísticas y un segundo anexo con unos informes que 25 DPAS (incluida la AEPD) han realizado previamente en sus respectivos territorios.

En esta iniciativa, el Comité ha pretendido obtener información sobre el perfil, la posición y el trabajo de los DPDs; recabar la experiencia y conclusiones de las autoridades que tengan previsto realizar inspecciones en este ámbito, estén iniciándolas o pretendan continuarlas; sensibilizar sobre los requisitos aplicables a los DPDs; garantizar que estos cumplen el papel clave que tienen asignado y evaluar las necesidades actuales.

Las DPAS han estado preparando este informe, en el seno del Comité, a lo largo de todo el año 2023. Una vez adoptado, el CEPD está abierto a su actualización caso de que sea necesario.

Este **informe sobre la designación y situación de los DPD** se encuentra en el **siguiente enlace**.

DECLARACIONES

Declaración 1/2023 sobre la primera revisión del funcionamiento de la decisión de adecuación para Japón

En enero de 2019 la Comisión Europea aprobó la decisión de adecuación de Japón. Dicha adecuación preveía una revisión a los dos años, revisión que se ha llevado a cabo en 2021.

Como resultado de la revisión, la Comisión Europea preparó un borrador de informe sobre el que pidió opinión a representantes designados por el EDPB y finalmente publicó su informe definitivo el 3 de abril de 2023.

El citado informe es positivo y recoge los avances que Japón ha realizado en este sentido como, por ejemplo, mediante la adopción de nuevas normativas, fortaleciendo así el marco legal entorno a la protección de datos, alineándose aún más a los estándares EU.

Con base en lo anterior, el EDPB ha realizado una declaración de apoyo, solicitando que la siguiente revisión se realice dentro de cuatro años.

Esta **declaración 1/2023** se encuentra en el **siguiente enlace**.

Grupo de trabajo (Taskforce) sobre ChatGPT

El Plenario del CEPD decidió crear el 13/04/23 una estructura específica, denominada "Task Force" (TF) para coordinar los expedientes sancionadores locales abiertos por las autoridades de control del Espacio Económico Europeo (EEE) sobre los tratamientos de datos personales realizados por la entidad norteamericana Open AI (OAI) en el servicio ChatGPT.

El CEPD tomó esta decisión ya que, hasta el 15 de febrero de 2024, OAI no disponía de un establecimiento dentro del EEE, lo que impedía activar el denominado mecanismo de ventanilla única del RGPD, también conocido como One-Stop-Shop, o OSS, por sus siglas en inglés.

Este mecanismo OSS proporciona un canal formal de coordinación entre las autoridades de control concernidas en cada expediente para acordar en concertación los borradores de decisiones relativos a tratamientos transfronterizos de datos.

Por consiguiente, era necesario crear un sistema de coordinación entre las autoridades de control, al margen del OSS, para armonizar las decisiones que las respectivas autoridades de control deberán de tomar en un futuro sobre este servicio. Desde su creación, este grupo ha mantenido reuniones periódicas intercambiando información.

8.1.2 Grupo de trabajo (Taskforce) sobre competencia, consumo y protección de datos

Se han celebrado **cinco reuniones** de este grupo durante 2023.

Se decidió por parte del grupo designar puntos de contacto nacionales en las autoridades de consumo y competencia para llevar a cabo el desarrollo de los trabajos. La AEPD tiene ya puntos de contacto nacional en la CNMC y en la Oficina de Enlace Única para la Cooperación para la Protección al Consumidor (CPC) de la Dirección General de Consumo (Ministerio de Derechos Sociales, Consumo y Agenda 2030). Se han producido reuniones con los vocales designados para esta cooperación y la AEPD se viene sumando a las reuniones de la CNMC y la CPC en foros internacionales.

Se ha circulado un primer cuestionario por el Secretariado del CEPD para determinar las formas de cooperación entre las autoridades administrativas nacionales de los Estados miembros involucradas en el seno del CEPD que ha sido circulado a CNMC y CPC para su cumplimentación.

La AEPD ha participado también en la reunión del Grupo de Trabajo de Consumo de la Comisión Europea sobre los nuevos casos presentados ante la COM UE en relación las obligaciones de transparencia y legitimidad de los modelos de negocio de las plataformas de servicios digitales. Se ha participado también en las reuniones del Grupo de Alto Nivel de la Comisión Europea para la ejecución de la Ley de Mercados Digitales de la UE.

8.1.3 Grupo de Trabajo (Taskforce) sobre cooperación de los miembros del CEPD en otros foros internacionales

La AEPD ha participado en un total de **3 reuniones** durante 2023.

La AEPD, como miembro de la mesa del Comité Consultivo de la Convención 108 del Consejo de Europa (T-PD), ha venido informando al grupo sobre los trabajos del Comité.

La representación de la AEPD en el T-PD fue comandada por este mismo para informar de los trabajos en el seno del CAI (Comité sobre Inteligencia Artificial del Consejo de Europa). La AEPD forma parte de la delegación del Reino de España en el CAI y en tal condición ha venido participando en las reuniones del mismo destinadas a la elaboración de la primera convención de inteligencia artificial del Consejo de Europa. La AEPD ha venido informando puntualmente a las taskforce sobre asuntos internacionales del Comité Europeo de Protección de Datos sobre e resultado de los trabajos de redacción de este borrador de la convención. La AEPD ha venido recibiendo información puntual de los trabajos de UNESCO, OCDE, Asamblea Global de la Privacidad (GPA), G-7 y G-20 en materia de protección de datos y privacidad.

8.1.4 Grupo de Alto Nivel para la mejora de la ejecución de la cooperación policial y judicial en la UE

La AEPD ha participado en **2 reuniones del Grupo de Trabajo de Altos Expertos la Comisión Europea** para la mejora de la ejecución de la cooperación policial y judicial en la UE. Participó también en las **reuniones de los tres subgrupos de Trabajo del GTA**.

El objetivo del grupo es mejorar el acceso de las fuerzas policiales y judiciales nacionales, EUROPOL y Eurojust a los datos operacionales necesarios gestionados por las OTTs y SPIs (grandes proveedores y plataformas de servicios electrónicos) con fines de análisis operativo e investigación en materia de cibercriminalidad y lucha contra el terrorismo y el crimen organizado y contra los crímenes graves.

8.1.5 Grupo de Alto Nivel para la aplicación de la Ley de Mercados Digitales de la Unión Europea

Durante 2023 la AEPD ha participado en **tres reuniones** del GAN de la Comisión Europea sobre la aplicación de la ley de Mercados Digitales (DGA).

Se han tratado entre otros asuntos la creación de dos subgrupos de trabajar con el fin de analizar la correcta interpretación de los art. 5.2 y 7 de la ley europea de mercados digitales.

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

8.2.1 Comité de Supervisión Coordinada (CSC)

Durante 2023, el Comité de Supervisión Coordinada continúo asumiendo la supervisión de los distintos "grandes sistemas IT de la Unión Europea" a través de las actuales autoridades comunes de supervisión de los sistemas informáticos en el ámbito de la Cooperación policial y judicial de la Unión Europea:

- **SIS II** (sistema Schengen),
- **VIS** (visados),
- **Eurodac** (inmigración),
- **JSA y JIS** (aduanas),
- **Europol** (policía europea)
- **Eurojust** (órgano de cooperación judicial europea).

Son objeto también de la supervisión coordinada las actividades de la Oficina de la Fiscalía Europea y del IMI (sistema informático de Mercado Interior). Por este motivo, las referencias a las autoridades comunes de los sistemas IT de Europol, Eurojust y SIS II que ya han pasado a la nueva supervisión coordinada bajo el CSC se eliminan en esta Memoria anual de 2023.

El Comité ha desarrollado durante 2023 las actividades incluidas para dicho año en su programa de trabajo para el periodo 2022-2024, que establece las actividades a realizar en el marco de la supervisión de los sistemas informáticos citados. Se han celebrado en total cuatro reuniones presenciales y reuniones mensuales en formato remoto. En dichas reuniones, se ha venido elaborando el nuevo marco de supervisión de los diferentes sistemas.

En el ámbito de la supervisión general de los sistemas se han diseñado talleres conjuntos sobre estrategias para la supervisión de los grandes sistemas IT en el ámbito de la cooperación policial y judicial y se ha desarrollado un plan de iniciativas para la participación de la sociedad civil.

En el marco de esta última, se ha invitado a la participación de actores de la sociedad civil como ONGs (ej.: STATEWATCH) y asociaciones profesionales etc.

En relación con el sistema IT **SIS II**, se ha realizado un primer workshop con casos de estudios sobre el ejercicio de auditoría en el sistema SIS II. Se han elaborado además modelos de cuestionario para monitorizar la aplicación de artículos específicos del Reglamento SIS, como su art. 36 sobre alertas sobre control específico y modelos armonizados para la recogida de datos estadísticos del sistema.

En relación con el sistema **EUROJUST** se han venido discutiendo las fórmulas de cooperación entre las autoridades judiciales y en particular los acuerdos con equipos de investigación conjunta con Estados terceros y las cláusulas de protección de datos a incluir en dichos acuerdos.

Por otra parte, la discusión del diseño de actividades para la monitorización de los tratamientos de datos de menores de edad por parte de las autoridades de protección de datos ha sido también objeto de atención por el CSC.

El uso de canales seguros de comunicación de datos y la mejora del intercambio de mensajes en SIENA por parte de **EUROPOL** y las autoridades judiciales en el marco de los intercambios de datos por parte de equipos de investigación conjunta fue también objeto de estudio por parte del Comité.

Por lo que se refiere al sistema IT EUROPOL, el Comité examinó con el EDPS los hallazgos del informe anual sobre los tratamientos de datos operacionales en el marco EUROPOL. Entre los asuntos tratados destacan las transferencias de datos a fuerzas policiales de terceros Estados con un nivel de protección de datos en el marco de procedimientos de cooperación policial.

Se abordó también el asunto de los tratamientos de datos de menores de edad en dichos procedimientos, la necesidad de licitud de estos tratamientos y su proporcionalidad de conformidad con la jurisprudencia del TJUE. Existe una especial preocupación por la utilización de menores en el crimen organizado y en particular en delitos específicos como el robo con fuerza de domicilios privados. Las delegaciones estudiaron la armonización de los procesos de introducción de descripciones en los sistemas IT en el caso de menores involucrados en crímenes a edades muy tempranas.

En relación con la oficina de la fiscalía europea EPPO, la AEPD ha venido siguiendo el despliegue de las oficinas nacionales EPPO y en particular de la oficina española. El CSC ha monitorizado también la inspección conjunta llevada a cabo por la agencia portuguesa de protección de datos y el Supervisor Europeo de Protección de Datos en la oficina EPPO de Portugal.

El CSC ha seguido discutido también, en vista del resultado de la inspección, sobre las necesidades de ejecución de las oficinas únicas nacionales del EPPO.

8.2.2 Grupo de Coordinación de la Supervisión VIS (VIS SCG)

Durante 2023, la Agencia ha continuado con sus trabajos en el **VIS SCG** en el marco del programa 2022-24 aprobado en el ejercicio 2023.

Como continuación a la auditoría Schengen de España llevada a cabo entre el 20 y el 25 de marzo de 2022, que incluyó la auditoria del sistema VIS de visados, la AEPD ha tenido reuniones con las autoridades del Ministerio de Exteriores en al ámbito de las actividades consulares para continuar con el plan de actuaciones en la monitorización y seguimiento de la aplicación de la protección de datos personales en el ámbito de la concesión de visados. Esta actividad ha seguido las recomendaciones aprobadas por el VIS SCG en plan de actuación 2022-24.

La AEPD ha participado también en las discusiones sobre el nuevo plan común de inspecciones del sistema VIS que se establece como una actividad coordinada bajo la dirección de la Agencia Portuguesa de Protección de Datos.

En el marco de las reuniones del SCG VIS, la Comisión Europea ha venido informando regularmente de sus inspecciones y auditorias. Ha informado también sobre el desarrollo de los trabajos de su propuesta para un “visado digital europeo”.

8.2.3 Grupo de Coordinación de la Supervisión de Eurodac (GCS) (sistema de información huellas dactilares)

La AEPD participo durante 2023 en las **dos reuniones anuales del GCS Eurodac** en el Comité Europeo de protección de datos.

En 2023 se ha procedido a continuar con el programa para el periodo 2022-24 que desarrolla los siguientes asuntos.

1. La entrada en vigor y aplicación del Reglamento de interoperabilidad, y su efecto e interacción con el Reglamento Eurodac.

2. La sugerencia de temas a tratar durante las inspecciones de Eurodac a nivel nacional, con el fin de proporcionar orientación a las Autoridades de Control.

3. La actividad del SCG de Eurodac en el marco de la supervisión coordinada en el marco del CEPD.

4. La cuestión de los HIT falsos.

En este marco, la AEPD informó al Grupo de Supervisión de la Coordinación de EURODAC sobre la futura inspección de la AEPD al punto de contacto nacional Eurodac en cumplimiento del plan de actuaciones de la agencia para la supervisión de los sistemas IT de cooperación policial y judicial. Las autoridades de protección de datos fueron informadas por EU-LISA sobre los incidentes en el sistema y en particular por los errores o "falsos positivos" acaecidos durante el año 2023.

El GSC se ocupó también del acceso de las fuerzas policiales y jueces al sistema EURODAC. Finalmente, el GSC aprobó el informe de actividad 2020-21 y su publicación en el DOCE.

A instancias del GSC, se discutió también sobre la influencia del reglamento de interoperabilidad en la operativa del sistema IT Eurodac y de los Reglamentos UE de screening y Eurodac a la vista del informe de Schengen de 16 de mayo de 2023. Se decidió seguir de cerca el proceso y estudiar el impacto de estas normas en el nivel nacional. Se ha formado un grupo de trabajo para este asunto en el seno del GSC.

8.2.4 Participación de la AEPD en otros foros internacionaltes

• 8.2.4.1 Consejo de Europa

Comité Consultivo y Mesa de la Convención 108+ del Consejo de Europa

Durante 2023 la Agencia Española de Protección de Datos participó en las dos reuniones ordinarias del Comité Consultivo en formación de Plenario y en las tres reuniones en formación de Mesa. En 2022 se produjo la renovación de la Mesa, órgano de dirección de los trabajos del Comité Consultivo. La Agencia forma parte de la Mesa al haber sido elegido uno de los miembros de la delegación española como miembro de esta. Dado que la elección de los miembros es realizada a título personal la Agencia siguió contando con dos miembros en el Comité con representación en Plenario y Mesa.

Como se mencionó en el informe de 2021, el Estado español ratificó en fecha 28 de enero de 2021 Convenio 108+ que ha sido depositado. Hasta finales de 2023, un total de 43 Estados parte han firmado la convención, de los cuales 28 han procedido también a su ratificación. 3 estados observadores son también firmantes de la convención: Argentina, Uruguay e Isla Mauricio.

A continuación, se recogen los **documentos aprobados por el Consejo de Europa en materia de protección de los datos personales** durante el ejercicio 2022-23:

- Módulo segundo de las Cláusulas Contractuales Estándar del Consejo de Europa para transferencias internacionales de datos personales.
- Recomendaciones sobre protección de datos en los tratamientos de datos personales para la lucha contra el lavado de dinero, la falsificación y la financiación del terrorismo.
- Aprobación de la resolución de la Mesa de la convención para comenzar los trabajos sobre las recomendaciones en materia de protección de datos personales en el contexto de las neurociencias.

Comité de Inteligencia Artificial

El Comité de Inteligencia Artificial representa a los 46 Estados parte del Consejo de Europa que son miembros del Comité y a siete Estados que tienen la condición de observadores. Tiene como misión elaborar un texto consolidado de borrador de la primera convención del Consejo de Europa en materia de inteligencia artificial que será presentado al Comité de Ministros del Consejo de Europa en mayo de 2024. La Convención tiene plazo de presentación del borrador a la asamblea en marzo de 2024.

La Comisión Europea lidera las negociaciones en colaboración con las delegaciones de los Estados miembros de la UE que son partes del Comité CAI. La AEPD ha participado en un total de 16 reuniones del Comité para la elaboración del texto del borrador de la convención en formación de Plenario y Mesa de redacción.

- 8.2.4.2 Asamblea Global de Privacidad (GPA)

La 45ª edición de la Reunión Anual de la Asamblea Global de Privacidad tuvo lugar este año en Bermuda del 15 al 20 de octubre.

En esta edición **se aprobaron** las siguientes **resoluciones**:

- Resolución sobre IA y empleo.
- Resolución sobre Datos de Salud e Investigación Científica.
- Resolución sobre el logro de estándares globales de Protección de Datos.
- Resolución sobre la biblioteca GPA.
- Resolución sobre sistemas de IA generativa.
- Resolución sobre el establecimiento de un grupo de trabajo sobre la perspectiva interseccional de género en la protección de datos.
- Premio Resolución sobre Privacidad y Derechos Humanos.

Además de las resoluciones anteriores, la GPA aprobó su Plan Estratégico para el periodo 2023-2025.

Todos estos **documentos** son accesibles en el **siguiente enlace**.

- 8.2.4.3 Grupo Internacional de Trabajo sobre Protección de Datos en Tecnología – Grupo de Berlín

El Grupo Internacional de Trabajo sobre Protección de Datos en Tecnología (IWGDPT por sus siglas en inglés), también denominado "Grupo de Berlín", centra su atención en las tendencias y la evolución del sector tecnológico, como el "Big Data", el "Internet de las cosas o IoT" o la inteligencia artificial. Para ello, el grupo elabora recomendaciones y directrices para utilizar estas tecnologías de forma acorde con los requisitos de protección de datos.

En su trabajo conjunto, el Grupo de Berlín se beneficia de su composición heterogénea y transnacional, con participantes procedentes de autoridades supervisoras de la protección de datos, agencias gubernamentales, organizaciones internacionales y organizaciones no gubernamentales, así como de la investigación y el mundo académico. La AEPD aprecia especialmente el intercambio de opiniones y la cooperación con colegas internacionales para lograr las recomendaciones más completas y favorables a la protección de datos sobre nuevas tecnologías para un público internacional como es el público objetivo del Grupo de Berlín. Se reúne dos veces al año en distintas partes del mundo.

Las reuniones del año 2023 tuvieron lugar en Roma (Italia) y en Ottawa (Canadá).

Durante el año 2023 el **Grupo de Berlín aprobó y publicó** los siguientes **documentos**:

- Documento de trabajo sobre telemetría y datos de diagnóstico.
- Documento de trabajo sobre "ciudades inteligentes".

Estos **documentos del Grupo de Berlín** se encuentran accesibles en el **siguiente enlace**.

9. La cooperación con Iberoamérica

9.1. Encuentro RIPD febrero 2023

Durante los días **27 y 28 de febrero de 2023**, se celebró el Encuentro de la Red Iberoamericana de Protección de Datos (RIPD) en Santa Cruz de la Sierra (Bolivia).

En el Encuentro se repasaron los nuevos desarrollos legislativos nacionales en la Región y se desarrollaron los paneles: "**De la teoría a la práctica. Adoptando mecanismos regionales para fomentar la transferencia internacional de datos**" en el que se abordó la problemática de las transferencias internacionales. "**Protección de datos en salud**", donde se trataron el impacto y la regulación de la inteligencia artificial en el ámbito sanitario. "**Brechas de Seguridad**". "**La protección de las personas en el ámbito digital, iniciativas de las autoridades de control**". Se desarrollaron también una serie de ponencias responsabilidad proactiva en la protección de datos, la privacidad desde el diseño y por defecto, las evaluaciones de impacto en el ámbito privado y público. Hubo un espacio dedicado a la Sociedad Civil sobre la violencia de género digital. En la sesión cerrada se renovó al INAI como Presidencia de la RIPD y se definió la estrategia a seguir para lograr un pronunciamiento de la CIDH sobre el derecho a la protección de datos.

9.2. Acción coordinada RIPD. Inteligencia Artificial - ChatGPT

El **27 de abril**, y a iniciativa de la Presidencia y la Secretaría de la RIPD, se celebró una reunión de autoridades de la RIPD con el fin de abordar la problemática asociada al servicio ChatGPT. Se acordó cooperar de forma efectiva en cuanto a las acciones de las autoridades en el marco de sus competencias nacionales. Esta acción es la primera acción coordinada de investigación que se desarrolla en el marco de la RIPD y de su Plan Estratégico 2021-2025.

9.3. Acción coordinada RIPD. Solicitud CoIDH

Solicitud de Opinión Consultiva elaborada de forma conjunta por el INAI y el INCAM que tiene como propósito realizar una solicitud formal a la Corte Interamericana de Derechos Humanos (CoIDH) para que esta se pronuncie, mediante una Opinión Consultiva, respecto de la interpretación del contenido esencial y alcance del derecho fundamental a la protección de datos personales, a la luz del contenido del artículo 11 de la Convención Americana sobre Derechos Humanos (CADH).

9.4. Encuentro XX aniversario RIPD

El Encuentro ha servido, para reforzar alianzas y apoyar a las diversas entidades que conforman la RIPD. En el ámbito de las organizaciones internacionales debemos destacar las colaboraciones en el mencionado Encuentro de organismos como la Organización de Estados Americanos, la Federal Trade Commission, la Organización para la Cooperación y el Desarrollo Económicos, la Organización de las Naciones Unidas a través de su Relatora Especial para la Privacidad, el Consejo de Europa, la Comisión Europea o el Supervisor Europeo de Protección de Datos. Se han reforzado las alianzas con otras Redes internacionales de Protección de Datos que tuvieron una participación directa en el Encuentro: La Comisión de Protección de Datos Personales de Singapur, en representación de ASEAN Asociación de Naciones de Asia Sudoriental y La Comisión Nacional para el Control de la Protección de Datos Personales de Marruecos, como Secretaría Permanente de la Red Africana de Protección de Datos.

Durante el Encuentro que nos ocupa, que se ha llegado a considerar como una "refundación de la RIPD", se ha llegado al consenso por parte de las Autoridades de la Región de la modificación de los Estatutos de la Red para actualizarlos en base a criterios comunes. Se ha incidido también en la

necesidad de la "internacionalización de la RIPD" a través de colaboraciones y convenios con otras redes mundiales de protección de datos, así como el aumento de su visibilidad en la Región.

Se ha aprobado una declaración sobre Neuroderechos mediante la cual la RIPD se adhiere a las declaraciones del Comité Jurídico Interamericano de la OEA.

- **Creación de cuatro grupos de trabajo:**
  - ChatGPT
  - Neurodatos
  - Violencia Digital y Salud Digital
  - WorldCoin
- **Actualización web RIPD.**
- **Gestión repositorio en web RIPD** incluyendo herramientas y guías elaboradas en los países de la Región.
- En abril de 2024 se realizará un **taller de trabajo en Lima, Perú** para analizar los avances de los cuatro grupos de trabajo y la adhesión a las Cláusulas Contractuales Modelo por parte de las Autoridades Nacionales de la Región.
- En mayo de 2024 se celebrará el **Encuentro de 2024** en el que se aprobaría la redacción definitiva del nuevo Reglamento de la RIPD y los documentos con los resultados de los cuatro grupos de trabajo.

Para **más información** sobre este **encuentro XX aniversario RIPD** consulte el siguiente enlace.

9.5. Programa InterCoonecta 2023 de la AECID

Presentación al Programa InterCoonecta y adjudicación.

En el marco de este programa cuyo objetivo principal es la gobernanza democrática y la capacitación técnica de las Autoridades de la Región, se desarrollarán 4 cursos de formación para el personal de las entidades garantes de la Protección de Datos y apoyará el desarrollo del Encuentro anual RIPD 2024.

9.6. Convocatoria SEGIB

En el marco de la convocatoria de la SEGIB, de la que la AEPD ha sido adjudicataria como Secretaría Permanente de la RIPD, se han ejecutado las acciones correspondientes a las **dos categorías**:

- **Difusión.** A través del Encuentro XX aniversario RIPD. Estos fondos han apoyado la financiación del Encuentro XX aniversario, facilitando la participación de Autoridades de la Región.
- **Capacitación.** Visita de Estudios por parte de la AGETIC de Bolivia.

9.7. Webinario

Webinario sobre acuerdo de adecuación en materia de protección de datos entre la Unión Europea y el gobierno de Estados Unidos denominado EU-US Data Privacy Framework.

9.8. Colaboraciones

Con el fin de analizar sinergias y posibilidades de colaboración en materia de protección de datos y en el marco del proceso de internacionalización de la RIPD se han desarrollado las **siguientes actuaciones y reuniones** con Organismos Internacionales y Regionales:

- **Autoridad de Costa Rica.** Gestión con el CoE adhesión Costa Rica convenio 108+
- **Universidad Latinoamericana de Ciencia y Tecnología.** Costa Rica. Colaboración para pasantía, difusión y formación.
- **IDEA Internacional.** Participación en seminarios.
- **SEGIB.** Carta Iberoamericana de Principios y Derechos en Entornos Digitales. Colaboración en materia de Protección de Datos. Participación en seminarios.
- **Comisión de Protección de Datos Personales de Singapur**, en representación de ASEAN Asociación de Naciones de Asia Sudoriental.
- **Comisión Nacional para el Control de la Protección de Datos Personales de Marruecos**, como Secretaría Permanente de la Red Africana de Protección de Datos.
- **Agencia de Privacidad de California (CPPA).**
- **Federal Trade Commission.**
- **UNESCO.** Colaboración en LAC y UE en Neurotecnologías e Inteligencia Artificial.
- **Organización de los Estados Americanos.** Colaboración en Neuroderechos.
- **Comisión Europea.** Flujos transfronterizos en la Región.

LA AGENCIA EN CIFRAS

1. Inspección de datos

1. El inicio de la potestad de supervisión. Reclamaciones, comunicaciones y actuaciones por iniciativa propia

La Subdirección General de Inspección de Datos (SGID, en adelante) es el órgano dependiente de la Directora de la Agencia que, en caso de posible vulneración de la normativa o de no atención al ejercicio de derechos, analiza los indicios, realiza las actuaciones de evaluación o las de investigación oportunas y, cuando procede, instruye los procedimientos adecuados para proponer a la Directora la adopción de la resolución que corresponda.

Las reclamaciones pueden recibirse directamente en la Agencia, que es la situación más frecuente, aunque también pueden llegar a través de alguna Autoridad de Control de alguno de los Estados miembros del Espacio Económico Europeo (EEE). Estas últimas tienen un carácter transfronterizo y se admiten a través del mecanismo de ventanilla única, establecido en el artículo 60 del RGPD: son reclamaciones presentadas en otro Estado miembro del EEE o actuaciones que una Autoridad de Control (AC) del EEE ha decidido iniciar por propia iniciativa y en la cuales se ven afectados ciudadanos o establecimientos del responsable en España. 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 presunta infracción. Los casos recibidos de otras AC muestran una tendencia creciente en los últimos años.

Bien como consecuencia de las reclamaciones, bien por propia iniciativa, la Agencia puede determinar la apertura de actuaciones de investigación para alcanzar una mejor y más concreta determinación de los hechos que puedan infringir la normativa de protección de datos, así como la identificación del responsable. Durante el año 2023 ha subido ligeramente el número de investigaciones que se han realizado por propia iniciativa con respecto a 2022.

Dentro de los casos en los que se actúa por iniciativa propia hay que destacar las actuaciones de investigación que se realizan, cuando procede, a raíz de las notificaciones de brechas de datos personales. Las notificaciones se efectúan de acuerdo con el artículo 33 del RGPD. Estas brechas se reciben en primera instancia en la División de Innovación Tecnológica (DIT) de la AEPD y, tras un primer análisis, cuando existan datos objetivos que justifiquen un análisis en mayor profundidad, la Directora acuerda iniciar una investigación de oficio e instar a la SGID para que comience las actuaciones previas de investigación tendentes a acreditar los hechos.

Aunque por encima de estas variaciones, lo más destacado por su volumen y nivel de crecimiento y lo que más impacta en el inicio de nuevos casos en 2023 ha sido el altísimo incremento de las reclamaciones recibidas en la Agencia.

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

Tabla 1: Entradas de nuevos casos a inspección

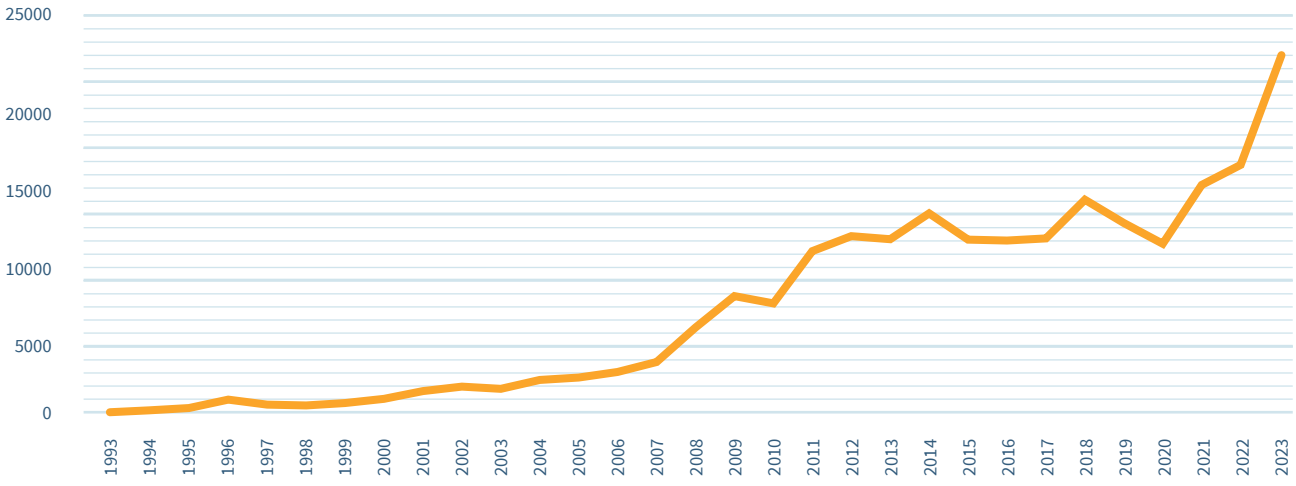
Tipo de entrada	2021	2022	2023	% relativo	Δ% anual
Reclamaciones* presentadas ante la AEPD	13.905	15.128	21.590	97%	43%
Casos transfronterizos procedentes de otras AC del EEE	581	651	708	3%	9%
Propia iniciativa de la AEPD (inc. brechas)	85	43	50	0%	16%
TOTAL	**14.571**	**15.822**	**22.348**	**100%**	**41%**

** Incluye denuncias en las que los datos personales no conciernen al solicitante*

La tendencia alcista de los últimos años se acentúa fuertemente en el número de entradas recibidas, especialmente en las reclamaciones, que suponen un 43% más que el año 2022 y un 55% más que hace dos años. Así, por tercer año consecutivo, se bate récord en cuanto al número de reclamaciones recibidas en esta Agencia, siendo ya más del doble de las recibidas en 2020.

Se cumplen 30 años de vida de la Agencia y, en este camino, el aumento de las reclamaciones ha sido una constante, acompañando a las sucesivas reformas normativas, y a la propia evolución social y los mayores riesgos de los tratamientos, por el volumen y extensión de los datos generados y la ubicuidad de los nuevos servicios y dispositivos que los tratan. Pero nunca se había experimentado el crecimiento con la pendiente que se observa desde el inicio de esta década. La evolución de las reclamaciones en estos 30 años se repasa en el **Anexo B: Evolución de las reclamaciones 1993-2023**.

Reclamaciones presentadas en la AEPD



Aunque el aumento en los casos transfronterizos es más moderado, un 9% (22% con respecto al 2021), este tipo de reclamaciones son bastante más costosas tanto en tiempo como esfuerzo del personal de la Agencia. Esto es así ya que existe la necesidad de llegar a un consenso con otras autoridades del EEE.

En 2023, a pesar del extraordinario incremento en la entrada, la SGID ha sido capaz de aumentar su capacidad resolutiva hasta las más de 20.000 reclamaciones, quedando la tasa de reclamaciones resueltas frente a reclamaciones recibidas en un 94%, y evitando así que el número de reclamaciones pendientes terminara el año en números difíciles de asumir. Sin embargo, pese a todo el esfuerzo que se ha realizado, las reclamaciones sin resolver al final del año son más de 4.900, un 32% superior a la cifra del año anterior. El reto de este año era mayúsculo, y la posibilidad de colapso en la SGID, una realidad. Las reclamaciones resueltas en el año han sido un 37% superior al año anterior, lo que pone de manifiesto el citado esfuerzo desde todos los frentes: organizativo, tecnológico, personal, etc. En la siguiente tabla se pueden consultar las cifras relacionadas con la tasa de resolución de reclamaciones:

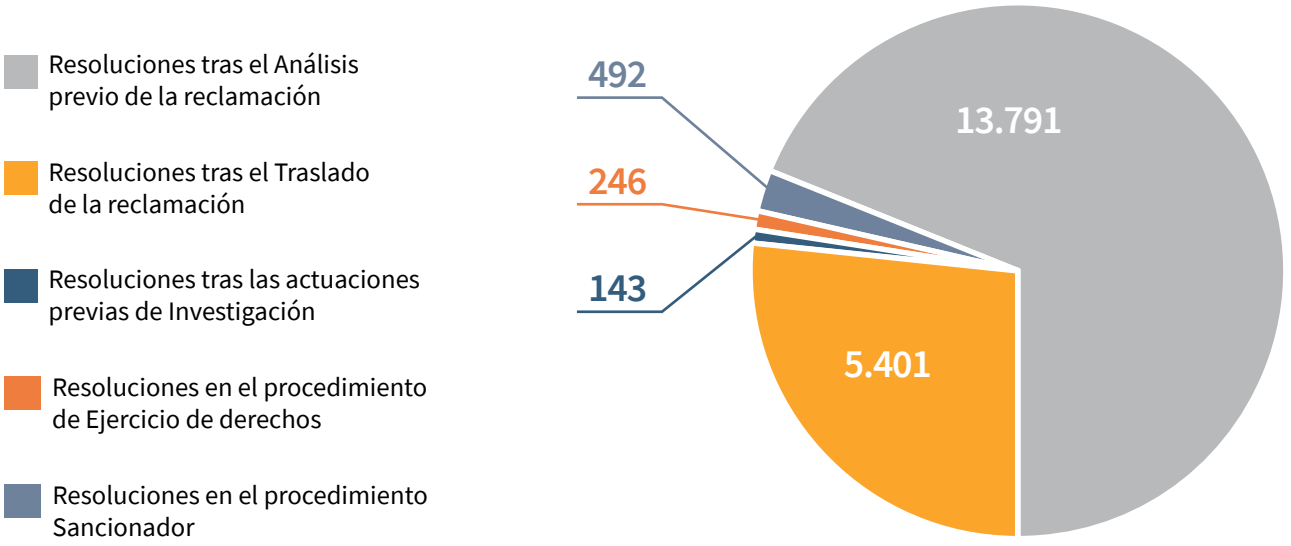
Tabla 2: Reclamaciones resueltas y pendientes

Tasa de resolución de reclamaciones	2021	2022	2023	Δ% anual
Reclamaciones* resueltas en el año	14.098	14.937	20.391	37%
Reclamaciones pendientes de resolver al finalizar el año	3.516	3.707	4.906	32%
Tasa de reclamaciones resueltas vs. recibidas en el año	101%	99%	94%	-5%

** Incluye toda reclamación por infracción de la normativa, con independencia de que los datos personales le conciernan.*

2. Resoluciones

Fase de resolución de las reclamaciones



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. Las entradas reflejadas en el apartado anterior pueden dar lugar a diferentes actuaciones y 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 una misma infracción y sujeto reclamado pueden agruparse y, al contrario, en una reclamación pueden aparecer múltiples reclamados, dando origen a múltiples procedimientos y, por lo tanto, a diferentes resoluciones.

2.1 Resoluciones durante el Análisis previo 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 previo de admisibilidad de la reclamación.

Si del análisis se desprende que la reclamación no cumple los requisitos de admisibilidad establecidos en la normativa, se inadmitirá y, en caso contrario, prosperará a la siguiente fase, donde se continuará con la evaluación sobre la admisibilidad. El motivo principal de inadmisión es el de no apreciarse indicios racionales de la existencia de una infracción en el ámbito competencial de la Agencia. Este año 2023, el porcentaje de resoluciones en esta fase se ha incrementado hasta situarse en el 69%. El aumento deriva de la gran cantidad de reclamaciones recibidas durante el año, muchas de las cuales no cumplen los requisitos para ser tramitadas, al no aportar toda la información necesaria que permita apreciar indicios racionales de la existencia de infracción. En este sentido, la Agencia está poniendo gran empeño en que las reclamaciones que reciba sean completas, aportando la documentación mínima necesaria para poder ser admitidas, y que no se reciban reclamaciones que no podrán fructificar (por no suponer una infracción, por no estar dentro del ámbito competencial de la Agencia, por falta de evidencias, etc.). En este sentido se ha publicado en 2023 la **resolución por la que se aprueban los modelos de presentación de reclamaciones**, en los que se detalla la información que tienen que aportar los reclamantes para que su reclamación pueda surtir efectos.

La siguiente tabla muestra los datos referentes a las resoluciones:

Tabla 3: Resoluciones en fase de Análisis previo de la reclamación

Tipo de resultado	2022	2023	% relativo	Δ% anual
Resoluciones tras la fase de Análisis de la reclamación*	**8.190**	**12.416**	**66%**	**52%**
Inadmisiones a trámite	7.928	12.135	65%	53%
Competencia de otras AC nacionales (CGPJ, AC auton.)	262	281	2%	7%
Resoluciones en otras fases	**5.436**	**6.282**	**34%**	**16%**
TOTAL	**13.626**	**20.073**	**100%**	**37%**

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

El motivo principal de inadmisión a trámite es que no se aprecien indicios de infracción en materia de protección de datos personales. A este respecto, resulta muy importante que los ciudadanos incluyan en sus reclamaciones las evidencias necesarias que demuestren los hechos reclamados, y en esta línea se está trabajando para que la entrada de reclamaciones por sede electrónica se realice de forma guiada, para que el ciudadano entienda en primer lugar si existe una infracción que pueda reclamar ante la Agencia y, de haberla, que la acompañe del soporte documental necesario.

2.2 Resoluciones posteriores

Con la entrada en vigor del RGPD y de la LOPDGDD, se introdujo una fase de traslado de la reclamación al responsable o encargado del tratamiento o, en su caso, al DPD, con la pretensión de resolver con mayor rapidez las reclamaciones, de acuerdo con las disposiciones del artículo 65 de la LOPDGDD. Estos traslados pueden conducir a la solución de la reclamación, o a aportar información que contribuya a clarificar la situación de manera que se pueda determinar que no ha existido infracción de la normativa de protección de datos. De esta forma, se consigue resolver un número elevado de reclamaciones en un tiempo reducido, con independencia de la actuación inspectora que siempre se puede realizar de acuerdo con las competencias que tiene atribuidas la SGID.

La inclusión de la fase de traslado ha supuesto una gran mejora con relación a los procedimientos de trabajo anteriores. En 2023, tras haber procedido al traslado de la reclamación, se dictó resolución finalizando su tramitación en el 86% de los casos, dando así una respuesta más rápida a los reclamantes que la que se conseguía con la normativa anterior y solucionado de una manera más ágil su reclamación.

El aumento del porcentaje de reclamaciones que se resuelven en fases tempranas (análisis de admisibilidad y traslado de la reclamación), ha conllevado la consecuente reducción en el número de actuaciones previas de investigación y de procedimientos. Esto permite a la SGID responder a la mayor complejidad de los tratamientos analizados con una adecuada distribución de los recursos disponibles, puesto que estas actuaciones posteriores requieren una importante dedicación de tiempo y personas.

La mayor eficacia de las actuaciones se refleja en la reducción de las resoluciones de archivo de las actuaciones previas de investigación. Las investigaciones terminan en un mayor porcentaje en la apertura de procedimientos, por tanto se inician menos actuaciones previas de investigación que no alcanzan su objetivo principal: determinar la infracción y el infractor.

Por su parte, la Agencia consideró la existencia de responsabilidades que debían ser depuradas en procedimiento sancionador en el 8% de los casos resueltos. Cabe señalar que en 2023 se ha dado cobertura normativa en la LOPDGDD al nuevo procedimiento de Apercibimiento, separado del procedimiento sancionador. Dado que solo se han realizado tres resoluciones con este nuevo procedimiento por los breves plazos transcurridos desde su aprobación, su número se reporta en la memoria agregado con los del procedimiento sancionador. Por otra parte, los cambios normativos también alcanzan a las sanciones impuestas a las administraciones públicas, que se resolverán en adelante con la declaración de infracción, reservando así la figura del apercibimiento a los supuestos en que se estime la apertura de un procedimiento de apercibimiento, para cualquier tipo de sujeto responsable.

En la siguiente tabla se muestra la distribución completa de resoluciones que se realizan después del análisis previo de la reclamación, según la fase en que se alcanza la finalización del caso.

Tabla 4: Resoluciones en fases posteriores al análisis previo de la reclamación

Tipo de resultado	2022	2023	% relativo	Δ% anual
Resoluciones tras el Traslado de la reclamación*	**4.268**	**5.401**	**86%**	**27%**
Respuesta satisfactoria del responsable o encargado	2.912	3.475	55%	19%
Ser plena competencia de otra AC del EEE	411	531	8%	29%
Actuar como autoridad interesada en el EEE (archivo provisional)	196	274	4%	40%
Otros motivos tras traslado**	749	1.121	18%	50%
Resoluciones tras las actuaciones previas de Investigación*	**288**	**143**	**2%**	**-50%**
Archivo de actuaciones previas de investigación	288	143	2%	-50%
Resoluciones en el procedimiento de Ejercicio de derechos	**305**	**246**	**4%**	**-19%**
Resuelto en el procedimiento de ejercicio de derechos	305	246	4%	-19%
Resoluciones tras procedimiento Sancionador	**575**	**492**	**8%**	**-14%**
Resuelto en procedimiento sancionador -Multa	385	367	6%	-5%
Resuelto en procedimiento sancionador - Apercibimiento o declaración de infracción	126	61	1%	-52%
Resuelto en procedimiento sancionador - Archivo	64	64	1%	0%
TOTAL	**5.436**	**6.282**	**100%**	**16%**

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

*** Incluye denuncias de las Fuerzas y Cuerpos de Seguridad del Estado y de ciudadanos cuyo derecho a la protección de datos no se ve afectado por la infracción, que finalizan con la información al responsable de sus obligaciones en relación con la infracción denunciada, la normativa a la que debe dar cumplimiento, y la advertencia de que en caso de no ajustarse se podrá iniciar las actuaciones pertinentes.*

2.3 Tiempos medios de resolución

Se reflejan a continuación los tiempos medios, en días, hasta que se dicta la resolución final. Debe tenerse en cuenta que las resoluciones que se realizan antes de la admisión a trámite son de inadmisión. Esto ocurre durante la evaluación de la reclamación, es decir, después del análisis previo o después del traslado de la reclamación al responsable o encargado del tratamiento.

En fase de Análisis previo de la reclamación, el tiempo medio responde al tiempo desde que tiene entrada la reclamación hasta que se resuelve su inadmisión, después de analizar la verificación formal del contenido y su fundamento. Debe tenerse en cuenta que el artículo 65.5 de la LOPDGDD establece un plazo de 3 meses para este concepto.

Tabla 5: Tiempo medio de resolución en análisis previo

Tiempos medios de resolución en fase de Análisis (en días)	2022	2023	Δ% anual
Resoluciones tras el Análisis de la reclamación*	25	32	28%
TIEMPO MEDIO	**25**	**32**	**28%**

** Incluye reclamaciones relacionadas con el ejercicio de derechos*

El aumento de los tiempos de análisis previo deriva directamente del caudal de reclamaciones recibido en 2023, que ha superado la capacidad de los recursos dedicados, y hasta la realización de un plan de choque en el que se pidió un sobreesfuerzo al personal para atajar la acumulación de reclamaciones en la entrada. Teniendo en cuenta el incremento de la carga de trabajo en 2023 (reclamaciones un incremento del 43% en la entrada de reclamaciones, lo que ha supuesto un aumento del 52% de resoluciones en la fase de análisis previo) y el incremento de personal en la subdirección, que, frente a ello, ha sido solo de un 20%, el número medio de días resultante ha aumentado menos de lo que correspondería proporcionalmente al aumento de carga de trabajo por persona. Esta salvedad es igualmente aplicable al resto de tiempos de resolución que se desglosan a continuación.

En la fase de traslado de la reclamación al responsable o encargado, el tiempo medio responde al tiempo desde que tiene entrada la reclamación hasta que se firma la resolución de inadmisión, tras el traslado al responsable y el análisis de la respuesta recibida. El tiempo medio es inferior a los tres meses que dispone la normativa para la admisión a trámite, aunque de nuevo es superior al del año previo por idénticos motivos.

Superadas estas dos fases, la reclamación se admite a trámite y se inician los procedimientos establecidos en la Ley. 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.

El tiempo medio global de resolución ha aumentado, aunque muy ligeramente respecto al año 2022. Con este dato se cambia a la tendencia bajista en los tiempos de resolución que se venía logrando en los últimos años, resultado directo del aumento exponencial de las reclamaciones, así como del aumento de complejidad de los tratamientos de datos que se realizan y que a su vez determinan una mayor complejidad de las investigaciones y procedimientos de esta Agencia.

Tabla 6: Tiempo medio de resolución según el procedimiento en que se resuelve			
Tiempos medios de resolución según el procedimiento (en días)	**2022**	**2023**	**Δ% anual**
Resoluciones tras las actuaciones de Traslado*	82	91	11%
Resoluciones tras las actuaciones previas de Investigación	262	269	3%
Resoluciones en el procedimiento de Ejercicio de derechos	84	110	31%
Resoluciones en el procedimiento Sancionador	242	292	21%
TIEMPO MEDIO	**109**	**112**	**3%**

** Incluye reclamaciones relacionadas con el ejercicio de derechos*

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, con independencia de que finalicen o no el expediente y, por lo tanto, den o no lugar a resoluciones. Un ejemplo de ello sería un traslado de reclamación que no da frutos, o unas actuaciones previas de investigación que dan lugar a un procedimiento sancionador. Estas actuaciones no generan una resolución y, por lo tanto, no aparecen detalladas en el apartado anterior, pero sí suponen una tramitación de la que se da cuenta en este apartado. 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 apartado anterior.

Se debe puntualizar que el número de reclamaciones evaluadas en la fase de análisis previo de admisibilidad puede oscilar frente al número de reclamaciones presentadas en el año, puesto que es un trámite que tiene una duración media de 31 días como se indica más adelante, por tanto se inicia el año analizando reclamaciones pendientes del último mes del año anterior, y de la misma forma se finaliza el año sin poder concluir el análisis del total de reclamaciones presentadas en las últimas semanas del año.

Se puede observar un fuerte aumento de actuaciones en las primeras etapas, consistente con el gran aumento de reclamaciones presentadas, así como con el aumento de resoluciones en la fase de traslado de la reclamación al responsable o encargado del tratamiento. Siguiendo con la tendencia del año pasado, el número de actuaciones de investigación ha descendido. Los motivos son varios, principalmente por el aumento de resoluciones en fases anteriores, y por los criterios seguidos para su inicio: ha aumentado su rigor, acompañado de una mayor profundidad en las investigaciones. Esto último ha tenido un efecto directo sobre el porcentaje de investigaciones que culminan en procedimientos sancionadores, aumentando en 10 puntos con respecto al año anterior, y 21 con respecto a hace 2 años. La reducción en los procedimientos sancionadores y de derechos también deriva del aumento de resoluciones en fases previas, a lo que se añade en el caso del ejercicio de derechos un descenso en las reclamaciones específicamente relacionadas con ellos.

El aumento en el número de recursos de reposición tramitados también es consistente con el aumento del número de resoluciones dictadas.

Tabla 7: Actuaciones realizadas			
Número de actuaciones finalizadas según la fase del procedimiento	**2022**	**2023**	**Δ% anual**
Análisis previo de admisibilidad de reclamaciones*	14.654	21.156	44%
Actuaciones de traslado*	5.150	6.281	22%
Actuaciones previas de investigación	476	316	-34%
Procedimientos de ejercicio de derechos	305	246	-19%
Procedimientos sancionadores	575	492	-14%
Recursos de reposición	735	940	28%
TOTAL	**21.895**	**29.431**	**34%**

** Incluye reclamaciones relacionadas con el ejercicio de derechos*

3.1 Tiempos medios de tramitación

Los tiempos que aparecen en este apartado miden 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. La misma causa que se expuso al describir el aumento de los tiempos medios de resolución aplica naturalmente a cada una de las fases del procedimiento.

Tabla 8: Tiempos medios de tramitación			
Tiempos medios de actuaciones realizadas en la gestión de la reclamación según la fase del procedimiento (en días)	**2022**	**2023**	**Δ% anual**
Reclamaciones analizadas*	24	31	32%
Actuaciones de traslado*	57	56	0%
Actuaciones previas de investigación	200	206	3%
Procedimientos de ejercicio de derechos	67	84	25%
Procedimientos sancionadores	111	130	17%
Recursos de reposición	86	106	23%
TIEMPO MEDIO	**40**	**43**	**7%**

** Incluye reclamaciones relacionadas con el ejercicio de derechos*

4. Administraciones públicas sancionadas por incumplimiento de requerimientos y medidas

En relación con la eficacia de las actuaciones y resoluciones de la Agencia, la SGID supervisa el cumplimiento de los requerimientos de información realizados al amparo de los poderes de investigación regulados en el artículo 58.1 del RGPD, y de las medidas de adaptación a la normativa impuestas en las resoluciones de conformidad con los poderes correctivos regulados en el artículo 58.2.

La falta de respuesta a los requerimientos de información supone una infracción tipificada en el artículo 83.5.e) del RGPD, calificada como muy grave a efectos de prescripción en el artículo 72.1 de la LOPDGDD.

Por su parte, la falta de acreditación de las medidas correctivas impuestas supone una infracción tipificada en el artículo 83.6 del RGPD, calificada igualmente como muy grave a efectos de prescripción en el artículo 72.1 de la LOPDGDD.

En la tabla siguiente se informade los responsables públicos que han sido sancionados por la Agencia por las infracciones descritas durante el año 2023. De acuerdo con el artículo 77 de la LOPDGDD, se les sanciona declarando la infracción.

Tabla 9: Administraciones Públicas sancionadas por incumplimiento de requerimientos y medidas correctivas

Investigado	Tipo entidad investigada	Artículo infringido	Artículo de tipificación	Resolución
Ayuntamiento de Las Palmas De Gran Canaria	Administración Local	RGPD 58.2	83.6	https://www.aepd.es/documento/ps-00619-2022.pdf
Fundación Pública Andaluza para la Gestión de la Investigación en Salud de Sevilla (Fisevi)	Administración Autonómica	RGPD 58.1	83.5	https://www.aepd.es/documento/ps-00220-2023.pdf
Ayuntamiento de Los Llanos de Aridane	Administración Local	RGPD 58.2	83.6	https://www.aepd.es/documento/ps-00234-2023.pdf
Departamento de Educación, Cultura y Deporte del Gobierno de Aragón	Administración Autonómica	RGPD 58.2	83.6	https://www.aepd.es/documento/ps-00238-2023.pdf
Consejeria de Sanidad de la Junta de Comunidades de Castilla La Mancha	Administración Autonómica	RGPD 58.2	83.6	https://www.aepd.es/documento/ps-00241-2023.pdf

5. Recursos

Los recursos interpuestos frente a resoluciones de los procedimientos de la SGID se muestran a continuación, según hayan sido de reposición, extraordinarios de revisión, o contencioso-administrativos.

Tabla 10: Recursos presentados ante la Agencia			
Tipo de recurso	**2022**	**2023**	**Δ% anual**
Recursos de reposición	898	952	6%
Recursos extraordinarios de revisión	12	16	33%
Recursos contencioso-administrativos	115	128	11%
TOTAL	**1025**	**1.096**	**7%**

El aumento en recursos no resulta sorprendente si se correlaciona con el aumento en el número de resoluciones emitidas por la Agencia.

Los recursos de reposición y revisión resueltos anualmente por la AEPD se muestran en la siguiente tabla. Se puede apreciar un aumento importante en el incremento de recursos resueltos, superior al incremento de recursos presentados ante la Agencia. Esto se debe a que se ha realizado un importante esfuerzo, con algunos cambios organizativos, tendentes a intentar resolver este aumento de los recursos.

Tabla 11: Recursos resueltos			
Tipo de recurso	**2022**	**2023**	**Δ% anual**
Recursos de reposición	735	940	28%
Recursos extraordinarios de revisión	11	18	64%
TOTAL	**746**	**958**	**28%**

6. Clasificaciones

6.1 Reclamaciones planteadas con mayor frecuencia

Se muestran las 10 áreas de actividad con mayor número de reclamaciones recibidas en 2023, que suponen en conjunto algo más del 80% del total de reclamaciones recibidas en el año:

Tabla 12: Reclamaciones más frecuentes

Reclamaciones planteadas con mayor frecuencia	2022	2023	% relativo	Δ% anual
TOP 10	**12.020**	**17.431**	**81%**	**45%**
Publicidad (excepto spam)	2.000	4.279	20%	114%
Servicios de Internet	2.221	2.897	13%	30%
Videovigilancia	2.197	2.843	13%	29%
Comercio, transporte y hostelería	906	1.504	7%	66%
Entidades financieras/acreedoras	767	1.362	6%	78%
Ficheros de Morosidad	1.159	1.263	6%	9%
Reclamación de Deudas	910	975	5%	7%
Sanidad	543	803	4%	48%
Administración pública	796	802	4%	1%
Asuntos laborales	521	703	3%	35%
Otros	**3.108**	**4.159**	**19%**	**34%**
TOTAL	**15.128**	**21.590**	**100%**	**43%**

Destaca sobremanera el aumento de las reclamaciones recibidas con relación a la recepción de publicidad no deseada. Y esto es así a pesar de los esfuerzos que ya se vienen realizando desde la AEPD para favorecer los mecanismos de mediación en este tipo de conflictos. La gran mayoría de estas reclamaciones versan sobre llamadas telefónicas y están relacionadas, principalmente, con el sector de telecomunicaciones o de suministros de agua, gas o electricidad. La aprobación de la nueva regulación sobre las llamadas publicitarias en la Ley 11/2022, de 28 de junio, General de Telecomunicaciones (LGTel), que ha entrado en vigor durante 2023, ha generado un aumento de este tipo de reclamaciones, dado que se han seguido recibiendo este tipo de llamadas, a pesar de que se esperaba un efecto diferente.

En general, y dado el gran incremento en el número de reclamaciones, no es de extrañar que todo el resto de los grupos de actividad también se hayan visto incrementados. Aunque lo hacen especialmente el sector del comercio, transporte y hostelería (+66%) donde son destacables los aumentos de reclamaciones contra empresas de mensajería o paquetería; y el sector de las entidades financieras (+78%), principalmente relacionadas con el ejercicio de derechos.

6.2 Áreas más frecuentes en procedimientos sancionadores

Se muestran las 10 áreas de actividad con mayor número de procedimientos sancionadores finalizados en 2023, que representan el 86% del total de sancionadores resueltos en el año:

Tabla 13: Procedimientos sancionadores más frecuentes

Grupo de actividad	2022	2023	% relativo	Δ% anual
TOP 10	**465**	**419**	**86%**	**-10%**
Videovigilancia	164	164	33%	0%
Servicios de internet	88	70	14%	-20%
Administración Pública	53	31	6%	-42%
Publicidad (spam email/SMS)	29	28	6%	-3%
Contratación fraudulenta	17	27	6%	59%
Telecomunicaciones	11	27	6%	145%
Comercio, transporte y hostelería	21	26	5%	24%
Asuntos laborales	27	18	4%	-33%
Publicidad (excepto spam)	23	14	3%	-39%
Quiebras de seguridad	32	14	3%	-56%
Otros	**110**	**71**	**14%**	**-35%**
TOTAL	**575**	**490**	**100%**	**-15%**

Sigue destacando los procedimientos de videovigilancia, muchos de los cuales están relacionados con comunidades de vecinos o viviendas particulares, seguido de los relacionados con los servicios de Internet, aunque el número de estos procedimientos sancionadores ha bajado con respecto al año anterior. A pesar de que el mayor número de reclamaciones presentadas está relacionado con la publicidad no deseada y de

que la gran mayoría están relacionadas con llamadas del sector de las telecomunicaciones o del de suministros de agua, gas o electricidad, el número de sancionadores relacionados con esta casuística no tiene un porcentaje relativo tan elevado; esto se debe a que en muchos casos los responsables de las llamadas no se encuentran en España o no se les pueden llegar a identificar.

7. Ámbito transfronterizo (EEE)

La aplicación del RGPD desarrolla en su capítulo VII los mecanismos de cooperación entre autoridades de control del Espacio Económico Europeo, en los que es de plena aplicación el Reglamento.

7.1 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 participa 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 respectivamente.

Tabla 14: Casos transfronterizos participados

Papel de la AEPD	2022	2023	Δ% anual
Nuevos casos liderados como autoridad principal	15	25	67%
Nuevos casos en cooperación como autoridad interesada	201	301	50%
TOTAL	**216**	**326**	**51%**

De los casos en los que España ha actuado como autoridad principal, cabe destacar los siguientes procedimientos, por el importe de la multa impuesta:

Tabla 15: Principales casos transfronterizos en los que la Agencia ha sido autoridad principal

Responsable	Infracción	Multa
OPEN BANK, SA	Art. 25 y 32 del RGPD	2.500.000€
GLOVOAPP23, SL	Art. 13, 25, 32, 35 y 5.1.e) del RGPD	550.000€
THE MAIL TRACK COMPANY	Art. 13, 14, 5.1.a) y 6.1 del RGPD	100.000€

Se puede leer más sobre estos y más casos transfronterizos participados como autoridad líder en el apartado “6.2 Reclamaciones y procedimientos más relevantes”.

En cuanto a los casos en los que España ha participado como autoridad interesada, dado su relevancia e importe de la multa interpuesta, cabe destacar los siguientes casos:

Tabla 16: Principales casos transfronterizos en los que la Agencia ha sido autoridad interesada

Responsable	Multa
FACEBOOK IRELAND LIMITED	1.200.000.000€
TIKTOK	345.000.000€
INSTAGRAM	180.000.000€
WHATSAPP INC	5.500.000€

La tramitación de estos procedimientos fue realizada por la autoridad irlandesa, en cooperación con la AEPD y otras autoridades del Espacio Económico Europeo. Las resoluciones han sido publicadas por la autoridad de ese país y se recogen en el **repositorio** del Comité Europeo de Protección de Datos.

7.2 Peticiones 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 autoridades de control, como otras solicitudes de asistencia y consulta recibidas por la AEPD, así como los proyectos de decisión analizados y participados por la AEPD. Las entradas procedentes de otros estados del EEE se estabilizan con un ligero incremento del 1%. Aumentan la entrada de nuevos casos transfronterizos y las consultas procedentes de otras autoridades, pero se reducen los proyectos de decisión de casos en los que la AEPD participa. Puesto que este último supuesto se trata de un proceso complejo que puede durar varios años, el descenso de decisiones en el año depende del inicio de casos en años previos.

Tabla 17: Solicitudes y decisiones recibidas en procedimientos de cooperación

Tipo de entrada	2022	2023	Δ% anual
Casos transfronterizos procedentes de otras AC	651	708	9%
Solicitudes de asistencia de otras AC	311	294	-5%
Consultas de otras AC en procedimientos transfronterizos	48	51	6%
Proyectos de decisión de casos en los que la AEPD participa*	132	99	-25%
Operaciones conjuntas en las que la AEPD participa	0	0	0%
TOTAL	**1.142**	**1.152**	**1%**

** Los proyectos de decisión recibidos, aun siendo emitidos por la principal, suponen el trabajo subsiguiente de negociación y consenso entre todas las autoridades participantes y requieren una gran cantidad de recursos y de esfuerzo.*

7.3 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 hacia el resto de autoridades de control europeas.

El mayor volumen de casos y consultas hacia otras autoridades (+40%) deriva fundamentalmente del aumento de reclamaciones y expedientes tramitados por la SGID en 2023. En cuando a las decisiones lideradas por la AEPD, en este año se han resuelto un mayor número de procedimientos transfronterizos, parte de los cuales se habían iniciado en años anteriores. Los proyectos de decisión emitidos por la AEPD suponen un trabajo adicional de negociación y consenso entre todas las autoridades europeas participantes, que dilata los plazos necesarios para su resolución.

Tabla 18: Solicitudes y decisiones remitidas en procedimientos de cooperación

Tipo de notificación	2022	2023	Δ% anual
Casos transfronterizos compartidos con otras AC	24	64	167%
Solicitudes de asistencia a otras AC	93	102	10%
Consultas a otras AC en procedimientos transfronterizos	18	10	-44%
Proyectos de decisión de casos liderados por la AEPD	25	48	92%
TOTAL	**160**	**224**	**40%**

7.4 Grupos de trabajo internacionales

Además del trabajo de negociación y consenso en cada expediente transfronterizo en el que la Agencia ha participado, la SGID también ha estado presenta en distintas sesiones de grupos de trabajo dependientes del Comité Europeo de Protección de Datos (CEPD).

Tabla 19: Grupos de trabajo europeos con la participación de la SGID

Grupo de trabajo	Propósito
Cooperation Expert Subgroup	Enfocar los procedimientos establecidos por el RGPD a los efectos del mecanismo de cooperación. Orientar sobre cuestiones de procedimiento relacionadas con el mecanismo de cooperación. Prestar asistencia mutua internacional y otras herramientas de cooperación para hacer cumplir el RGPD fuera de la UE (artículo 50 del RGPD).
Enforcement Expert Subgroup	Analizar la necesidad de aclaraciones u orientación adicionales, basadas en experiencias prácticas con la aplicación de los capítulos VI, VII y VIII del RGPD. Evaluar las posibles actualizaciones de las herramientas existentes del subgrupo de cooperación. Realizar un seguimiento de las actividades de investigación. Hacer preguntas prácticas sobre investigaciones. Orientar sobre .la aplicación práctica del Capítulo VII del RGPD, incluidos los intercambios sobre casos concretos. Orientar sobre la aplicación del Capítulo VIII del RGPD junto con el Grupo de Trabajo sobre Multas administrativas. Analizar los procedimientos del artículo 65 y del artículo 66.

Tabla 19: Grupos de trabajo europeos con la participación de la SGID	
Grupo de trabajo	**Propósito**
IT Users Expert Subgroup	Desarrollar y probar herramientas informáticas utilizadas por el CEPD con un enfoque práctico. Recopilar comentarios sobre el sistema de TI por parte de los usuarios. Adaptar los sistemas y manuales. Discutir otras necesidades de negocio, incluidos los sistemas de teleconferencia y videoconferencia.
Taskforce on Administrative Fines	Elaborar directrices para la armonización del cálculo de las multas.
Cookie Banner Taskforce	Intercambiar puntos de vista sobre el análisis jurídico y las posibles infracciones. Prestar apoyo a las actividades a nivel nacional. Agilizar la comunicación.
101 Complaints Taskforce	
Support Pool of Experts	Ayudar a las autoridades de supervisión a aumentar su capacidad para supervisar y hacer cumplir la salvaguarda de los datos personales.
Sistema de Información Schengen –SIS-	Establecer reuniones de coordinación de Sistema de Información Schengen de segunda generación –SIS II-con las autoridades nacionales SIS II en el marco de la planificación de la evaluación Schengen.
Ajuste fino del RGPD	Proponer una adaptación del RGPD en aquellos aspectos relacionados con temas transfronterizos.

8. Multas

8.1 Evolución de las multas impuestas

Las siguientes cifras hacen referencia a las sanciones económicas impuestas en resolución definitiva, con independencia de su estado de ejecución y recaudación:

Tabla 20: Volumen de multas			
Evolución de las multas impuestas	**2022**	**2023**	**Δ% anual**
Número de multas	378	367	-3%
Importe total	20.775.361	29.817.410 €	44%

El importe total aumenta de forma importante con respecto al año anterior, a pesar de la reducción mencionada en el número de procedimientos sancionadores, todo ello por la mayor complejidad de los tratamientos analizados, su mayor alcance, y por tanto mayor impacto de las infracciones. Las multas superiores al millón de euros impuestas a personas jurídicas por resoluciones firmadas en 2023 y que han devenido firmes y ejecutivas son publicadas por la Agencia en el BOE, de conformidad con lo establecido por la LOPDGDD.

Se detallan a continuación:

Tabla 21: Multas superiores al millón de euros en resolución firme y ejecutiva		
Responsable	**Infracción**	**Multa**
BANCO BILBAO VIZCAYA ARGENTARIA, S.A.	Art. 6.1 RGPD, art. 25 RGDP, art 32 RGPD	1.184.000€
CAIXABANK, S.A.	Art. 5.1.f) RGPD, art. 25 RGPD, art. 32 RGPD	5.000.000€
OPEN BANK, SA.	Art. 25 RGPD, art. 32 RGDP	2.500.000€

Hay que resaltar que si bien el número de reclamaciones tiene una tendencia ascendente y un incremento muy fuerte en los últimos años, y que por lo tanto el número de resoluciones que emite la Agencia va en sintonía con ese datos, el importe de las multas no tiene por qué ser ascendente, dado que las multas que se imponen dependen de las infracciones cometidas, de los agravantes que pueda haber y de las personas, físicas o jurídicas, que los hayan cometido, dado que las multas tienen que ser efectivas, proporcionadas y disuasorias, de tal forma que no salga más rentable una sanción por una infracción que la adaptación al cumplimiento de la normativa.

8.2 Áreas con mayor importe global de multas

La siguiente tabla desglosa las 6 áreas de actividad con mayor importe en sanciones en 2023:

Tabla 22: Desglose de multas por temas				
Importe de multas en euros según el tema	**2022**	**2023**	**% relativo**	**Δ% anual**
Seis temas con mayor importe total en 2023	**14.241.901€**	**26.433.600 €**	**89%**	**86%**
Quiebras de seguridad	821.800 €	12.907.000 €	43%	1471%
Entidades financieras / acreedoras	596.200 €	5.321.000 €	18%	792%
Derechos protección datos	5.900 €	2.633.400 €	9%	44534%
Contratación fraudulenta	706.800 €	2.571.500 €	9%	264%
Telecomunicaciones	632.000 €	1.942.000 €	7%	207%
Servicios de Internet	11.479.201 €	1.058.700 €	4%	-91%
Otros	**6.533.460 €**	**3.383.810 €**	**11%**	**-48%**
TOTAL	**20.775.361 €**	**29.817.410 €**	**100%**	**44%**

El gran aumento sancionador en alguno de estos temas con respecto al año anterior se corresponde con multas individuales en procedimientos de gran impacto.

Anexo A: Datos del Canal Prioritario

En 2019 la AEPD creó un sistema específico para perseguir la difusión ilegítima de contenidos especialmente sensibles que pusieran en alto riesgo los derechos y libertades de los afectados, conocido como Canal Prioritario. Adicionalmente, a efectos de facilitar la comunicación de este tipo de casos a los menores de edad, se flexibilizaron los requisitos de sus comunicaciones electrónicas, facilitando un medio de contacto basado en un formulario abierto, sin necesidad de presentar la reclamación mediante un certificado digital.

A.1 Entradas recibidas a través del Canal Prioritario

A continuación, se muestran las entradas recibidas por los dos canales referidos anteriormente.

Tabla 23: Entradas recibidas por el Canal Prioritario

Tipo de entrada	2022	2023	Δ% anual
Reclamaciones presentadas ante la AEPD	255	413	62%
Comunicaciones del canal de menores (14-18 años)	167	159	-5%
TOTAL	**422**	**572**	**36%**

Se puede apreciar el incremento total de reclamaciones recibidas por estos dos tipos de entrada. Llama la atención el descenso que ha habido de las comunicaciones recibidas a través del canal de menores, a pesar de que es una de las infracciones que están aumentando últimamente.

A.2 Entradas tramitadas con carácter de urgencia tras el análisis de la Agencia

Cada entrada que llega a través del Canal Prioritario se analiza en profundidad para determinar si el caso reúne las características para ser tratado como sensible, en cuyo caso se procede a su tramitación con carácter de urgencia. En el resto de los casos, también se puede continuar su tramitación, aunque ya por la vía ordinaria y sin el carácter de urgencia, debido a que, tras el análisis de las mismas, se observa que no tienen relación con el objetivo del Canal. La siguiente tabla muestra las entradas que, después de dicho análisis, fueron canalizadas por el canal urgente.

Tabla 24: Entradas tratadas por vía urgente

Tipo de entrada	2022	2023	Δ% anual
Reclamaciones recibidas por el Canal Prioritario	33	29	-12%
Reclamaciones recibidas por canales ordinarios	10	7	-30%
Comunicaciones del canal de menores (14-18 años)	17	5	-71%
TOTAL	**60**	**41**	**-32%**

Se puede observar la gran diferencia que existe con relación a la tabla anterior. Muchas reclamaciones se presentan a través de este canal, puede que para que se traten de manera urgente. Sin embargo, el análisis previo que se realiza en el Agencia permite discriminar y tratar de manera urgente sólo aquellos casos en los que se están difundiendo un contenido sensible sin consentimiento que pueda afectar gravemente a los derechos y libertades de los afectados.

A.3 Intervenciones realizadas con carácter de urgencia

Cuando se determina la naturaleza especialmente sensible de los datos personales divulgados y la afectación grave a los derechos y libertades de las personas y pueda causar un daño irreparable, puede resultar necesario y proporcionado realizar una intervención de urgencia para adoptar medidas provisionales que permitan salvaguardar el derecho fundamental a la protección de los datos personales de los afectados.

En tales casos, se requiere a los responsables la retirada de los contenidos sensibles con la mayor inmediatez posible. En el caso de no poder identificar al responsable se realiza esa petición a los proveedores de servicios correspondientes. En la siguiente tabla se muestra el número de intervenciones realizadas con carácter de urgencia y los casos en los que han resultado ser eficaces, retirándose los contenidos expuestos.

Tabla 25: Intervenciones de retirada de contenidos

Tipo de Actuación	2022	2023	Δ% anual
Intervenciones con carácter de urgencia para la retirada de contenidos	**51**	**36**	**-29%**
Medidas cautelares adoptadas	31	26	-16%
Solicitudes de retirada urgente enviadas	20	10	-50%
Intervenciones que han resultado eficaces	**46**	**34**	**-26%**
Medidas cautelares que han resultado eficaces	28	24	-14%
Solicitudes de retirada urgente que han resultado eficaces	18	10	-44%

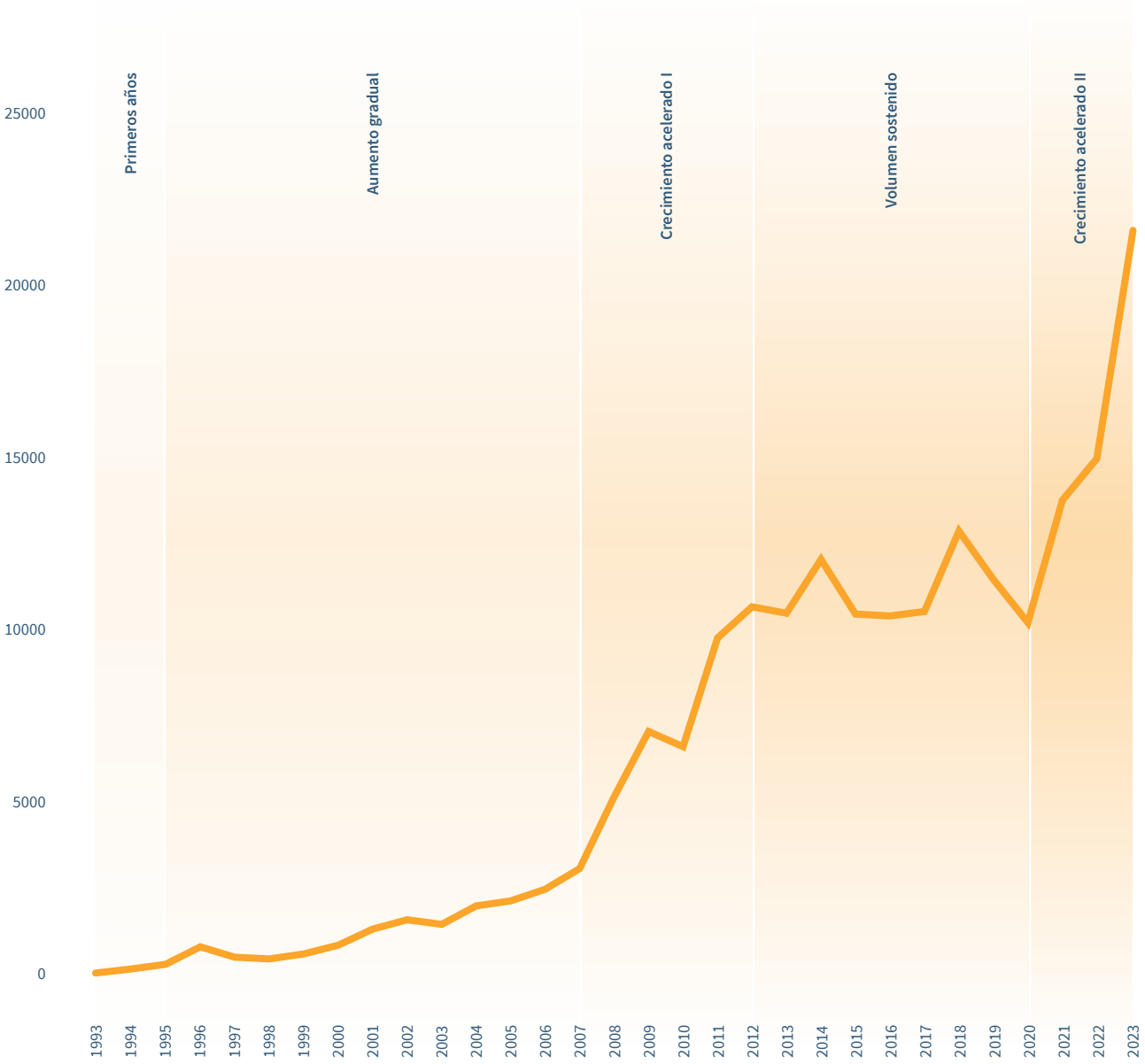
Se ha de notar que las dos medidas cautelares que no han resultado eficaces en el año se firmaron durante los últimos días de 2023, por ello a final de año figuran pendientes de cumplimiento. No obstante, estas medidas se cumplieron durante los primeros días de 2024, las medidas cautelares han resultado eficaces en un 100%.

Anexo B: Evolución de las reclamaciones 1993-2023

En este año que la Agencia cumple 30 años de historia, se presenta a continuación un breve recorrido de la actividad de las SGID a través del análisis de las reclamaciones que tramita. La evolución de las reclamaciones presentadas son un claro reflejo de la propia evolución de la protección del derecho fundamental a la protección de datos personales, tanto en la creciente sensibilización de los ciudadanos, poderes públicos y agentes sociales y económicos respecto de su trascendencia social e individual, como del alcance y diversidad de tratamientos que afectan al mismo.

El crecimiento de las reclamaciones ha sido constante en estos 30 años, pero han sido dos los períodos de crecimiento más acentuado que han llevado el número de reclamaciones a nuevos niveles, el segundo aún abierto a fecha de cierre de esta Memoria.

Gráfico 3: Reclamaciones presentadas en la AEPD



Primeros años (1993-1995)

Aun cuando los primeros escritos conteniendo reclamaciones o denuncias en materia de protección de datos se remontan a finales del año 1993, puede afirmarse que la Subdirección General de Inspección de Datos comienza a tener una actividad significativa en materia de supervisión de derechos e instrucción de procedimientos sancionadores en 1994. Este año supone un avance significativo desde el punto de vista de la aplicación de la Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD). Durante el mismo se ha hecho realidad la presencia de la Agencia de Protección de Datos como tal, se la ha dotado de la necesaria infraestructura tanto presupuestaria como de edificio y personal, y se han diseñado los servicios de la Inspección. Asimismo, en 1994 finaliza el plazo de inscripción inicial de ficheros en el Registro General de Protección de Datos.

De esta manera, en 1994 se recibieron 81 reclamaciones, subiendo a 334 en 1995, primer año completo en el que se consolida la actividad de la Inspección.

En estos primeros años, la mitad de las reclamaciones recibidas describen infracciones relacionadas con los datos de naturaleza económico-financiera (y, entre ellos, especialmente, los relativos a la solvencia, el crédito y la morosidad). También se recibe un volumen importante de reclamaciones en relación con la publicidad no deseada, tanto la realizada por empresas para la promoción y venta de productos a sus propios clientes como la realizada en la prestación de servicios de esta naturaleza a otras empresas.

Aumento gradual (1996-2007)

El volumen de reclamaciones iría aumentando en los años siguientes de forma gradual, a un ritmo medio de alrededor del 25% anual, al tiempo que se va consolidando la actividad de la Agencia y profundizándose el marco normativo.

El año 2000 es un año marcado en materia de protección de datos, por dos hechos de especial trascendencia. La entrada en vigor de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD), en el mes de enero que, sustituyendo a la LORTAD, se convierte en el principal texto normativo sobre la materia en nuestro país, y la Sentencia del Tribunal Constitucional 292/2000, de fecha 30 de noviembre, por la que el órgano supremo de interpretación de nuestra Constitución viene a definir el derecho a la protección de datos como un derecho independiente en nuestro sistema constitucional.

Las reclamaciones recibidas superan por primera vez el millar en 2001, continuando ese crecimiento gradual hasta las 3.000 en 2007.

Los ficheros de solvencia y morosidad y el marketing directo continúan ocupando las preocupaciones de los ciudadanos durante los años finales del siglo XX. Sin embargo, ya durante el año 2000 fueron muy numerosas las actuaciones de inspección realizadas en relación con actividades desarrolladas en el seno de Internet, iniciadas como consecuencia de las denuncias presentadas por los ciudadanos, cada vez más preocupados por la incidencia que la Red puede tener en la protección de su propia intimidad. En este sentido, el objeto de las denuncias versaba principalmente sobre la publicación indebida de datos personales, la remisión de mensajes a través del correo electrónico o la utilización de los datos recabados por Internet para finalidades distintas a la que ocasionó su recogida. En la primera década del siglo XXI van naciendo nuevos servicios online e incrementándose las reclamaciones recibidas por la incidencia de estas nuevas tecnologías en la privacidad de los ciudadanos: la difusión de datos en Internet a través de eMule, la difusión de imágenes en YouTube, las políticas de conservación de datos de los motores de búsqueda y el correo electrónico en Internet son algunas de las principales áreas de reclamación en este ámbito.

También comienzan a recibirse en número importante denuncias acerca de tratamientos realizados por operadores de telecomunicaciones, sector que mantiene una parte relevante de las preocupaciones de los ciudadanos en los años siguientes, siendo en el 2002 el sector con mayor número de reclamaciones, por encima de las relacionadas con los ficheros de solvencia y morosidad. El problema más significativo que se plantea en estos años en el sector de telecomunicaciones es el relacionado con la preasignación de líneas telefónicas para la prestación del servicio por otro operador, llevada a cabo sin conocimiento ni consentimiento del afectado.

También merecen especial atención las resoluciones dictadas en respuesta a denuncias respecto del tratamiento de datos de salud. De todas las categorías de datos calificados por la LOPD como datos especialmente protegidos, son los de salud los que suscitan mayores problemas en cuanto a su protección. Las reclamaciones más habituales son las relacionadas con las medidas de seguridad exigibles y con el deber de secreto sobre las informaciones relacionadas con la salud de las personas.

A partir de 2004, comienzan a destacar las reclamaciones relacionadas con un ámbito que crecerá de forma importante en los años siguientes: la videovigilancia. En 2007, tras experimentar un crecimiento del 412% con respecto al año anterior, se convierten en uno de los tipos de reclamación más frecuentes, impulsado por el incremento exponencial de la instalación de cámaras de videovigilancia por razones de seguridad. Esta actividad era habitualmente desarrollada por las Fuerzas y Cuerpos de Seguridad del Estado en el ámbito de su regulación específica, así como por entidades financieras, y en estos años se extiende a otros sectores y a particulares. Son especialmente significativos los datos relativos a los titulares de ficheros de videovigilancia: tras los sectores de turismo y hostelería, el comercio y la sanidad, aparecen las comunidades de propietarios.

Crecimiento acelerado I (2008-2012)

La importancia de las funciones encomendadas a la Agencia, su mayor presencia en la sociedad, la atribución de nuevas competencias y el incremento experimentado en su actividad hacen que, desde 2008 a 2012, el ritmo de entrada de reclamaciones se acelere con incrementos en algunos años del 50%, y superándose por primera vez las 10.000 reclamaciones recibidas en 2012.

En 2008 el Centro de Investigaciones Sociológicas (CIS) incluyó en su barómetro de febrero un cuestionario dirigido a evaluar la concienciación ciudadana sobre la protección de datos personales, arrojando como resultado que más de un 70% de los ciudadanos en España se mostraba preocupado por la protección de datos y el uso de información personal. Asimismo, el barómetro del CIS reflejaba que el 52,4% de los ciudadanos españoles afirmaba conocer la existencia de una ley que les protege contra posibles abusos que puedan producirse con sus datos personales, y situaba en un 64% el porcentaje de los ciudadanos que aseguraba tener conocimiento de la existencia de la AEPD como organismo encargado de la defensa de sus derechos.

En estos años se produce también un crecimiento de las reclamaciones para tutelar el ejercicio de los derechos de los ciudadanos incluidos en la LOPD (Acceso, Rectificación, Cancelación y Oposición), especialmente los de Acceso (2 de cada 10) y Cancelación (7 de cada 10). En 2008, los procedimientos para la tutela de derechos iniciados por reclamaciones de los ciudadanos se incrementaron en un 88%, y en 2011, hasta un 35% de las reclamaciones recibidas solicitaban la tutela del ejercicio de alguno de los derechos. Este porcentaje iría reduciéndose en los años siguientes.

Las denuncias más frecuentes en este periodo siguen haciendo referencia a los sectores de telecomunicaciones, los servicios financieros y ficheros de solvencia, y a la videovigilancia. Este último se consolida como un fenómeno en claro aumento.

Por otra parte, continúa el crecimiento del ámbito de Internet, que supone el cuarto ámbito en volumen de reclamaciones por detrás de los tres señalados. La evolución de la web 2.0 multiplica la oferta de nuevos servicios que están teniendo una acogida masiva entre los usuarios de Internet (buscadores, redes sociales, ...). Estos servicios se interrelacionan entre sí de forma que las posibilidades de obtener y tratar información personal aumentan de forma vertiginosa. El "derecho al olvido" en Internet se erige en uno de los más intensos temas de debate en el entorno de los nuevos servicios de Internet, hasta su identificación por la jurisprudencia del TJUE en 2014.

Volumen sostenido (2013-2020)

Desde 2013 a 2020 el volumen de reclamaciones se mantiene en torno a esa cifra de 10.000 reclamaciones, con una clara excepción en 2018, año en el que empieza a aplicarse el RGPD, lo que supone una clara promoción del derecho a la protección de datos, y el nacimiento de nuevos derechos y obligaciones, recibiéndose ese año más de 13.000 reclamaciones, un 22% más que el año anterior.

La aplicación del RGPD también trajo consigo nuevos ámbitos de actuaciones: las reclamaciones transfronterizas por el mecanismo de ventanilla única y la consecuente necesidad de cooperación entre autoridades europeas, y las investigaciones de violaciones de seguridad que afectan a los datos personales, que deben ser notificadas a la Agencia.

También se inicia en 2019 el Canal Prioritario de la Agencia, para dar respuesta urgente en caso de difusión ilegítima de contenidos sensibles, cuando afecten gravemente a los derechos y libertades o puedan producir perjuicios de muy difícil reparación.

Gracias a la intervención de la Agencia se logra, en unos plazos muy reducidos, la retirada de fotografías y vídeos de contenido sexual o violento que se visualizan a través de internet sin consentimiento de los afectados, muchas veces pertenecientes a colectivos vulnerables.

Telecomunicaciones, servicios financieros, videovigilancia y servicios de internet continúan siendo los ámbitos en los que se producen mayor número de reclamaciones.

El año 2020 se verá fuertemente influido por la epidemia de Covid19 y la suspensión de plazos administrativos, volviendo al entorno de las 10.000 reclamaciones. En este año se recibió un número relevante de reclamaciones relacionadas con la conciliación de la garantía de la asistencia sanitaria y el control de la pandemia con el derecho fundamental a la protección de datos personales.

Crecimiento acelerado II (2021-2023)

El último trienio ha venido marcado por una nueva fase de crecimiento explosivo de las reclamaciones, finalizando 2023 con un volumen que será cercano a las 22.000 reclamaciones, por tanto, más del doble que solo tres años antes.

En estos años las reclamaciones más frecuentas pasan a ser las relacionadas con los servicios de Internet, seguidas de las de videovigilancia y de las relacionadas con la publicidad. Entre estos tres ámbitos se acumulan el 40% de las reclamaciones recibidas en la Agencia.

En respuesta al alto número de reclamaciones por recepción de publicidad no deseada, la AEPD ha aprobado la modificación del código de conducta sobre tratamiento de datos en la actividad publicitaria promovido por Autocontrol, que recoge una vía para resolver de forma más ágil las reclamaciones en materia de protección de datos y publicidad que puedan plantear los ciudadanos, y al que se han adherido, entre otros, los principales operadores de telecomunicaciones del país.

En el ámbito de Internet, cobran cada vez mayor trascendencia los riesgos que sobre los menores supone el tratamiento de sus datos en redes sociales y en páginas web, entre ellas especialmente las dirigidas a público mayor de edad por la falta de un control de acceso efectivo. De acuerdo con los últimos datos publicados por el Instituto Nacional de Estadística (INE), por primera vez en España la proporción de niños de 10 a 15 años que disponen de teléfono móvil ha superado los 7 de cada 10, y el 95% han entrado en internet en los últimos tres meses. Por ello no es de extrañar que el número de reclamaciones en los que se ve afectado el derecho a la protección de datos de un menor en Internet ha ido en aumento, multiplicándose por dos de 2021 a 2023.

Las reclamaciones por el tratamiento de datos biométricos no son aún muy numerosas en datos absolutos, pero también están en claro crecimiento, habiéndose triplicado en estos dos años, principalmente por su uso en sistemas de verificación de identidad para el acceso a todo tipo de instalaciones, especialmente en el ámbito laboral y relacionadas con el control de jornada.

También destaca el importante aumento de las reclamaciones recibidas sobre comercio, transporte y hostelería y, dentro de este ámbito, el aumento de infracciones reclamadas relacionadas con el uso de datos personales por parte de empresas de reparto y paquetería;

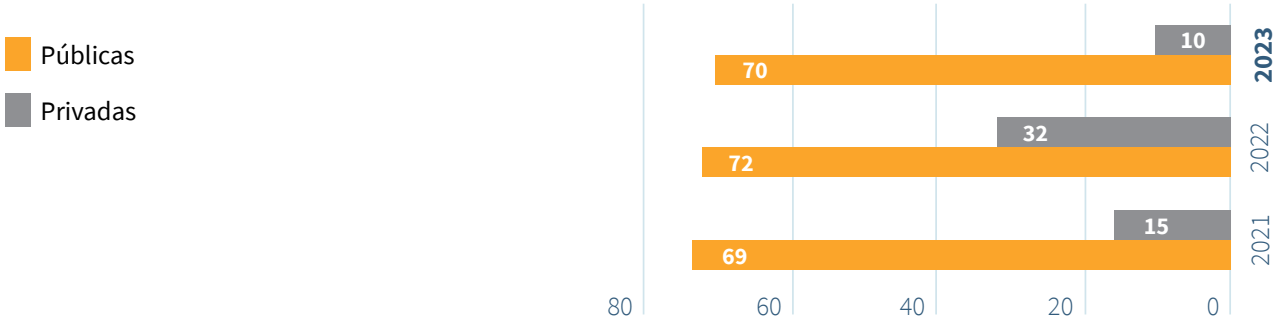
Por último, cabe reseñar un aumento también relevante en reclamaciones sobre contratación fraudulenta, que atañen principalmente a los sectores energético y de telecomunicaciones.

2. Gabinete Jurídico

Consultas

	Administraciones Públicas
AGE	47
CCAA	3
Entidades locales	1
Empresas públicas	3
Otros Organismos	16
TOTAL 1	**70**
	Consultas Privadas
Asociaciones y Fundaciones	1
Empresas	9
Particulares	0
Sindicatos	0
Otros	0
TOTAL 2	**10**
TOTAL	**80**

Evolución de consultas



Evolución de consultas por sectores (2022-2023)		
	2022	2023
Administraciones Públicas	72	**61**
Sanidad / Salud Pública	1	**5**
Particulares	1	**0**
Telecomunicaciones	24	**8**
Asesoría y consultoría	0	**0**
Sindicatos	0	**0**
Servicios informáticos	0	**0**
Asociaciones empresariales	0	**0**
Asociaciones y fundaciones	3	**1**
Solvencia patrimonial	0	**1**
Servicios	0	**0**
Agua y energías	0	**0**
Seguridad	0	**0**
Transporte	0	**0**
Servicios financieros	1	**1**
Investigación	1	**0**
Servicios de mensajería	0	**2**
Seguros	1	**2**
Partidos políticos	1	**0**
Comunidades de propietarios	0	**0**
Industria y construcción	0	**0**
Educación	2	**2**

Nota: Existen consultas que versan sobre más de un sector y son clasificadas en el que más relevancia tengan. Asimismo otras categorías están en desuso y tienden a desaparecer se mantienen en términos comparativos con el ejercicio anterior. Se han añadido nuevas que en el ejercicio anterior tienen 0.

Evolución de consultas por materias (2021-2022)		
	2022	2023
Conceptos Generales*	49	**49**
Ámbito de Aplicación	4	**1**
Licitud	11	**15**
Derecho de Información y Transparencia	26	**9**
Finalidad	3	**0**
Minimización y Proporcionalidad	16	**5**
Exactitud/Calidad de datos	6	**0**
Plazo de Conservación	1	**1**
Integridad y Confidencialidad	0	**0**
Consentimiento	10	**4**
Interés Legítimo	1	**0**
Responsable	4	**2**
Encargado	1	**1**
Corresponsable	0	**1**
Derechos	3	**3**
Tratamientos Videocámaras	0	**1**
Categorías Especiales de datos	14	**13**
Seguridad en el Tratamiento	3	**0**
Responsabilidad Activa	0	**0**
Delegado Protección Datos	3	**3**
Gestión Riesgo y Evaluación de Impacto	2	**0**
Transferencias Internacionales	0	**0**
Transparencia y acceso a registros públicos	0	**6**

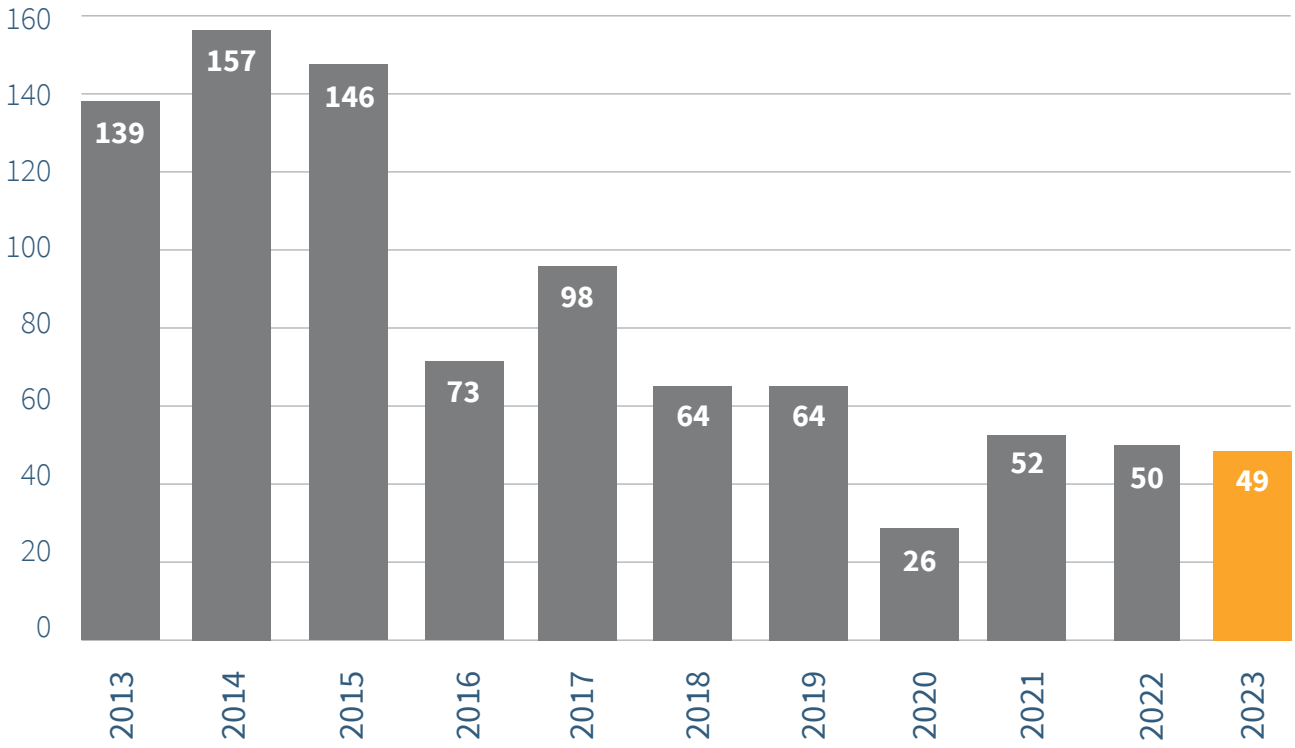
** **Conceptos Generales:** se incluyen aquí las consultas sobre proyectos de disposiciones generales.*

Evolución de consultas por materias (2022-2023)		
	2022	2023
Telecomunicaciones	24	**12**
Menores	0	**4**
Administración electrónica	0	**0**
Estadística	0	**0**
Códigos de Conducta	3	**1**

Nota: Existen consultas que versan sobre más de una materia y que por su relevancia constan en más de un apartado.

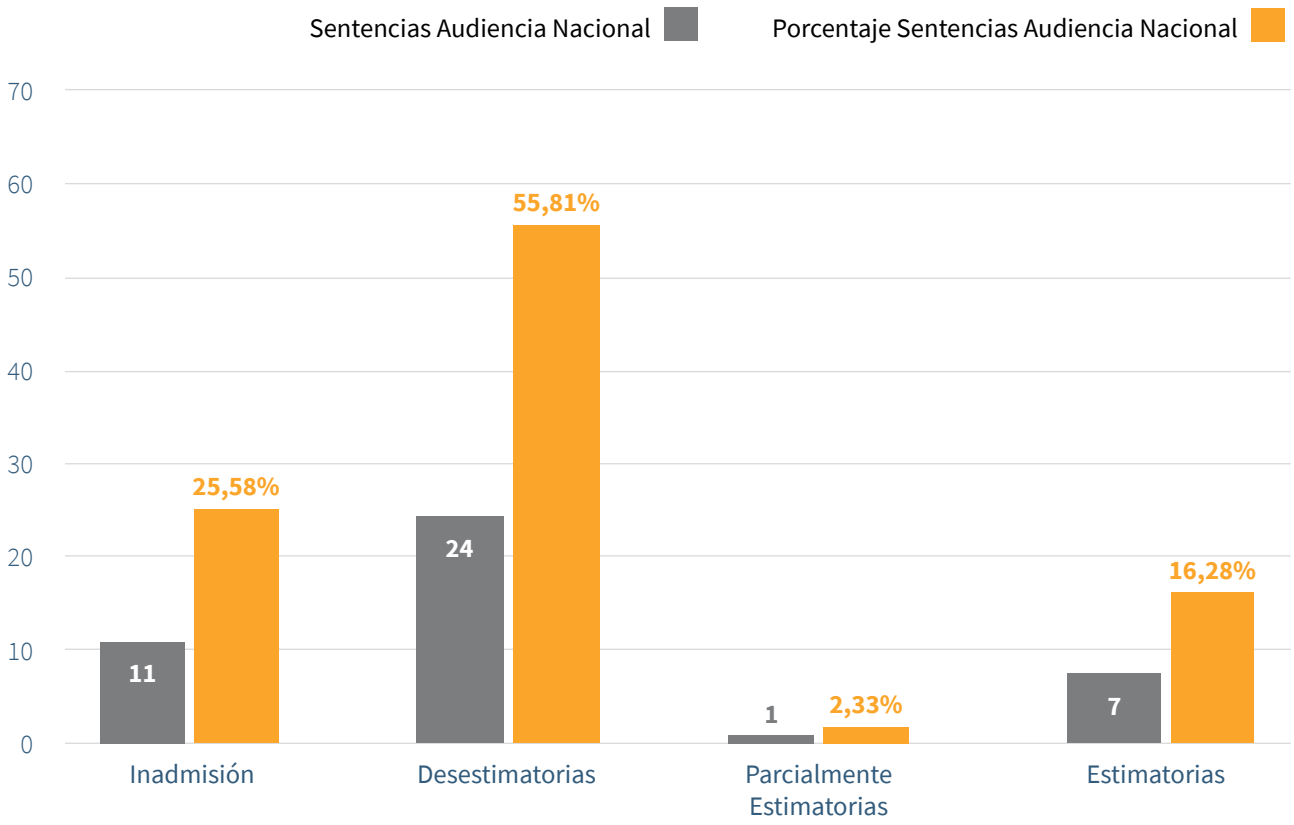
Evolución de informes preceptivos a disposiciones generales (2013-2023)

Disposiciones Generales



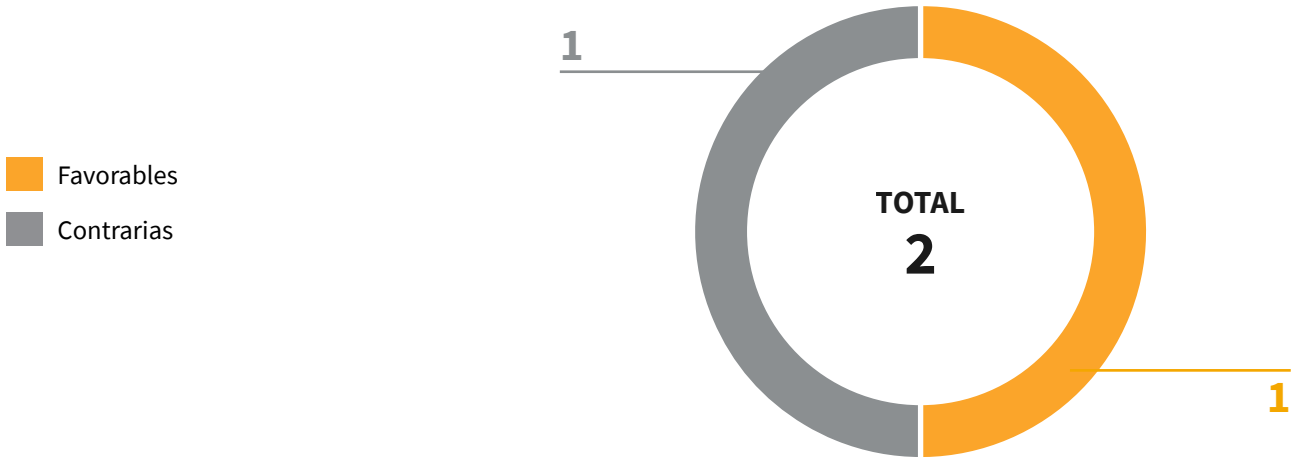
Evolución informes preceptivos (2013-2023)			
Año	Disposiciones generales	RD 424/2005	Total
2013	139	21	162
2014	157	23	182
2015	146	15	173
2016	73	23	97
2017	98	28	126
2018	64	24	88
2019	64	12	76
2020	26	15	41
2021	52	5	57
2022	50	24	74
2023	**49**	**8**	**57**

Sentencias Audiencia Nacional 2023



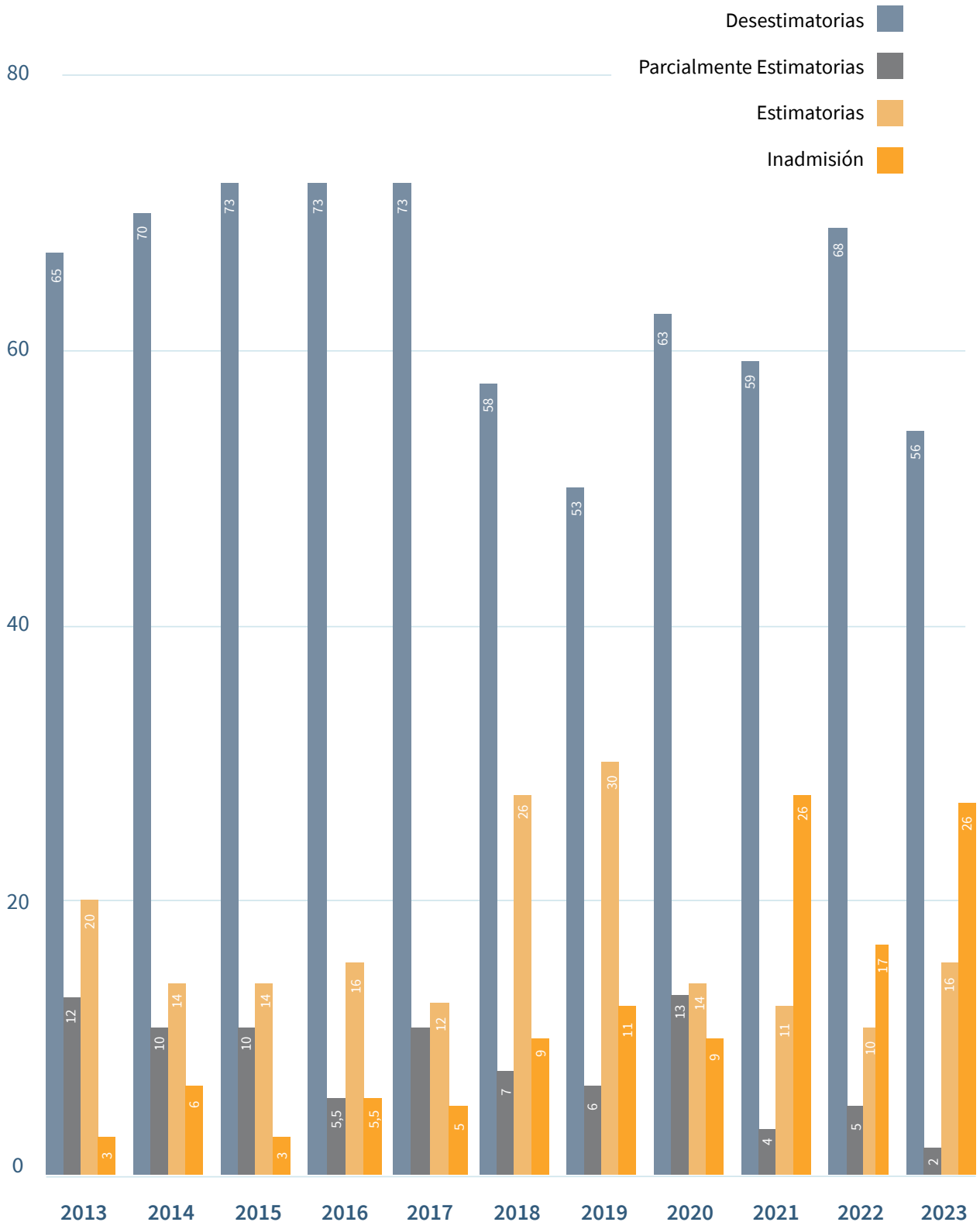
TOTAL Sentencias Audiencia Nacional	**43**

Sentencias Tribunal Supremo (2023)



Evolución por sentido del fallo en porcentajes (2013-2023)				
Ejercicio (año)	Desestimatorias	Parcialmente Estimatorias	Estimatorias	Inadmisión
2013	65	12	20	3
2014	70	10	14	6
2015	73	10	14	3
2016	73	5,5	16	5,5
2017	73	10	12	5
2018	58	7	26	9
2019	53	6	30	11
2020	63	13	14	9
2021	59	4	11	26
2022	68	5	10	17
2023	**56**	**2**	**16**	**26**

Evolución por sentido del fallo en porcentajes (2013-2023)



Comparativa por sector recurrente (2022-2023)		
	2022	2023
Particulares	50	**42**
Banca y seguros	1	**2**
Telecomunicaciones	5	**2**
Solvencia patrimonial y crédito	1	**0**
Distribución y venta	2	**0**
Agua y energía	4	**3**
Administraciones Públicas	2	**0**
Otros	2	**6**
Asociaciones y sindicatos	0	**2**
Sociedad de la información	0	**2**
Publicidad y prospección comercial	2	**0**
Salud	0	**4**
TOTAL	**69**	**63**

Nota: Se incluyen todo tipo de resoluciones de la Audiencia Nacional y el Tribunal Supremo, sentencias, autos, providencias, diligencias de ordenación, etc.

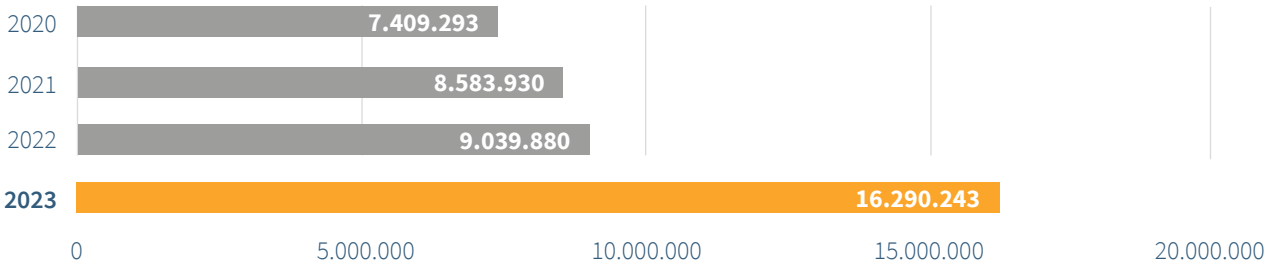
3. Atención al ciudadano y sujetos obligados

Consultas totales planteadas ante el área de Atención al Ciudadano				
	2021	2022	2023	% 2022-2023
Presenciales	64	110	189	71,82%
Telefónicas	41.022	42.562	46.958	10,33%
Sede electrónica y email	3.779	3.766	4.397[1]	16,76%
Consultas servicio Chatbot[2]			17.337	
TOTAL	**44.865**	**46.438**	**68.881**	**48,33%**

[1] Incluye las consultas del canal de atención al ciudadano (3.411); así como las quejas y sugerencias atendidas conforme al Real Decreto 51/2005, de 29 de julio, por el que se establece el marco general para la mejora de la calidad en la Administración General del Estado (136); y también las consultas del canal DPD (850).

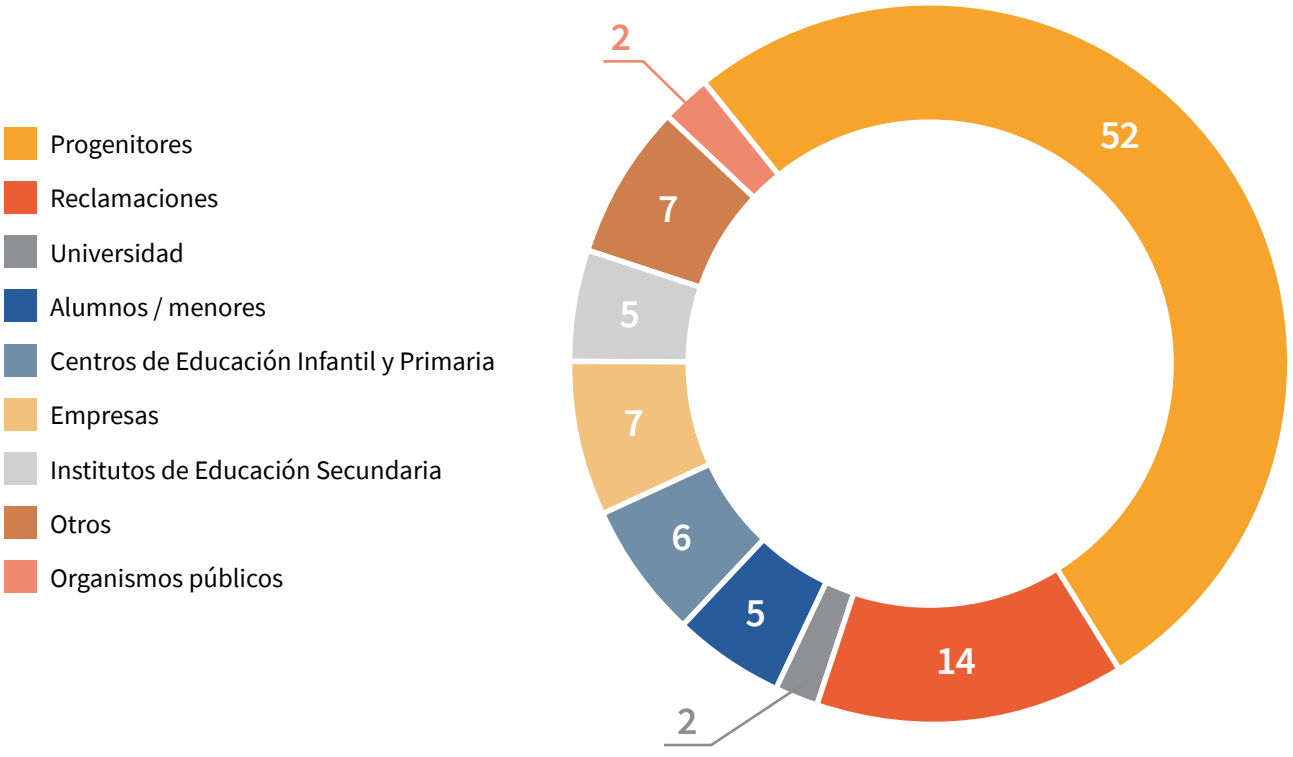
[2] Es un servicio permanente (24x7) de respuesta inmediata con posibilidad de derivar a un agente. Disponible en la web desde el 12 de abril de 2023.

Comparativa de visitas a la web (*www.aepd.es*)					
	2020	2021	2022	2023	% 2022-2023
Nº de visitas	7.409.293	8.583.930	9.039.880	16.290.243	80,20%



Consultas específicas sobre el tratamiento de datos de menores				
	2021	2022	2023	% 2022-2023
Teléfono	564	1.243	2.029	63%
WhatsApp	624	607	1.374	126%
Correo-e	366	362	427	18%
Sede electrónica	235	156	219	40%
TOTAL	**1.789**	**2.368**	**4.049**	**71%**

Consultas por categorías[3] (en porcentajes)



[3] Este gráfico está elaborado con las consultas recibidas en el Área de Educación y Menores, a través del correo de Canal Joven y Sede electrónica.

Accesos a la web www.tudecideseninternet.es	
	2023
Número de visitas	83.364

Canal del DPD				
Consultas	2021	2022	2023	% 2022-2023
	669	695	850[4]	22,30%

[4] *A través de la sede electrónica (718) y derivadas de otros canales (132).*

Informe de Accesos a FAQ	
	Nº de visitas
Reglamento General de Protección de Datos. (RGPD)	178.152
Cuestiones sobre la sede electrónica	124.322
Menores y educación	7.186
Delegado de Protección de Datos	66.318
Tratamiento de datos en el Ámbito Laboral	62.015
Reclamaciones ante AEPD y ante otros organismos competentes	60.387
Comunidades de Propietarios	57.242
Tus Derechos (Información, Acceso, Rectificación y Cancelación)	56.639
Solvencia patrimonial (ficheros de morosos)	50.792
Videovigilancia	47.161
Transferencias internacionales, BCR y Códigos de conducta	34.430
Transparencia y protección de datos	29.204
Redes sociales, difusión ilegítima de contenidos sensibles	22.564
Salud	21.371
Procesos electorales	20.287
Publicidad no deseada	12.142
TOTAL	**910.212**

Áreas temáticas	
Áreas de actuación	**Nº de visitas**
Internet y redes sociales	164.694
Un móvil es más que un móvil	106.643
Canal prioritario	90.819
Publicidad no deseada	84.952
Salud	84.832
Educación y Menores	83.364
Videovigilancia	68.676
Reclamaciones de telecomunicaciones	65.563
Administraciones públicas	65.452
Innovación y tecnología	32.084
Violencia de género	30.800

Temas más consultados en la atención telefónica			
Orden	Temas de consulta	2022	2023
1	Reclamaciones	10.023	**11.570**
2	Reglamento general de protección de datos (RGPD)	7.272	**8.211**
3	Derechos	5.294	**5.503**
4	Videovigilancia	3.431	**3.965**
5	Ficheros de solvencia patrimonial	1.939	**1.898**
6	Comunidades de propietarios	1.043	**1.239**
7	Herramienta FACILITA	1.254	**1.180**
8	Delegados de Protección de Datos	1.137	**1.089**
9	Cuestiones técnicas de la sede electrónica	1.220	**1.023**
10	Tratamiento de datos en el ámbito laboral	468	**630**
11	Transparencia y Protección de Datos	91	**77**
12	Otras cuestiones	3.476	**3.875**

Canal de consulta-web con respuesta inmediata 24 horas | CHATBOT			
Orden	Categorías de consulta	2023	%
1	Reclamaciones ante la AEPD	3.289	18,97
2	Tus derechos	2.750	15,86
3	Publicidad no deseada	2.122	12,24
4	Reglamento general protección de datos	1.948	11,24
5	Videovigilancia	1.653	9,53
6	Internet y redes sociales	1.421	8,2
7	Ficheros de morosos	1.199	6,92
8	Protección de datos en el ámbito laboral	1.112	6,41
9	Comunidades de propietarios	747	4,31
10	Educación y menores	549	3,17
11	Salud	547	3,16

Otros contenidos	
Guías	**Descargas**
La guía que no viene con el móvil	**425.422**
Guía sobre el uso de las cookies	**350.064**
Guía sobre el uso de videocámaras para seguridad y otras finalidades	**84.516**
Gestión del riesgo y evaluación de impacto en tratamientos de datos personales	**62.670**
Compra segura en INTERNET - Guía Práctica	**59.222**
Guía para el responsable de tratamiento de datos personales	**55.463**
Guía de Privacidad y Seguridad en Internet	**53.531**
Guía para la gestión y notificación de brechas de seguridad	**52.249**
Guía para pacientes y usuarios de la Sanidad	**48.772**
Guía para el cumplimiento del deber de informar	**46.005**
Directrices para la elaboración de contratos entre responsables y encargados del tratamiento	**42.367**
La protección de datos en las relaciones laborales	**42.306**
Guía sobre tratamientos de control de presencia mediante sistemas biométricos	**41.864**
Guía de Protección de Datos por Defecto	**40.277**
Guía para el ciudadano	**38.788**
Protección de datos y Administración Local	**35.436**
Guía de protección de datos y prevención de delitos	**27.529**
Información para proyectos del «sandbox» para la transformación digital del sistema financiero	**26.005**
Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial	**22.796**
Guía de Privacidad desde el diseño	**21.124**
Orientaciones y Garantías en los procedimientos de anonimización	**20.765**

Otros contenidos	
Guías	**Descargas**
Listado de elementos para el cumplimiento normativo	**19.108**
Guía de administradores de fincas	**16.176**
Guía para profesionales del sector sanitario	**15.222**
Código de buenas prácticas en protección de datos para proyectos Big Data	**15.158**
Informe utilización por profesores y alumnos de aplicaciones que almacenan datos en nube	**14.630**
Drones y Protección de Datos	**13.791**
Guía para clientes que contraten servicios de Cloud Computing	**13.238**
Requisitos para Auditorías de Tratamientos que incluyan IA	**11.422**
Aproximación a los espacios de datos desde la perspectiva del RGPD	**9.547**
Guía de protección de datos y prevención de delitos: fichas prácticas	**9.492**
Guía de Privacidad desde el diseño (versión en inglés)	**9.152**
Guía de Tecnologías y Protección de Datos en las AA.PP	**9.106**
10 malentendidos relacionados con la anonimización	**8.640**
Guía para la gestión y notificación de brechas de seguridad (versión en inglés)	**8.636**
La protección de datos como garantía en las políticas de prevención del acoso: recomendaciones de la AEPD	**8.251**
Orientaciones para la validación de sistemas criptográficos en la protección de datos	**8.184**
Orientaciones para la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo	**6.911**
Orientaciones sobre cookies y analítica web en portales de las administraciones públicas	**6.893**
Orientaciones para tratamientos que implican comunicación de datos entre Administraciones Públicas ante el riesgo de brechas de datos personales	**6.510**
Cómo gestionar una fuga de información en un despacho de abogados	**6.105**

Otros contenidos	
Guías	**Descargas**
Risk Management and Impact Assessment in the Processing of Personal Data	**5.280**
10 Malentendidos sobre el Machine Learning (Aprendizaje Automático)	**5.256**
RGPD compliance of processings that embed Artificial Intelligence An introduction	**5.218**
Guía sobre el uso de las cookies (versión en inglés)	**4.718**
Audit Requirements for Personal Data Processing Activities involving AI	**4.606**
Decálogo de Principios. Verificación de edad y sistemas de protección de personas menores de edad ante contenidos inadecuados	**3.592**
Orientaciones para prestadores de servicios de Cloud Computing	**3.578**
Guidelines for Data Protection by Default	**2.976**
Drones y Protección de Datos (versión en inglés)	**2.185**
Criterios de acreditación para los organismos de supervisión de códigos de conducta	**1.920**
Technologies and Data Protection in Public Administrations	**1.598**
10 Misunderstandings about Machine Learning	**1.486**
10 Misunderstandings Related to Anonymisation	**1.431**
Guidelines for conducting a data protection impact assessment in regulatory development	**1.346**
Roadmap to ensure compliance with data protection regulation	**905**
FAQ de las pruebas de concepto sobre sistemas de verificación de edad (publicada en la web el 14/12/23)	**741**
Guidelines on Cookies and Web Analytics in Public Administration Websites	**708**
Decalogue of principles. Age verification and protection of minors from inappropriate content (publicada en la web el 18/12/23)	**88**
Frequently Asked Questions about the Proofs of Concept of systems for age verification (publicada en la web el 18/12/23)	**83**
Technical note with the description of the Proofs of Concept of Systems for Age Verification (publicada en la web el 18/12/23)	**67**

Otros contenidos	
Infografías	**Descargas**
Responsabilidad de los y las menores (y de sus padres y madres) por los actos cometidos en Internet	**297.657**
Información sobre consentimiento para tratar datos personales de menores de edad	**55.914**
Decálogo para el personal sanitario y administrativo	**23.659**
Criterios para el tratamiento de datos personales en centros educativos	**23.522**
Cuándo y cómo se debe comunicar una brecha de datos a los afectados	**22.881**
Cuáles son tus derechos de protección de datos	**19.833**
Plan digital familiar	**16.801**
Mapa de referencia para tratamientos que incluyen Inteligencia Artificial	**15.170**
Quién es quién en el tratamiento de datos personales en tu centro educativo	**11.215**
Actuación del coordinador/a de bienestar y protección del alumnado	**11.150**
¿Cómo afectan las pantallas a la salud?	**9.268**
Recomendaciones para usuarios en la utilización de chatbots con Inteligencia Artificial	**9.128**
Los derechos que tienes para proteger tus datos personales	**8.109**
¿Qué debes tener en cuenta antes de dar un teléfono móvil a tu hijo o hija?	**7.741**
Infografía Protección del menor en Internet	**7.101**
Canal prioritario para comunicar la difusión de contenido sensible y solicitar su retirada	**4.924**
Riesgos asociados a sistemas de verificación de edad y resumen del decálogo de principios	**4.803**
Infografía: Medidas para minimizar el seguimiento en internet	**3.468**
10 consejos básicos para comprar en internet de forma segura	**3.292**
Riesgos del internet de las cosas en el hogar (publicada el 14/12/2023)	**2.279**
Protección de datos en vacaciones	**2.076**

Otros contenidos	
Infografías	**Descargas**
Cómo evitar la publicidad no deseada	**1.623**
Infografía: El control es tuyo, que no te controlen	**1.601**
Reference Map Personal data processing embedding Artificial Intelligence	**1.357**
Recomendaciones en la contratación a distancia de servicios de telecomunicaciones y energía	**1.229**
Juguetes conectados	**1.189**
Compra segura en internet	**996**
Facilita Emprende	**855**
Reglamento de Protección de Datos	**809**
Denuncia la difusión de contenidos violentos o sexuales en Internet	**646**
Infografía: Measures to minimise internet tracking	**618**
Protege sus datos en la vuelta a clase	**585**
Recommendations for users in the use of chatbots with artificial intelligence	**568**
Balance Plan Estratégico	**476**
Canal Prioritario - Igualdad	**364**
Personal Data Breach Communication	**345**
Privacy Risks of Internet of Things at Home	**301**
Risks associated with age verification systems and summary of the Decalogue of principles (publicada el 18/12/2023)	**86**

Otros contenidos	
Notas técnicas	**Descargas**
Protección del menor en Internet	**20.345**
Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo	**15.154**
La K-anonimidad como medida de la privacidad	**9.592**
14 equívocos con relación a la identificación y autenticación biométrica	**8.952**
El deber de informar y otras medidas de responsabilidad proactiva en apps para dispositivos móviles	**8.160**
El uso de las tecnologías en la lucha contra el COVID19	**7.246**
Introducción a las tecnologías 5G y sus riesgos para la privacidad	**5.931**
Medidas para minimizar el seguimiento en internet	**3.805**
K-anonymity as a privacy measure	**3.171**
Nota técnica de las pruebas de concepto sobre sistemas de verificación de edad (Publicada el 14/12/23)	**2.590**
Privacidad en DNS	**2.644**
Recomendaciones para el despliegue de aplicaciones móviles en el acceso a espacios públicos	**2.466**
Control del usuario en la personalización de anuncios en Android	**2.432**
The duty to inform and other accountability measures for mobile devices	**1.437**
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”	**1.332**
Acceso de aplicaciones a la pantalla en dispositivos Android	**1.134**
Preview of "An Analysis of Pre-installed Android Software and Risks for Users' Privacy", an study by IMDEA NETWORKS and UC3M	**945**
Introduction to 5G technologies and their risks in terms of privacy	**937**
User controls for ad personalisation on Android	**893**
14 misunderstandings with regard to biometric identification and authentication	**861**

Otros contenidos	
Notas técnicas	**Descargas**
DNS Privacy	**801**
Guidelines for social distance and access control apps due to COVID-19	**743**
Measures to minimise internet tracking	**710**
Technologies in the fight against COVID19	**645**
Access to applications on the screen for Android devices	**512**
Recommendations to protect personal data in situations of mobility and telecommuting	**483**
Otras publicaciones	**Descargas**
Informe sobre políticas de privacidad en internet. Adaptación al RGPD	**12.925**
Introducción al hash como técnica de seudonimización de datos personales	**10.482**
Orientaciones para la aplicación de la disposición adicional octava y la disposición final duodécima de la LOPDGDD	**9.305**
Adecuación a la normativa a 'coste cero' y otras prácticas fraudulentas	**8.730**
Fingerprinting o Huella digital del dispositivo	**7.879**
Consecuencias administrativas, disciplinarias, civiles y penales de la difusión de contenidos sensibles	**7.167**
FAQ sobre el COVID-19	**6.646**
Preguntas frecuentes sobre la anulación del Escudo de Privacidad	**5.898**
Decálogo para la adaptación al RGPD de las políticas de privacidad en internet	**5.745**
LOPD: Novedades para el Sector Público	**5.554**
Plan de inspección de oficio de la atención sociosanitaria	**4.152**
Fingerprinting o Huella digital del dispositivo (Versión en Inglés)	**3.399**
LOPD: Novedades para el Sector Privado	**3.007**
LOPD: Novedades para los ciudadanos	**2.700**

Otros contenidos	
Otras publicaciones	**Descargas**
25 años de la Agencia Española de Protección de Datos	**2.386**
Plan de inspección de oficio sobre contratación a distancia en operadores de telecomunicaciones y comercializadores de energía	**2.287**
Plan de inspección sectorial de oficio Hospitales Públicos	**2.199**
Análisis de los flujos de información en Android	**1.954**
Introduction to the Hash function as a personal data pseudonymisation technique	**1.901**
Análisis de los flujos de información en Android (Versión en Inglés)	**1.611**
FAQ about the COVID-19	**1.363**
Encuesta sobre el grado de preparación de las empresas españolas ante el RGPD (AEPD-CEPYME)	**1.180**
Guidelines for Implementation of the Eighth Additional Provision and Twelfth Final Provision of the LOPDGDD	**644**
Memorias	**Descargas**
Memoria AEPD 2022	**60.865**
Memoria de Responsabilidad Social 2022	**32.445**

Pacto digital para la protección de personas

Pacto digital para la protección de personas	
	2023
Entidades adheridas (totales)	509

Códigos de Conducta [5]					
	Aprobados	Modificados	Inadmitidos	En tramitación	Iniciativas
2023	0	1	0	15*	7
Total códigos de conducta modificados					**1**

** Cuatro códigos son de carácter transnacional, en uno de ellos la AEPD actúa como co-revisora.*

[5] En el proceso de Códigos de Conducta se mantienen reuniones con todos los promotores, con el fin de aclarar las cuestiones relativas a la tramitación de los Códigos.

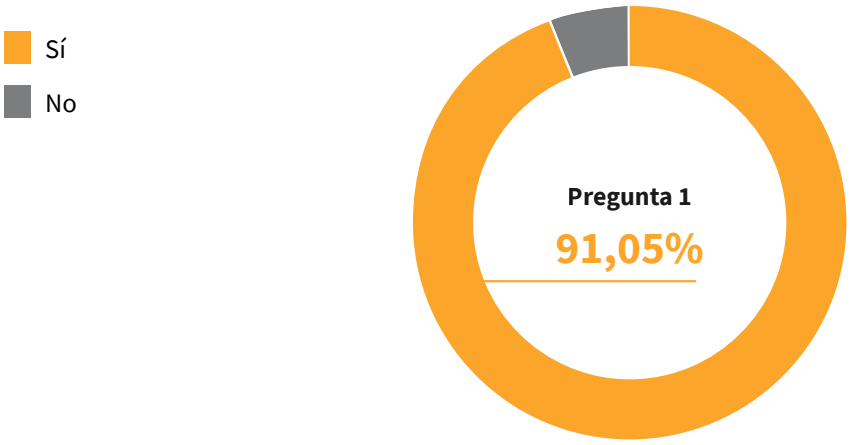
Encuestas de Calidad 2023			
Resumen general		**SI**	**NO**
1	¿Está satisfecho/a con el contenido de la información recibida?	5.527	543
2	¿Considera que la persona que le atendió tiene los conocimientos técnicos suficientes?	5.535	535
3	¿Está satisfecho/a con la corrección en el trato por parte del operador?	5.704	366
Total de encuestas contestadas		**6.070**	

Análisis de respuestas		**SI**	**NO**
1	¿Está satisfecho/a con el contenido de la información recibida?	91,05%	8,95%
2	¿Considera que la persona que le atendió tiene los conocimientos técnicos suficientes?	91,19%	8,81%
3	¿Está satisfecho/a con la corrección en el trato por parte del operador?	93,97%	6,03%
Total de encuestas contestadas		**100%**	
Promedio de satisfacción		**92,09%**	

Encuestas de Calidad

Número Total 6.070

¿Está satisfecho con el contenido de la información recibida?

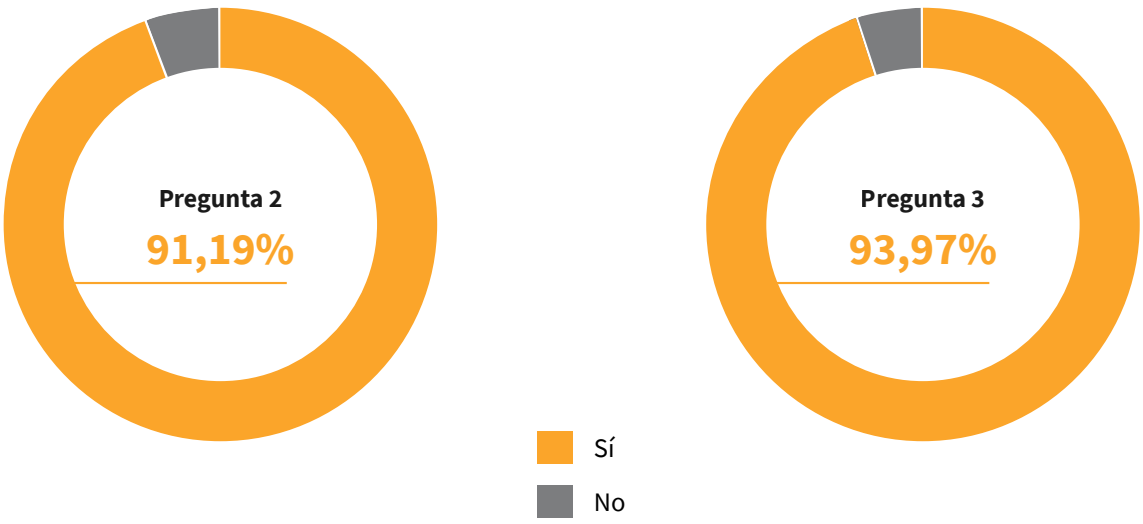


Encuestas de Calidad

Número Total 6.506

¿Considera que la persona que le atendió tiene los conocimientos técnicos suficientes?

¿Está satisfecho/a con la corrección en el trato por parte del operador?



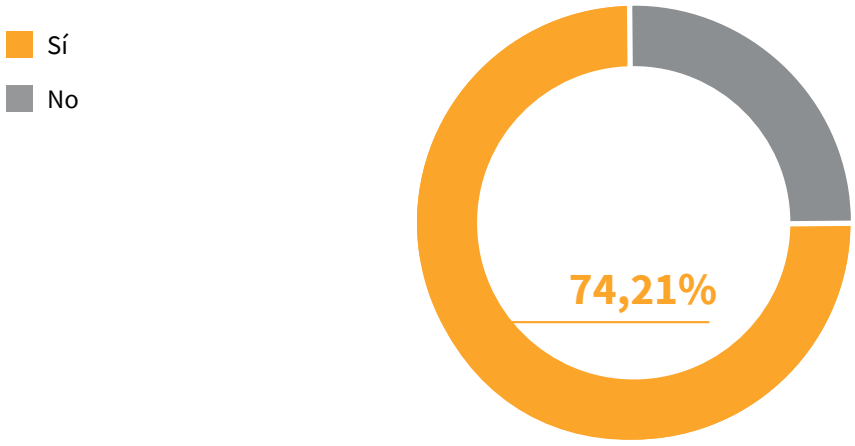
Encuestas de Satisfacción del Chatbot 2023		
Resumen general	**SI**	**NO**
1 Queremos saber su opinión sobre el servicio. ¿Le hemos ayudado?	843	293
Total de encuestas contestadas	**1.136**	

Análisis de respuestas	**SI**	**NO**
1 Queremos saber su opinión sobre el servicio. ¿Le hemos ayudado?	74,21%	25,79%
Total de encuestas contestadas	**100%**	
Índice de Satisfacción del Cliente	**74,21%**	

Encuestas de Satisfacción

Número Total 1.136

¿Está satisfecho con el contenido de la información recibida?



Accesos a la sección de transparencia			
2021	2022	2023	% 2022-2023
166.290	127.549	173.463	36%

Solicitudes de acceso a la información pública[6]						
Año	Solicitudes	Concedidas	Inadmitidas[7]	Concedidas parcialmente	Denegadas	Desistidas
2023	112	45	47	4	4	10

[6] *Dos solicitudes se encuentran actualmente en trámite.*

[7] *Inadmitidas incluye: Devueltas a Unidad Central 7 y finalizaciones anticipadas (por acumulación u otras causas, 12).*

Reclamaciones ante el CTBG			
Año	Reclamaciones	Estimatorias	Desestimatorias[8]
2023	9	0	9

[8] *Desestimatorias incluye Archivadas 2 e Inadmitidas 1.*

Registro de Delegados de Protección de Datos comunicados[9]		
Titularidad		Total notificados
Entidades Privadas		101.691
Entidades Públicas		9.379
	Administración General del Estado	195
	Comunidades Autónomas	457
	Entidades Locales	4.794
	Otras personas Jurídico-Públicas - Consejo General del Poder Judicial - Notarios - Colegios Profesionales - Universidades - Cámaras de Comercio - Comunidades Regantes	3.933
TOTAL		**111.070**

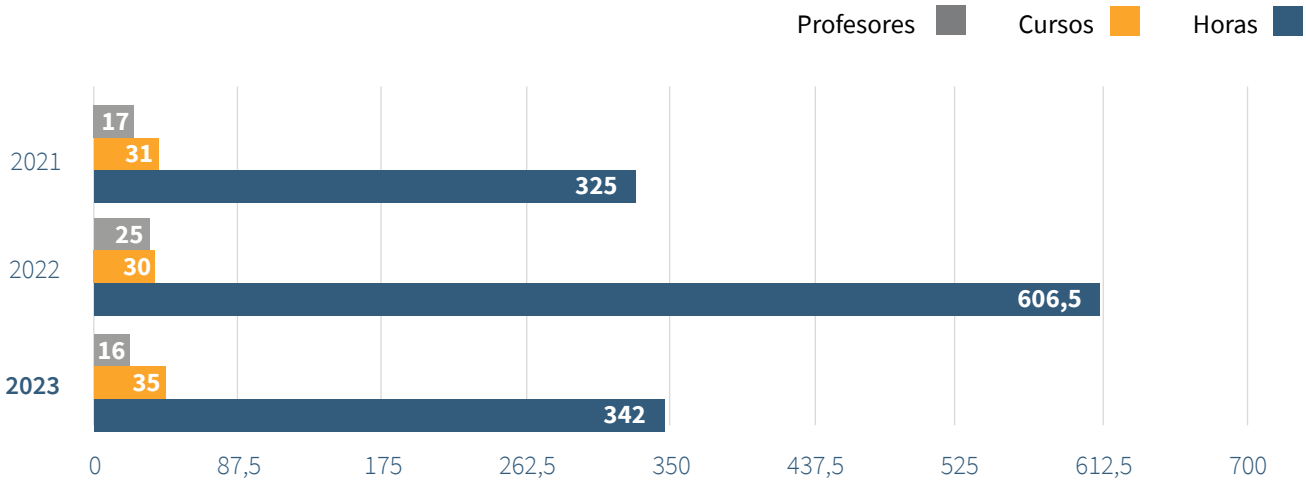
[9] *Durante 2023 se han atendido 991 consultas e incidencias relativas a la comunicación de los DPD.*

Transferencias Internacionales desde 2019		
	2023	Total acumulado
Autorizaciones de transferencias internacionales	-	1 (Art. 46.3.b RGPD)
Normas Corporativas Vinculantes (BCR) adoptadas por la AEPD	2	10
Normas Corporativas Vinculantes (BCR) en tramitación por la AEPD como autoridad líder	12	-
Normas Corporativas Vinculantes (BCR) en las que la AEPD ha participado como co-revisora	4	37

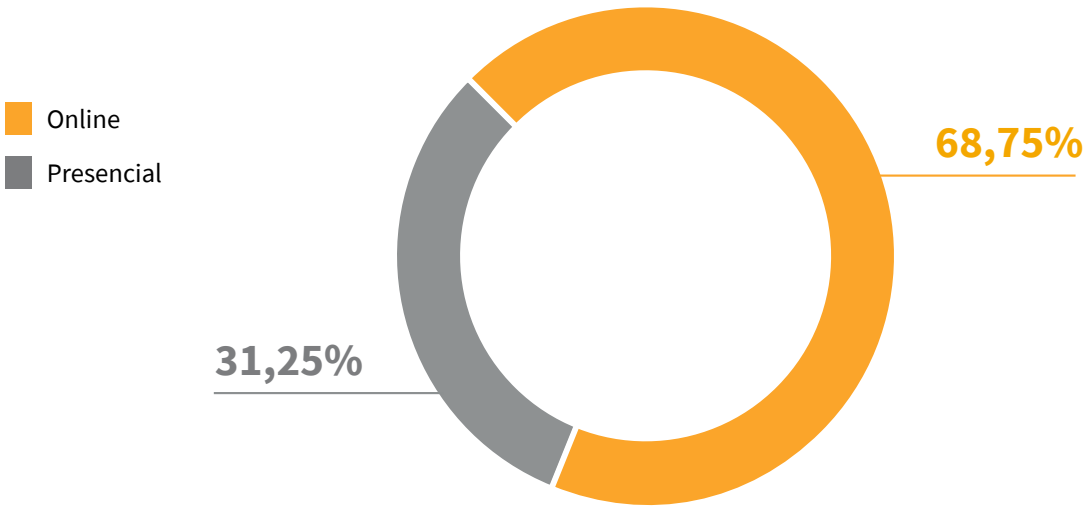
Esquema de Certificación de DPD (AEPD-DPD)			
	2021	2022	2023
Auditorías	12	4	3
Revisión de preguntas de examen	8.538	3.932	3.696
Elaboración de exámenes	95	72	78
Seguimiento de entidades de formación	164	136	324
Seguimiento de entidades de certificación	13	15	14
Reconocimiento de formación universitaria	1	1	1
DPD Certificados	175	138	169
Total DPD Certificados:			**1.100**

Formación[10]			
	2021	2022	2023
Cursos	17	25	**16**
Profesores	31	30	**35**
Horas	325	606,5	**342,5**

[10] Coordinadas por la Subdirección General de Promoción y Autorizaciones.



Formato del curso



A continuación, se detallan las actividades formativas que la AEPD ha desarrollado a lo largo del año 2023, cuya gestión se ha realizado desde la Subdirección General de Promoción y Autorizaciones.

Cursos Generales de Protección de Datos (formato online o presencial)

Organismo	Fechas	Duración	Formato	Nº alumnos
Ministerio de Sanidad	27/02 - 02/03	20 h	On line	30
Ministerio Derechos Sociales	16/03 - 30/03	22,5 h	On line	20
Tribunal de Cuentas	18/04 - 28/04	20 h	On line	60
Universidad Las Palmas G.C.	08/05 - 11/05	20 h	On line	20
Ministerio del Interior	30/05 - 02/06	20 h	Presencial	20
Ministerio de Educación	05/06 - 14/06	20 h	Presencial	20
Ministerio de Trabajo	19/06 - 28/06	20 h	On line	20
Ministerio de Inclusión	04/07 - 07/07	20 h	Presencial	20
M. Política Territorial	21/09 - 05/10	20 h	Presencial	30
Ministerio de Justicia	18/09 - 21/09	20 h	On line	20
Ministerio de Defensa	06/10 - 20/10	20 h	On line	40
M. Transición Ecológica	30/10 - 10/11	20 h	On line	30
Ministerio de Inclusión	21/11 - 24/11	20 h	Presencial	20

Cursos Generales de Protección de Datos (formato Moodle), con la actualización de todo el temario

Organismo	Fechas	Duración	Nº alumnos
Ministerio de Transportes	24/04 -04/06	36 h	30
Ministerio de Defensa	23/10 - 03/12	36 h	40

Jornadas y otros cursos

Organismo	Fecha	Denominación / Comentarios
Asociación de Expertos Nacionales de la Abogacía Tecnológica (ENATIC)	25/01	Webinar Privacy Day. La figura del DPD.
ISMS Forum	16/02	XV Foro de la Privacidad. "Códigos de conducta, certificaciones, estándares y mecanismos de mediación para el fortalecimiento de la protección de datos".
Área de Derechos Humanos e Igualdad de la Policía Nacional	21/02	III Curso de Derechos Humanos, curso dirigido a Escala Superior -comisarios y comisarios principales- Policía Nacional. Dar a conocer las nuevas vulnerabilidades de los Derechos Humanos en las TIC.
Escuela Diplomática	08/03	"Protección de los datos personales en el exterior".
Unión Democrática de Pensionistas y Jubilados y la Fundación Telefónica	16/03	II Congreso sobre el Derecho a la Autonomía Personal 'La tecnología en la vida cotidiana de las personas mayores'. Conferencia de apertura.
Dirección General para la Igualdad de Trato y Diversidad Étnico Racial del Ministerio de Igualdad	24/03	III Semana Antirracista. Mesa redonda sobre la propuesta concreta del Ministerio de Igualdad de recogida de datos sobre origen étnico por parte del INE en el año 2026.
Centro de Estudios Jurídicos	04/05	Protección de Datos.
Asociación Española de Farmacéuticos de la Industria (AEFI)	06/06	41 Symposium AEFI. Mesa Redonda "Código de Conducta regulador del tratamiento de datos personales en el ámbito de los ensayos clínicos y otras investigaciones clínicas y de la farmacovigilancia".
ENATIC	07/06	Webinar. Radiografía de los DPD en España. Malas praxis, responsabilidad profesional y riesgos para responsables del tratamiento.

Cursos en el entorno educativo y de menores

Organismo	Fecha	Denominación / Comentarios
Fundación The Family Watch	16 de marzo	Presentación de la "Guía que no viene con el móvil" con las 10 claves que las familias han de tener en la entrega del primer móvil a sus hijos. Dirigido a expertos sobre salud mental.
Instituto Asturiano de Admón. Pública "Adolfo Posada"	18 y 25 de abril online	Tratamiento de datos en el entorno educativo. Dirigido al personal de Inspección Educativa.
Aulas Digitales de la Fundación Coca-Cola	21 de abril	Presentación de la "Guía que no viene con el móvil" con las 10 claves que las familias han de tener en la entrega del primer móvil a sus hijos.
Colegio de Abogados de Málaga	19 de mayo	III Congreso de Familia en Málaga, Mesa Redonda: "Desafíos actuales en menores y adolescentes: Acoso en redes sociales. Bullying".
AEPD/Agencia Española de Cooperación Internacional para el Desarrollo (AECID)	28 de junio	Webinario sobre digitalización y menores.
Generalitat Valenciana	24 de octubre	I Congreso de protección de datos en la comunidad educativa.
Universidad Rey Juan Carlos	10 de noviembre	I Congreso Internacional de Comunicación Clara. Especial atención a públicos vulnerables como el infantil.
AEPD/INTEF/INCIBE	16 de noviembre	MOOC "Educar en seguridad y privacidad".

Jornadas sobre violencia digital hacia las mujeres y el Canal Prioritario

Organismo	Fecha	Denominación / Comentarios
Fundación Diagrama	22/09	Jornada de prevención temprana de la ciberviolencia de género en jóvenes.
Unidad de Violencia sobre la Mujer-Subdelegación del Gobierno en Segovia	07/11	La dimensión digital de la Violencia contra la mujer.
Ministerio de Justicia	24/11	Jornada violencia de género.

Cursos que se programan e imparten para el personal al servicio de la Administración Pública a través del INAP

Denominación	Fecha	Nº de alumnos
Programa especializado para DPD de las AA.PP.	13/02 al 12/06	80
Aplicación del RGPD en las AA.PP.	20/02 a 24/03	300
Aplicación del RGPD en las AA.PP.	25/09 a 30/10	300

Cursos que se programan e imparten para el personal al servicio de la Administración Pública a través del INAP

Denominación	Fecha
Presentación de los Códigos de Conducta como instrumento para fomentar la resolución ágil de controversias (operadores de telefonía)	17 de enero
Encuentro DPD-EELL-Ayuntamientos capitales de provincia, de más de 100.000 habitantes, Diputaciones, Cabildos y Consejos Insulares	28 de marzo
Jornada sobre Protección de Datos e Investigación Sanitaria. Impacto de la innovación tecnológica el tratamiento de datos personales de la investigación sanitaria	3 de mayo
Jornada de calidad normativa en protección de datos: la función asesora de la Agencia en la elaboración de normas y la Memoria de Análisis de Impacto Normativo (MAIN); el análisis de riesgos y evaluaciones de impacto en protección de datos en la producción normativa, la incidencia del RGPD en el contenido de las normas y garantías a incorporar en la norma	23 de mayo
Sesión informativa con alumnos de la facultad de Derecho de Stetson University de Florida, sobre la protección de datos personales en el ámbito laboral	8 de junio
La AEPD y la Plataforma de Mayores y Pensionistas (PMP) organizan el Encuentro “Mayores en el entorno digital”	27 de junio

Facilita RGPD[11]	
	2023
Accesos	51.783
Cuestionarios finalizados	20.432
Acumulados	**1.109.161**

[11] Facilita RGPD, herramienta para facilitar la adecuación al RGPD de empresas y profesionales.

Facilita EMPRENDE[12]	
	2023
Accesos	2.746
Cuestionarios finalizados	695
Acumulados	**18.700**

[12] Facilita EMPRENDE, herramienta para ayudar a los emprendedores y startups tecnológicas a cumplir con la normativa de protección de datos.

GESTIONA[13] [14]			
Sección	**Abierto**	**Finalizado**	**Acumulados**
Evaluaciones de impacto en la privacidad (EIPD)	2.775	967	**33.453**
Análisis de riesgos	1.946	621	**31.437**

[13] Gestiona EIPD: Asistente para el análisis de riesgos y evaluaciones de impacto en protección de datos.

[14] Estas cifras de la herramienta GESTIONA se refieren exclusivamente al periodo comprendido entre el 1 de enero y el 14 de junio de 2023, momento en el que se publicó la nueva versión de esta herramienta.

GESTIONA V2[15]	
	2023
Accesos	25.369
Número de informes descargados	937

[15] La nueva versión de la herramienta GESTIONA denominada GESTIONA V2 únicamente permite ver el número de accesos y número de descargas del informe que realiza dado que el aplicativo se ejecuta directamente en el terminal del usuario y no proporciona ninguna información sobre el tipo de proceso realizado por el usuario.

Evalúa-Riesgo RGPD[16]		
	2022	2023
Accesos	101.897	222.463
Acumulados		**330.494**

[16] Evalúa_Riesgo RGPD: herramienta cuyo objetivo es ayudar a los responsables y encargados a identificar los factores de riesgo de los tratamientos de datos personales; hacer una primera evaluación no exhaustiva, del riesgo intrínseco, incluyendo la obligación de realizar una EIPD, y facilitando la gestión del riesgo residual al utilizar medidas y garantías para mitigar dicho riesgo.

COMUNICA-Brecha RGPD[17]	
	2023
Accesos	5.344
Cuestionarios finalizados	993
Acumulados	**16.706**

[17] Comunica-Brecha RGPD, recurso para que cualquier organización, responsable de un tratamiento de datos personales, pueda valorar la obligación de informar a las personas físicas afectadas por una brecha de seguridad de los datos personales.

ASESORA-Brecha RGPD[18]	
	2023
Accesos	6.491
Cuestionarios finalizados	1.883
Acumulados	**19.736**

[18] *Asesora-Brecha RGPD, recurso de utilidad para que cualquier organización, responsable de un tratamiento de datos personales, pueda valorar la obligación de notificar sin dilación indebida a la Agencia Española de Protección de Datos una brecha de datos personales, tal y como establece el artículo 33 del Reglamento General de Protección de Datos.*

ValidaCripto[19]	
	2023
Accesos	4.086
Número de informes descargados	125

[19] *La herramienta ValidaCripto fue publicada el 5 de octubre de 2023 y, por tanto, no existe valor acumulado de años anteriores.*

4. División de innovación tecnológica

Brechas de datos personales (Artículos 33 y 34 RGPD)	
Notificaciones de brechas de datos personales	**2.004**
Resoluciones para obligar a comunicar las brechas a los interesados	**30**
Traslados a la Subdirección General de Inspección de Datos	**16**
Número de interesados a los que se les han comunicado las brechas	**17.000.000**

Brechas de datos personales (Artículos 33 y 34 RGPD)	
Consultas previas recibidas	**3**

5. Presencia internacional de la AEPD

Reunión	Fecha	Lugar
Sesiones Plenarias del Comité Europeo de Protección de Datos	17 de enero	Videoconferencia
	13 y 14 de febrero	Bruselas (Bélgica)
	28 de febrero 28 de marzo 13 de abril 26 de abril	Videoconferencia
	24 y 25 de mayo	Bruselas (Bélgica)
	20 de junio 18 de julio 2 de agosto	Videoconferencia
	19 y 20 de septiembre	Bruselas (Bélgica)
	17 de octubre 27 de octubre	Videoconferencia
	14 de noviembre 12 de diciembre	Bruselas (Bélgica)

Reuniones de subgrupos del Comité Europeo de Protección de datos		
Reunión	**Fecha**	**Lugar**
Subgrupo de asesoramiento (Strategic advisory)	7 de febrero 23 de febrero 29 de marzo 26 de junio 17 de julio 5 de septiembre 12 de septiembre 16 de octubre 19 de octubre 24 de octubre 10 de noviembre 20 de noviembre 20 de diciembre	Videoconferencia

Reuniones de subgrupos del Comité Europeo de Protección de datos		
Reunión	**Fecha**	**Lugar**
Grupo de trabajo Cookie Banners	11 de octubre 15 de noviembre	Videoconferencia
Medios Sociales Digitales (Social Media)	23 de enero 23 de febrero	Videoconferencia
	23 de mayo	Bruselas (Bélgica)
	29 de junio 7 de septiembre 10 de octubre	Videoconferencia
	7 de diciembre	Bruselas (Bélgica)
Cooperación	18 enero	Videoconferencia
	9 de febrero	Bruselas (Bélgica)
	21 de marzo 18 de abril 24 de abril 16 mayo	Videoconferencia
	15 de junio	Bruselas (Bélgica)
	22 de agosto 30 de agosto 5 de septiembre 26 de septiembre 19 de octubre	Videoconferencia
	16 de noviembre	Bruselas (Bélgica)
Asuntos financieros	19 de enero 20 de febrero 6 de marzo 13 de marzo 4 de abril 3 de mayo 6 de junio 7 de julio 11 de julio	Videoconferencia

Reuniones de subgrupos del Comité Europeo de Protección de datos		
Reunión	**Fecha**	**Lugar**
Asuntos financieros	9 de septiembre	Bruselas (Bélgica)
	28 de noviembre	Videoconferencia
Transferencias internacionales	10 y 11 de enero 31 de enero y 1 de febrero 10 de febrero	Videoconferencia
	31 e mayo y 1 de junio	Bruselas (Bélgica)
	4 de julio	Videoconferencia
	5 y 6 de septiembre	Bruselas (Bélgica)
	4 y 5 de octubre 7 y 8 de noviembre	Videoconferencia
	5 y 6 de diciembre	Bruselas (Bélgica)
Grupo de trabajo Multas	7 de febrero	Videoconferencia
	9 de marzo	Bruselas (Bélgica)
	19 de abril 8 de junio 13 de septiembre 15 de noviembre 11 de diciembre	Videoconferencia
Grupo de trabajo 101 denuncias Schrems II del TJUE	6 de febrero 6 de marzo	Videoconferencia
Fronteras, viajeros y aplicación legislativa (BTLE)	26 de enero 10 de febrero 23 de marzo 4 de mayo	Videoconferencia
	15 de junio	Bruselas (Bélgica)

Reuniones de subgrupos del Comité Europeo de Protección de datos		
Reunión	**Fecha**	**Lugar**
Fronteras, viajeros y aplicación legislativa (BTLE)	15 de septiembre 26 de octubre	Videoconferencia
	30 de noviembre	Bruselas (Bélgica)
Disposiciones clave (Key Provisions)	25 de enero	Videoconferencia
	1 de marzo	Bruselas (Bélgica)
	18 de abril 30 de mayo 6 de julio	Videoconferencia
	26 de septiembre	Bruselas (Bélgica)
	26 de octubre 21 y 22 de noviembre	Videoconferencia
Supervisión del cumplimiento (Enforcement)	8 de febrero	Bruselas (Bélgica)
	17 de febrero 2 de marzo 16 de marzo 22 de marzo 4 de abril 18 de abril	Videoconferencia
	7 junio	Bruselas (Bélgica)
	19 de junio 27 de junio 4 de julio 10 de julio 20 de julio 22 de agosto 30 de agosto 12 de septiembre	Videoconferencia
	18 de octubre	Bruselas (Bélgica)
	5 de diciembre	Videoconferencia

Reuniones de subgrupos del Comité Europeo de Protección de datos		
Reunión	**Fecha**	**Lugar**
Usuarios de sistemas de información del CEPD (IT Users)	13 de marzo	Bruselas (Bélgica)
	16 de junio 9 de octubre 4 de diciembre	Videoconferencia
Tecnología	18 y 19 de enero	Videoconferencia
	16 de febrero	Bruselas (Bélgica)
	22 de marzo 19 de abril 10 de mayo	Videoconferencia
	14 de junio	Bruselas (Bélgica)
	13 de julio 13 de septiembre	Videoconferencia
	18 y 19 de octubre	Bruselas (Bélgica)
	16 de noviembre 4 de diciembre	Videoconferencia
Cumplimiento, Gobierno electrónico y Salud (Compliance, E-goverment & Health)	24 de enero 21 de febrero	Bruselas (Bélgica)
	16 de marzo	Videoconferencia
	27 de abril 17 de mayo	Bruselas (Bélgica)
	8 de junio 19 de junio 26 de junio 11 de julio	Videoconferencia
	21 de septiembre	Bruselas (Bélgica)
	20 de octubre 7 de noviembre 19 de diciembre	Videoconferencia

Reuniones de subgrupos del Comité Europeo de Protección de datos		
Reunión	**Fecha**	**Lugar**
Grupo de Trabajo Chat GPT	18 de abril 3 de mayo 12 de julio 6 de septiembre 20 de octubre 8 de noviembre 1 de diciembre	Videoconferencia
Grupo de Trabajo Competencia y Consumo	28 de abril	Videoconferencia
	21 de junio	Bruselas (Bélgica)
	6 de septiembre 15 de noviembre 23 de noviembre 15 de diciembre	Videoconferencia
Grupo de Trabajo Internacional	22 de mayo 10 de julio 18 de septiembre 27 de noviembre	Videoconferencia
Control de Agencias y Grandes Sistemas de Información UE		
Grupo de Supervisión Coordinada CSC	22 de marzo	Videoconferencia
	14 de junio	Bruselas (Bélgica)
	7 de septiembre	Videoconferencia
	29 de noviembre	Bruselas (Bélgica)
Grupo de Supervisión Coordinada del SIS II	22 de marzo	Videoconferencia
	14 de junio	Bruselas (Bélgica)
	7 de septiembre	Videoconferencia
	29 de noviembre	Bruselas (Bélgica)
Grupo de Supervisión Coordinada de EUROPOL	22 de marzo	Videoconferencia
	14 de junio	Bruselas (Bélgica)
	29 de noviembre	Bruselas (Bélgica)
Evaluación Schengen	8 - 15 de octubre	Riga (Letonia)

Otras reuniones		
Reunión	**Fecha**	**Lugar**
Meeting of Mediterranean experts and DPAs	26 – 31 de enero	(Rabat) Marruecos
XX Foro de Seguridad y Protección de Datos de Salud	17 – 16 de febrero	Palma de Mallorca
	5 de octubre	Málaga
Mobile World Congress	27 de febrero – 1 de marzo	Barcelona
Data Protection and EU Integration	14 – 15 de marzo	Varsovia (Polonia)
Privacy Symposium 2023	16 – 22 de abril	Venecia (Italia)
Spring Conference	9 – 12 de mayo	Budapest (Hungría)
Reunión Coordinación Agencias Autonómicas de PD	29 – 30 de mayo	Barcelona
Grupo de Berlin	5 – 7 de junio	Roma (Italia)
	5 – 8 de diciembre	Ottawa (Canadá)
Global PETs Regulator Network Conference	25 – 28 de junio	Tel Aviv (Israel)
Foro de Derechos Humanos en el Deporte (CoE)	29 – 30 de junio	París (Francia)
Personalized Digital Care and the European Health Data Space	26 – 30 de septiembre	León
Global Privacy Assembly	14 – 22 de octubre	Bermuda (Bermuda)
Meeting of the HLG on access to data for effective law enforcement	3 – 4 de octubre 21 de noviembre	Bruselas (Bélgica)
Normativa Int en materia de Ciberseguridad y PD Personales	18 – 24 de noviembre	Mexico City (México)
Taller de Certificación	22 – 24 de noviembre	Luxemburgo (Luxemburgo)
Octopus Conference 2023	13 – 15 de diciembre	Bucarest (Rumanía)
Meta EU Youth Forum	5 de diciembre	Bruselas (Bélgica)

Consejo de Europa		
Reunión	**Fecha**	**Lugar**
Comité Convención 108 – Mesa	22 – 24 de marzo 27 – 29 de septiembre	París (Francia)
Comité Convención 108 - Plenario	14 – 16 de junio 15 – 17 de noviembre	Estrasburgo (Francia)
Comité de Inteligencia Artificial	11 – 13 de enero 1 – 3 de febrero 19 – 21 de abril 31 mayo – 2 junio 23 – 26 de octubre	Estrasburgo (Francia)
	5 – 8 de diciembre	Videoconferencia

Reuniones RIPD	
Reunión	**Nº de encuentros**
Encuentro RIPD Santa Cruz de la Sierra, Bolivia	1
Encuentro XX Aniversario RIPD, La Antigua, Guatemala	1
Webinario DPF-Miembros RIPD	1
Acción conjunta RIPD ChatGPT	1
Acción conjunta RIPD CIDH	1
Reuniones Instituto Nacional de Transparencia, Acceso a la Información y protección de Datos Personales (INAI)	3
Visita Estudios AGETIC (Bolivia)	1
Reunión Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales de Estado de México y Municipios (INFOEM)	1
Reuniones Secretaría General Iberoamericana (SEGIB)	3

Reuniones RIPD	
Reunión	**Nº de encuentros**
Reuniones colaboración proyecto financiado por la UE	2
Reunión Comisión del Mercado Financiero de Chile (CMF)	1
Reunión Ministerio telecomunicaciones Ecuador	1
Reunión Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC), Bolivia	1
Reunión IPANDETEC, Panamá	1
Reunión Agencia de Privacidad de California (CPPA)	1
Reunión Agencia de Protección de Datos de los Habitantes (PRODHAB), Costa Rica	2
Reunión Universidad Latinoamericana de Ciencia y Tecnología, Costa Rica	1
AECID (Agencia Española de Cooperación Internacional para el Desarrollo)	6
Reuniones UNESCO	2
Reuniones Comité Ejecutivo RIPD	2
Ponencias en seminarios	3

6. Secretaría General

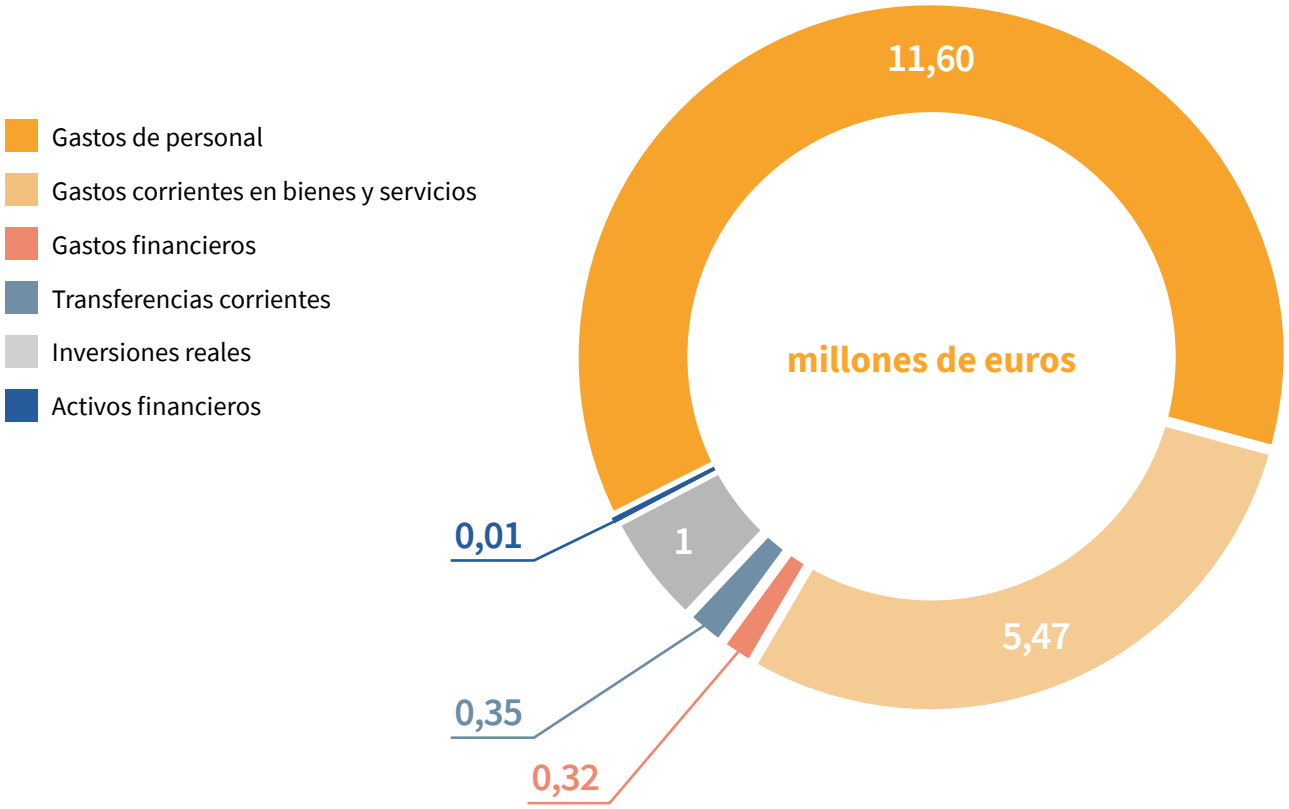
Evolución del presupuesto			
	Crédito Ejercicio		
	2021	2022	2023
Capítulo I	8.751.570	9.882.840	11.600.400
Capítulo II	5.235.310	5.359.840	5.468.240
Capítulo III	350.950	350.950	320.950
Capítulo IV	475.520	350.990	351.590
Capítulo VI	928.350	928.350	998.350
Capítulo VIII	20.800	11.200	11.200
TOTAL	**15.762.500**	**16.884.170**	**18.750.730**

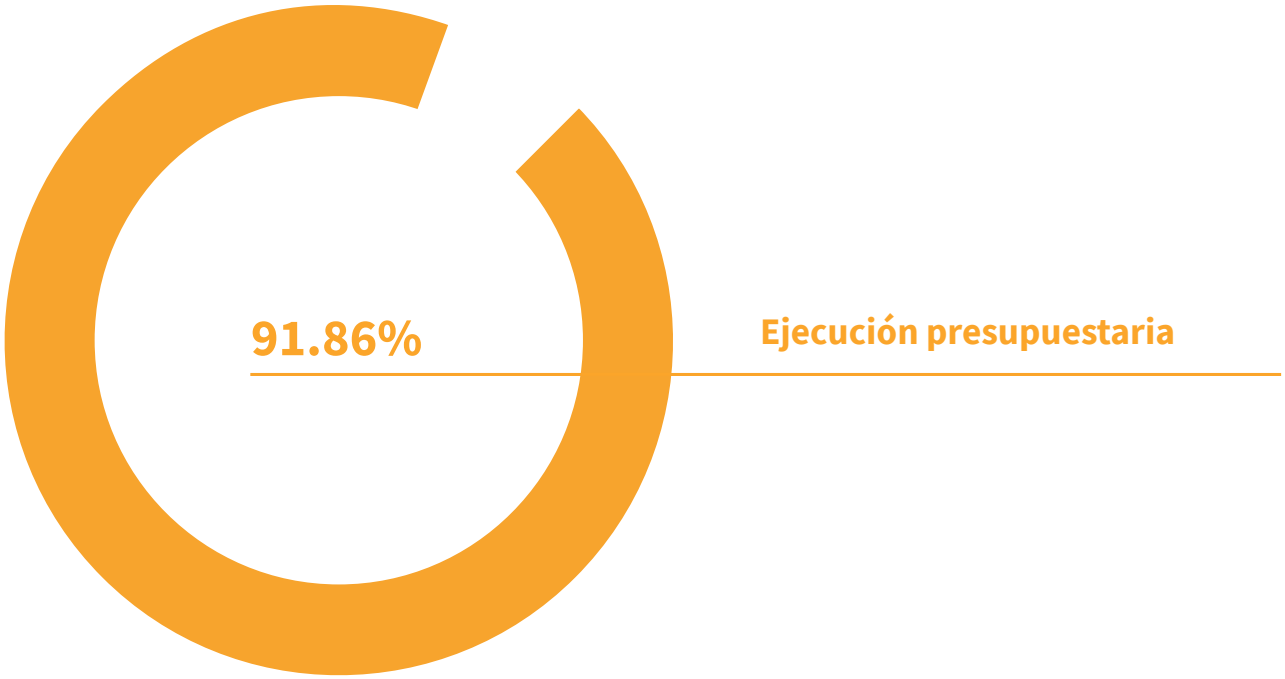
2023			
	Presupuesto definitivo	Obligaciones reconocidas	Porcentaje de ejecución
Gastos de personal	11.600.400	10.905.786,54	94,01%
Gastos corrientes en bienes y servicios	5.468.240	5.006.079,32	91,55%
Gastos financieros	320.950	1.128,38	0,35%
Transferencias corrientes	351.590	349.490	99,40%
Inversiones reales	998.350	1.216.948,08	121,90%
Activos financieros	11.200	4.825,80	43,09%
TOTAL	**18.750.730**	**17.484.258,12**	**93,25%**

2022			
	Presupuesto definitivo	Obligaciones reconocidas	Porcentaje de ejecución
Gastos de personal	9.882.840,00	9.505.277,87	96,18%
Gastos corrientes en bienes y servicios	5.359.840,00	4.818.377,76	89,90%
Gastos financieros	350.950,00	160.954,37	45,86%
Transferencias corrientes	350.990,00	347.990,00	99,15%
Inversiones reales	928.350,00	669.939,18	72,16%
Activos financieros	11.200,00	6.629,14	59,19%
TOTAL	**16.884.170,00**	**15.509.168,32**	**91,86%**

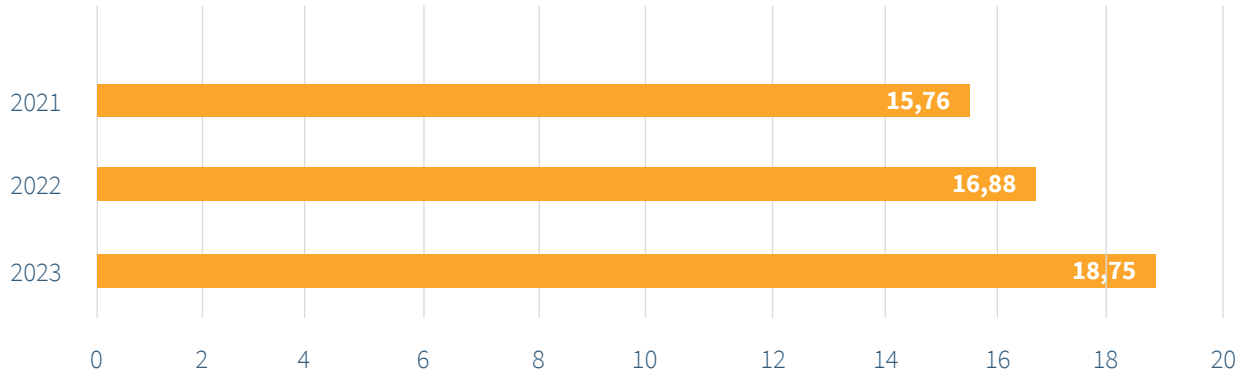
Diferencia 2023 - 2022		
	Presupuesto definitivo	Obligaciones reconocidas
Gastos de personal	1.717.560	1.400.508,67
Gastos corrientes en bienes y servicios	108.400	187.701,56
Gastos financieros	-30.000	-159.825,99
Transferencias corrientes	600	1.500
Inversiones reales	70.000	547.008,90
Activos financieros	0	-1.803,34
TOTAL	**1.866.560**	**1.975.089,80**

Distribución del presupuesto (en millones de euros)



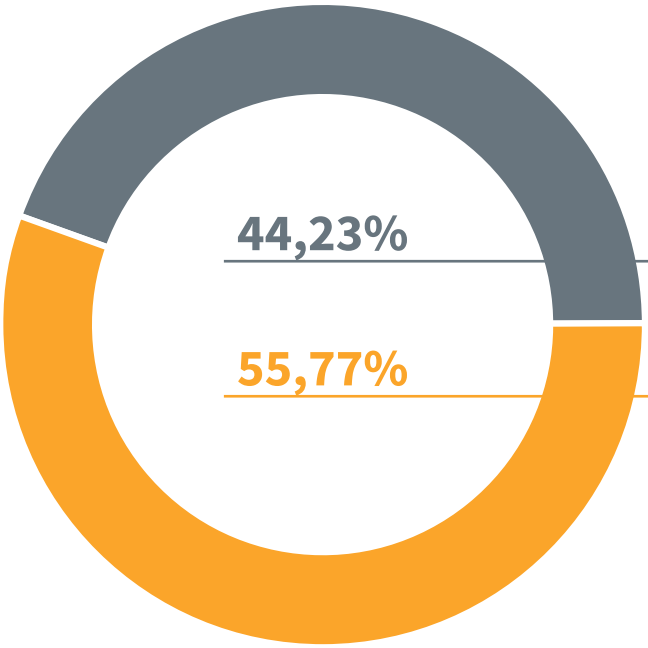


Evolución del crédito presupuestario (millones de euros)



Gestión de recursos humanos a 31 de Diciembre 2023		
	Dotación	**Cubiertos**
Funcionarios	236	198
Laborales	8	7
Laborales fuera de Convenio	2	2
Alto cargo	1	1
	TOTAL	**208**

La diferencia entre la dotación de puestos y la ocupación efectiva se debe a que en las plazas de personal funcionario se incluyen los puestos reservados a titulares se encuentran ocupando otro puesto de trabajo, los puestos creados para ser ocupados mediante oferta de empleo público, así como aquellos puestos que están en proceso de ser adjudicados en el concurso general en tramitación convocado por Resolución de 31 de octubre de 2023.



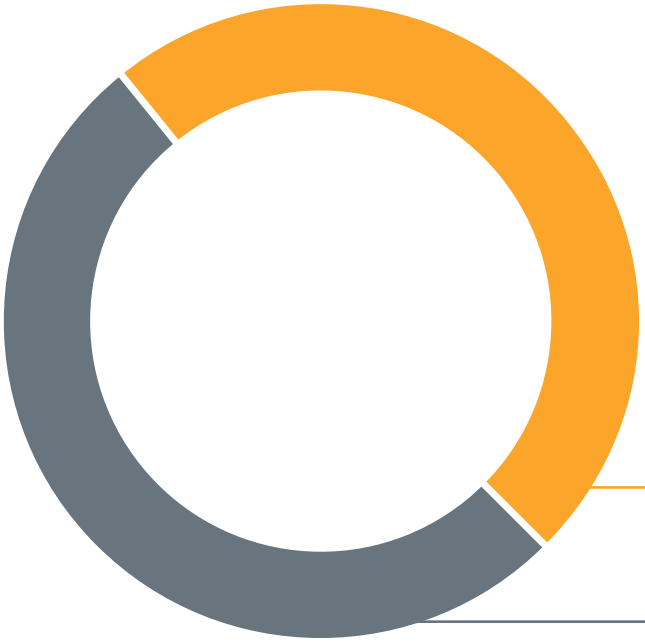
44,23%	Hombres	92
55,77%	Mujeres	116

Personal funcionario												
Nivel	30	29	28	26	24	22	20	18	17	16	15	14
Efectivos	11	8	46	75	0	30	0	20	2	5	1	0

Grupo	A1	A2	B	C1	C2
Efectivos	69	72	1	35	21

División por niveles					
	Nivel 30	Nivel 29	Nivel 28	Nivel 26	TOTAL
Hombres	4	6	28	33	**71**
Mujeres	7	2	18	40	**67**
TOTAL	**11**	**8**	**46**	**73**	**138**

División por niveles



Antes de la aprobación del Plan de Igualdad de la AEPD en 2020, la Agencia contaba con un 61,54 % de hombres frente a un 38,46 % de mujeres en dichos puestos. A 31 de diciembre de 2023, dichos porcentajes se sitúan en un ***51,45% de hombres frente a un 48,55% de mujeres****, esto es, en tan solo 4 años se ha incrementado en 10 puntos la presencia femenina en los niveles directivos y pre directivos de la Agencia.*

Mujeres **67**

Hombres **71**

Evolución de la plantilla de Personal Funcionario y Laboral (RPT)

Año	Dotaciones
2017	180
2018	186
2019	202
2020	202
2021	203
2022	217
2023	246

www.aepd.es
AEPD_es
AEPD
@aepd.es