agencia española protección datos

MEMORIA ANUAL 2021

prólogo

Las siguientes páginas recogen de forma exhaustiva las actividades y decisiones más relevantes de la Agencia Española de Protección de Datos (AEPD), sus cifras de gestión, y un análisis de las tendencias y los retos que afronta este derecho fundamental. Durante los más de seis años que he tenido el honor de dirigir este organismo la protección de datos ha tenido que hacer frente a numerosos desafíos, que arrancaron con las previsiones internas y externas necesarias para estar en condiciones de dar respuesta a la aplicación del Reglamento General de Protección de Datos. En este tiempo hemos hecho todo lo posible para proteger y garantizar este derecho, en especial, ante los nuevos retos que plantea un mundo digitalizado, poniendo a disposición de empresas y administraciones públicas, por un lado, y ciudadanos, por otro, más de 80 guías y herramientas para ayudarles con el cumplimiento de la norma y para que conozcan y ejerzan sus derechos. Este trabajo ha sido reconocido por la concesión de 18 premios a todo el equipo de la AEPD por parte de instituciones y organizaciones públicas y privadas en los últimos cuatro años, pero para la Agencia ha supuesto mucho más.

Las iniciativas que hemos realizado en los últimos años han sido de muy diversa índole, desarrollando guías, recomendaciones, herramientas, informes y acciones divulgativas, trabajando de forma estrecha con todos los sectores para promover que el cumplimiento de la normativa fuese proactivo y no sólo con el objetivo de evitar las medidas coercitivas y sancionadoras. En la Agencia estamos convencidos de que la privacidad es un factor de competitividad empresarial, y de que el desarrollo tecnológico sólo puede abordarse desde el respeto al derecho a los derechos fundamentales de las personas. Por ello, como puede consultarse en detalle en las páginas posteriores de esta Memoria, en 2021 pusimos en marcha una nueva iniciativa dirigida a impulsar un gran acuerdo por la convivencia ciudadana en el ámbito digital, compatibilizando la protección de datos con la innovación, la ética y la competitividad empresarial: *el Pacto Digital para la Protección de las Personas,* que cuenta ya con casi 400 entidades adheridas. Ese Pacto refleja la misión y visión que tiene la Agencia de la protección de datos en una doble vertiente: fomentar la responsabilidad activa de aquellos que tratan datos personales y ayudar a las personas a proteger su privacidad en internet, tanto a través de la concienciación y la educación como utilizando la potestad sancionadora cuando es necesario.

La adhesión al Pacto Digital por parte de aquellos que tratan datos supone asumir el compromiso con los principios y valores que contiene, como la ética digital, así como informar a las personas sobre el tratamiento de sus datos y el ejercicio de sus derechos, aplicar los principios de protección de datos, garantizar la licitud de los tratamientos, o aplicar los principios de privacidad desde el diseño y por defecto, entre otros.

Además, en estos años hemos realizado varias campañas de difusión masivas para dar a conocer que la ayuda que presta la Agencia a los ciudadanos puede ir mucho más allá del cumplimiento formal de la norma. La responsabilidad digital está estrechamente vinculada con el respeto a los derechos humanos y en este punto es necesario realizar una mención especial al *Canal prioritario de la AEPD* para solicitar la retirada urgente de contenidos sexuales o violentos publicados en Internet sin el consentimiento de las personas, un elemento que también está recogido en el Pacto Digital. Son muchas las acciones que se han seguido realizando este año para divulgar que los ciudadanos pueden acudir a la Agencia si se ven inmersos en una situación de este tipo, a la vez que concienciar sobre las responsabilidades de publicar sin permiso contenido de este tipo en Internet. Hemos adquirido este compromiso porque consideramos que una de las prioridades de la Agencia es proteger de forma efectiva a las personas en la Red, y especialmente a jóvenes y mujeres, que son los grupos más afectados por este tipo de situaciones. Como ciudadanos de un Estado de Derecho no podemos ni debemos resignarnos a que ese tipo de contenidos circulen libremente, y por eso era necesario dar un paso adelante y ofrecer una respuesta ágil y rápida desde las instituciones. Por otro lado, además de la responsabilidad administrativa que pueda derivarse de esa publicación, también se puede incurrir en responsabilidad civil, penal y laboral.

En paralelo, la Agencia ha tenido que seguir dando respuesta este año a los desafíos de protección de datos relacionados con la pandemia, articulando garantías para proteger los datos personales en los tratamientos relacionados con las medidas contra la COVID-19, en particular relacionadas con el uso del certificado COVID para el acceso a locales en el plano nacional y a través del Comité Europeo de Protección de Datos (CEPD) en el internacional. A ello se ha sumado la carga de trabajo relacionada con las reclamaciones recibidas por posibles incumplimientos de la normativa, que este año han crecido un 35% respecto al año anterior. Además, las reclamaciones resueltas en 2021 también han aumentado un 35%, una cifra muy destacable que ha permitido resolver reclamaciones

pendientes de ejercicios anteriores sin que hayan aumentado significativamente los tiempos medios de resolución.

Se hace necesario en este punto insistir en la necesidad de dotar a la Agencia de una mayor cantidad de medios humanos para continuar siendo un organismo puntero. Pese ello, como se puede apreciar en esta Memoria, los resultados tanto de la Subdirección General de Inspección, de Promoción y Autorizaciones, la Secretaría General, y las divisiones de Internacional e Innovación Tecnológica o el Gabinete Jurídico son admirables. Y en cuanto al modelo de cumplimiento, se ha constatado en muchas ocasiones que en las evaluaciones de impacto se intenta hacer un cumplimiento meramente formal sin dar respuesta al enfoque de riesgos sobre los derechos de las personas.

Resulta imposible hacer mención en este prólogo a todas las iniciativas y actividades realizadas en este año, por lo que animo a consultar el detalle de las mismas en las siguientes páginas. Ha sido un orgullo dirigir una Agencia de Protección de Datos que facilita la innovación, que escucha las necesidades tanto de los ciudadanos como de los sujetos obligados y que presta especial atención a los retos tecnológicos con un importante componente internacional. La evolución de este organismo no hubiera podido realizarse sin la dedicación absoluta de todas las personas que la componen, que han aceptado e incluso propuesto nuevos retos conscientes de la carga adicional de trabajo que podía suponer para ellas. Expresarles desde aquí mi gratitud por una entrega que está fuera de toda duda y que espero que en los próximos años se vea compensada con un aumento de los medios técnicos y humanos paralelo al de los retos que están por venir.

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

Índice

Memoria 2021

1. Principales hitos de 2021

El tratamiento de datos personales durante la pandemia de la COVID-19 ha continuado siendo uno de los principales hitos de la Agencia Española de Protección de Datos (AEPD) durante el año 2021.

La cuestión más relevante que se ha planteado en este ámbito en este año ha sido el relacionado con **la** emisión y utilización del conocido como certificado COVID regulado por el Reglamento (UE) 2021/953, de 14 de junio de 2021, relativo a un marco para la expedición, verificación y aceptación de certificados COVID-19 interoperables de vacunación, de prueba diagnóstica y de recuperación.

El certificado COVID, aprobado inicialmente con la finalidad de garantizar el derecho fundamental a la libre circulación de los ciudadanos en la Unión Europea, ha sido objeto de utilización posterior con otros fines en la generalidad de los Estados miembros y, en particular en España, como una de las medidas adoptadas por las autoridades sanitarias con el fin de evitar la extensión de los contagios en diversos establecimientos, mediante su exhibición.

La Memoria incluye un apartado específico sobre el certificado, describiendo sus implicaciones en relación con el tratamiento de los datos personales, tanto en los debates que tuvieron lugar durante la elaboración y aprobación de la norma, como respecto de su utilización por parte de las autoridades sanitarias de las comunidades autónomas. E incluyendo una síntesis sobre la jurisprudencia del Tribunal Supremo respecto de la utilización del certificado.

Otro de los hitos relevantes en 2021 es el relativo al desarrollo y cumplimiento del Plan de Responsabilidad Social de la Agencia Española de Protección de Datos.

La Responsabilidad Social en la AEPD busca como objetivo hacer de la Agencia una organización exigente en sus procedimientos y modelo de gestión, y ambiciosa en el impacto de cada uno de sus proyectos y actividades y en la orientación social de todas sus actuaciones, para configurar y consolidar la Agencia como un organismo abierto y cercano que refuerce y amplíe las vías de comunicación con todos los implicados, dando una respuesta integral a sus necesidades.

Sobre la base de este reto, el 27 de mayo de 2019 se aprobaron el Marco de Actuación, la Política de Responsabilidad Social de la AEPD y el Plan de Acción de Responsabilidad Social de la AEPD con 103 acciones a cumplir en el período 2019-2024. Dicho Plan recoge los compromisos internos y externos alineados con los Objetivos de Desarrollo Sostenible (ODS) de Naciones Unidas para la Agenda 2030, estructurándolos en 4 grandes ejes:

- Compromisos con la sociedad: se trata del 70% de las acciones, enfocadas especialmente a temas de prevención para una protección más eficaz de las personas, de igualdad de género y de innovación y emprendimiento.
- Compromisos con los empleados: el 13% de las acciones van dirigidas a favorecer la calidad del clima laboral y fomentar una gestión de las personas basada en la comunicación, la integridad, la participación, la seguridad en el trabajo y la conciliación y orientada a fomentar el compromiso de los empleados con la Agencia.
- Compromisos con el medio ambiente: un 10% de las acciones están relacionadas con el respeto al medio ambiente y la gestión eficiente de los recursos, reduciendo el uso y consumo de papel y mediante el desarrollo y puesta en marcha del proceso de digitalización de documentación, entre otras medidas.
- Compromisos con el buen gobierno y la transparencia: el 7% restante de las acciones están

encaminadas a implantar buenas prácticas que refuercen la confianza en la gestión de la institución y generen una cultura organizativa centrada en valores y compromisos y orientada a la mejora de la gestión, la transparencia, la integridad, la participación y la consecución de resultados.

De todas estas acciones, hay algunas de carácter puntual y no continuas, como la elaboración de determinadas guías y herramientas, pero la

mayoría de las son carácter plurianual, continuidad de actuaciones iniciadas en períodos anteriores, completándose durante los siguientes años. Dada la naturaleza y dimensión de las actividades de AEPD y el cumplimiento de más del 90% de las acciones previstas en el Plan, se hace si cabe más destacable una memoria específica anual 2021 de responsabilidad social que está en proceso de elaboración y que refleja el firme compromiso de la AEPD con un modelo interno de gestión vinculado a la RS, responsabilizándose y comprometiéndose con la generación de un impacto positivo en todas las acciones que desarrolla.

En 2021 se ha desarrollado una nueva iniciativa de la Agencia dirigida a promover un gran acuerdo por la convivencia ciudadana en el ámbito digital compatibilizando la protección de datos con la innovación, la ética y la competitividad empresarial: El Pacto Digital para la Protección de las Personas.

Se trata de una iniciativa dirigida a organizaciones empresariales, fundaciones, asociaciones de medios y grupos audiovisuales para su adhesión a un compromiso con la privacidad en sus políticas de sostenibilidad y en sus modelos de negocio.

En lo relativo al modelo proactivo de cumplimiento del Reglamento, de la experiencia obtenida desde su aplicación efectiva, en 2021 se han puesto de manifiesto deficiencias significativas, en relación con las evaluaciones de impacto en la protección de datos (EIPD) y la gestión de las brechas de seguridad.

Se ha constatado una deficiente calidad de las evaluaciones de impacto que se realizan como un intento de cumplimiento meramente formal sin dar respuesta al enfoque de riesgos para los derechos y libertades de los afectados que exige el principio de responsabilidad proactiva. Esta valoración se detalla en el apartado correspondiente de la Memoria.

En lo que respecta a las brechas de seguridad, en 2021 se constata que las causadas por ciber incidentes de origen interno y malintencionado siguen teniendo el mayor protagonismo, por lo que los responsables y encargados del tratamiento deben ser particularmente diligentes para aplicar medidas técnicas organizativas adecuadas para poder afrontarlas.

En cuanto a las actividades de supervisión de la Agencia cabe destacar los esfuerzos realizados por la Subdirección General de Inspección de Datos, que se han traducido en una mejora de la actividad y de los tiempos de resolución de

las reclamaciones, pese al aumento del número de casos y de la complejidad de las mismas. Su detalle se puede consultar en los apartados correspondientes de la Memoria en cifras.

Las medidas adoptadas para garantizar el derecho a la protección de datos personales se han complementado con el diseño de una estrategia basada en tres pilares: la simplificación y automatización de procesos y actuaciones, la propuesta de modificaciones normativas y la adecuación y reorganización de la plantilla de la Subdirección.

2. Actividades de la AEPD en la pandemia de la COVID-19

Durante el año 2021 la Agencia ha continuado participando de una manera proactiva en la articulación de garantías para la protección de datos personales en los tratamientos llevados a cabo respecto de las medidas adoptadas para hacer frente a la pandemia de la COVID-19.

En particular, en dicho ejercicio, han destacado las relacionadas con la ampliación temporal de los protocolos de monitorización remota de los ensayos clínicos que se describen en la memoria del año anterior, con el fin de posibilitar su aplicación en orden a facilitar dichas modalidades de investigación sanitaria más allá del marco temporal de la pandemia.

Actuación que se complementa con su participación en la **articulación de garantías**, tanto en el ámbito europeo en el seno del Comité Europeo de Protección de Datos (CEPD), como en el ámbito nacional respecto del certificado COVID.

Y la utilización de tecnologías no puede ser considerada de forma aislada, sino enmarcada en una estrategia coherente contra la lucha contra la COVID-19 basada en evidencias científicas, evaluando su necesidad y proporcionalidad, en relación con su eficacia conforme a los criterios de las autoridades sanitarias.

2.1. La monitorización remota de los ensayos clínicos

Como se describe en la memoria del año 2020, la Agencia intervino activamente en la elaboración de un protocolo que permitiera, en el marco de la pandemia, y con el fin de garantizar la seguridad de los sujetos de los ensayos clínicos y de los propios medicamentos, una monitorización remota de los ensayos clínicos.

tización de procesos y actuaciones, la propuesta de modificaciones normativas y la adecuación y reorganización de la plantilla de la Subdirección.

Protocolo que, sintéticamente, se articularon en torno una adenda del contrato firmado entre el promotor del ensayo clínico y el centro donde se realiza la investigación que incorpora dos anexos: un compromiso de confidencialidad del monitor y un protocolo de seguridad para la conexión remota a la información del ensayo.

El protocolo se desarrolló para atender una iniciativa de Farmaindustria, con las finalidades antes indicadas y en colaboración con la Agencia Española del Medicamento y Productos Sanitarios (AEMPS); Agencia esta última que consideró que desde la perspectiva sanitaria la utilización de este protocolo debía quedar limitada al periodo de duración de la pandemia de la COVID-19.

Con el fin de fomentar y facilitar su aplicación, la AEMPS modificó el apartado 63 del anexo VIII.C de sus instrucciones sobre ensayos clínicos

indicando, entre otros aspectos, cuál sería la posición jurídica del promotor del ensayo y del centro donde se realiza la investigación, considerando a ambos como responsables del tratamiento.

Adicionalmente, indicó que los datos del sujeto del ensayo estarían codificados evitando su identificación y que el personal autorizado por el promotor únicamente podría acceder a los datos identificativos para comprobar dichos datos personales coma los procedimientos del estudio clínico y el cumplimiento de las normas de buena práctica clínica; garantizando en todo caso la confidencialidad de los mismos.

En la aplicación del protocolo y de las instrucciones antes citadas se planteó una duda sobre si para permitir el acceso por parte del monitor a los datos identificativos de la historia clínica del paciente, de la que es responsable el centro donde se realiza la investigación, sería necesario que se articulará un contrato de prestación de servicios, es decir, de encargado del tratamiento entre el centro como responsable de dicha historia clínica y el monitor que accede por cuenta del promotor a dicha información.

Atendiendo a una consulta de la AEMPS sobre esta cuestión, la AEPD se pronunció indicando, en los términos contemplados en la legislación sectorial sobre ensayos clínicos, que el promotor es responsable del tratamiento y el monitor es un encargado del tratamiento para cumplir las obligaciones de monitorización que dicha normativa impone al promotor, por cuenta de éste. Excluyendo, por tanto, que el monitor pudiera configurarse como un encargado del tratamiento del centro sanitario para el acceso a los datos identificativos de la historia clínica, si bien, indicando que dicho acceso debería articularse con garantías adecuadas que garantizarán la confidencialidad de la información.

Con posterioridad, la posibilidad de utilizar el protocolo de monitorización remota en los ensayos clínicos más allá del periodo de la pandemia fue objeto de debate en el ámbito europeo y del Grupo de Trabajo de expertos en ensayos clínicos de la Comisión Europea y la Agencia Europea del Medicamento, dando lugar a una nueva consulta sobre su compatibilidad con la normativa de protección de datos personales por parte de la AEMPS.

En respuesta a dicha consulta, la Agencia remitió el informe 38/2021, cuyo contenido se describe en el correspondiente apartado de esta Memoria, en el que, sintéticamente, se formulan las siguientes conclusiones:

- Que para dar respuesta a las mismas el marco jurídico a analizar junto con el RGPD está integrado por el Reglamento (UE) 536/2014 sobre ensayos clínicos en medicamentos y el Real Decreto 1090/2015, de 4 de diciembre, que anticipó su aplicación en nuestro ordenamiento jurídico. Normativa que al regular detalladamente el conjunto de obligaciones de los sujetos intervinientes en los ensayos clínicos condiciona las conclusiones relacionadas con la aplicación del RGPD.

- Que se reitera en las conclusiones del informe 38/2021 sobre la posición jurídica de los sujetos intervinientes en el ensayo, argumentándola detallada y exhaustivamente. Y añadiendo que el monitor no puede ser en modo alguno un encargado del tratamiento del centro sanitario donde se realiza la investigación en lo que respecta al acceso a los datos identificativos de la historia clínica, debiendo garantizarse la obligación de confidencialidad sobre dicho acceso a través de un acto jurídico específico y distinto al de contrato de encargo del tratamiento.

Concluyendo que la monitorización remota de los ensayos clínicos con posterioridad a la pandemia de la COVID-19 es compatible con el RGPD, debiendo quedar la decisión sobre su utilización al criterio de las autoridades sanitarias competentes, que en ese momento optaban por dicha opción a fin de facilitar el desarrollo en los ensayos clínicos en el futuro.

2.2. La protección de datos y el certificado COVID

El desarrollo de vacunas y de procesos generalizados de vacunación, así como la generación de anticuerpos por parte de las personas que han padecido la enfermedad, posibilitó el desarrollo de iniciativas que pudieran eliminar, o al menos reducir, la limitación del derecho fundamental a la libre circulación en la Unión Europea.

Ante la adopción por diversos Estados miembros de iniciativas unilaterales para expedir certificados COVID-19 que podían implicar restricciones del derecho a la libre circulación y dificultar, consiguientemente, el buen funcionamiento del mercado interior, el Consejo Europeo tomó la iniciativa de elaborar un enfoque común, así como avanzar con carácter de urgencia en los trabajos sobre unos certificados digitales interoperables y no discriminatorios en relación con la COVID-19.

Como fruto de esta iniciativa se elaboró una propuesta de reglamento relativo a un marco para la expedición, verificación y aceptación de certificados COVID-19 interoperables de vacunación, de prueba diagnóstica y de recuperación a fin de facilitar la libre circulación durante la pandemia.

La base jurídica de la propuesta fue el artículo 21 del Tratado de Funcionamiento de la Unión Europea, que reconoce y garantiza el derecho a la libre circulación en la Unión. A tal efecto, se señala que las garantías para la libre circulación por razones de salud pública deben responder a los criterios de necesidad y proporcionalidad, basándose en criterios objetivos y no discriminatorios, debiendo garantizarse que los certificados sean interoperables, seguros y verificables.

En relación con la emisión de estos certificados, una de las principales cuestiones que se suscitaron fue la de evitar situaciones de discriminación privilegiando la vacunación. En ello, la iniciativa previó que el certificado verde digital pudiera incorporar tres contenidos: el certificado de vacunación, un certificado que indique el resultado y la fecha de una prueba de no padecer la enfermedad, incluidas las pruebas rápidas de antígenos, y un certificado que confirme que su titular se ha recuperado de una infección de COVID-19 tras una prueba posterior.

Se contempló la posibilidad de emitir en formato digital o en formato papel con un código de barras interoperables que permitiera verificar su autenticidad, validez e integridad, emitiéndose en la lengua del Estado miembro y en inglés, y siendo gratuito Y garantizándose la expedición y verificación segura de los certificados mediante Adicionalmente una infraestructura digital. Las entidades que pueden acceder al certificado quedan limitadas a las autoridades competentes del Estado miembro de destino y a los operadores transfronterizos de servicios de transportes de viajeros (aerolíneas y navieras), que tienen la obligación de colaborar con dichas autoridades.

La conservación de los datos se vinculaba al tiempo necesario para cumplir su finalidad, limitándola al periodo al que los certificados puedan garantizar la libre circulación en el marco de la pandemia.

La propuesta de Reglamento fue objeto de un dictamen conjunto del Supervisor Europeo de Protección de Datos y del Comité Europeo de Protección de Datos (Dictamen 04/2021) que, entre otros aspectos, apreció la compatibilidad del derecho a la protección de datos con las medidas para garantizar la libre circulación transfronteriza y valoró positivamente el certificado verde digital. Valoración positiva que se apoya en la necesidad de realizar un enfoque común para certificados interoperables y eliminar riesgos de falsificación.

Adicionalmente, a estas limitaciones de finalidad y conservación, se valoró positivamente el que se articulara mediante un sistema de información descentralizado.

En particular, la valoración positiva sobre el certificado estuvo relacionada con los riesgos de generar situaciones de discriminación que resultaban minimizados como consecuencia de que, al incluir la vacunación, las pruebas realizadas, incluidas las de antígenos, y la información sobre la recuperación de haber padecido la enfermedad, posibilitaría evitarlas al norte privilegiar ninguna de estas informaciones.

Otra de las cuestiones relevantes que se suscitó fue la relativa a la posibilidad de admitir el tratamiento de la información del certificado con fines ulteriores, señalando que sería admisible, si bien exigiendo nuevos análisis y bases jurídicas e incorporando en todo caso las garantías recogidas en el dictamen.

A este respecto, el considerando 48 del Reglamento aclara que "los Estados miembros pueden tratar los datos personales con otros fines si la base jurídica para su tratamiento con otros fines, incluidos los plazos de conservación correspondientes, está establecida en el derecho nacional, que deberá cumplir con el derecho de la Unión en materia de protección de datos y los principios de eficacia, necesidad y proporcionalidad, y debe incluir disposiciones específicas que determinen claramente el ámbito y aplicación y el alcance del tratamiento, la finalidad específica de que se trate, las categorías de entidades que puedan acreditar el certificado, así como las salvaguardas pertinentes para evitar la discriminación y el abuso, teniendo en cuenta los riesgos para los derechos y libertades de los interesados. Cuando el certificado se utilice con fines no médicos, los datos personales a los que se acceda durante el proceso de verificación no deben conservarse, según lo dispuesto en el presente Reglamento.

Atendiendo a la evolución de la pandemia en los territorios de las distintas comunidades autónomas, la utilización del certificado COVID para fines distintos a los inicialmente previstos en el Reglamento europeo, ha sido una de las principales medidas adoptadas por las autoridades sanitarias competentes exigiendo su exhibición para el acceso a una diversidad de locales y establecimientos.

Conforme a las previsiones de la Ley reguladora de la Jurisdicción Contencioso-administrativa, la eficacia de estas medidas debe someterse a la ratificación judicial por parte de los Tribunales Superiores de Justicia de cada comunidad autónoma, que en unas ocasiones las han ratificado y en otras no, lo que ha dado lugar a la interposición de recursos de casación ante el Tribunal Supremo.

De sus sentencias, cabe destacar las de 14 de septiembre y 1 de diciembre de 2021 en las que se analiza el posible conflicto entre las medidas adoptadas por las autoridades sanitarias entre los derechos fundamentales a la vida, la integridad física y la defensa y protección de la salud de los ciudadanos respecto de los derechos a la igualdad, a la intimidad y a la protección de

datos personales. Si bien dicho análisis se realiza teniendo en cuenta las circunstancias sanitarias concurrentes en cada comunidad autónoma y, en función de las mismas, se analiza la concurrencia de los principios de idoneidad proporcionalidad y necesidad. Partiendo de dicho análisis el Tribunal concluye, sintéticamente, que los derechos fundamentales no son absolutos ni ilimitados y que su limitación puede ser necesaria para coexistir con los restantes derechos fundamentales y bienes constitucionalmente protegidos considerando en el caso analizado la prevalencia del derecho a la vida y a la integridad física y a la defensa de la protección de la salud de los ciudadanos. Y cita, como base jurídica, que legítima el tratamiento de datos la Ley Orgánica 3/1986, de medidas especiales de salud pública, en la Ley 14/1986, General de Sanidad y en la Ley 33/2011, General de Salud Pública con el complemento de la autorización de los Tribunales antes indicada.

En lo que respectan al derecho fundamental al tratamiento de datos personales, la sentencia no realiza, en sentido estricto, una ponderación, sino que concluye directamente que no se aprecia limitación alguna del mismo.
En este sentido, argumenta que las medidas adoptadas se limitan a la mera exhibición del certificado para entrar en el interior de los establecimientos señalados "sin que, desde luego, puedan recogerse los datos de los asistentes a tales locales, ni pueda elaborarse un fichero, ni hacer un tratamiento informático al respecto" concluyendo que, en los términos descritos, no concurre un tratamiento de datos personales.

3. Desafíos para la privacidad

3.1. Pacto Digital para la Protección de las Personas

En enero de 2021 tuvo lugar el lanzamiento del *Pacto Digital para la Protección de las Personas*, iniciativa que promueve y persigue un gran acuerdo por la convivencia ciudadana en el ámbito digital, compatibilizando la protección de datos con la innovación, la ética y la competitividad empresarial.

El Pacto se presentó en el 'I Foro de Innovación, privacidad y sostenibilidad', que se celebró el 28 de enero de 2021 con ocasión del Día Internacional de la Protección de Datos.

El Pacto nace del compromiso que la Agencia, como organismo público, tiene con la sociedad para reforzar los derechos en el entorno digital, así como la protección de las personas en internet y concienciar a la vez de que junto a un derecho puede existir también una obligación.

La adhesión al Pacto supone asumir el compromiso con los principios y valores que contiene, como la ética digital, y las recomendaciones que incluye, como la de informar a las personas sobre el tratamiento de sus datos y el ejercicio de sus derechos, aplicar los principios de protección de datos, garantizar su licitud, la designación de delegados de protección de datos, o aplicar los principios de privacidad desde el diseño y por defecto, pero sin añadir más obligaciones que las que legamente corresponden.

La difusión del *Canal prioritario* entre los empleados y clientes de las entidades adheridas como herramienta para paliar situaciones de violencia digital y los materiales que la AEPD ha elaborado con la finalidad de sensibilizar sobre el valor de la privacidad y la importancia del tratamiento de los datos personales, en particular en el entorno laboral son otros de los compromisos que en la medida de sus posibilidades se asumen con la adhesión.

El Pacto recuerda las responsabilidades penales, civiles, laborales y administrativas que pueden derivarse de los tratamientos, difusiones, de datos un tratamiento sin la debida legitimación.

Así mismo, una parte importante del Pacto por su impacto en la sociedad la constituye el Decálogo

de buenas prácticas en privacidad para medios de comunicación y organizaciones con canales de difusión propios, con el que la Agencia quiere promover la lucha contra la violencia digital tanto entre los medios de comunicación como con todas aquellas organizaciones que disponen de canales de difusión para informar sobre temas de interés para sus públicos.

En este primer año se han celebrado un total de ocho reuniones con entidades adheridas del ámbito empresarial, del tercer sector y de los medios de información en las que se les informó de los distintos materiales y herramientas que facilitan el cumplimiento de la normativa aplicable; y presentar el Pacto a entidades que se interesaron por su adhesión.

El año finalizó con 349 entidades adheridas al Pacto Digital

3.2. Jurídicos

3.2.1 Consultas

Transcurridos más de tres años de aplicación del Reglamento General de Protección de Datos, se observa la importancia del nuevo modelo de cumplimiento basado en el principio de responsabilidad proactiva. Este nuevo paradigma ha tenido su reflejo tanto en las consultas planteadas como en los informes del Gabinete Jurídico sobre ellas, resaltando las implicaciones del citado principio y sus manifestaciones que se proyectan, no sólo en el aspecto formal, sino que abordan todos los ámbitos del tratamiento de datos de carácter personal.

Asimismo, ha sido un ejercicio que sigue marcado por la pandemia de COVID-19 con implicaciones tanto en las consultas sobre el modo de aplicar la normativa de protección de datos por parte de responsables y encargados del tratamiento, como respecto de los proyectos normativos objeto de informe preceptivo de la Agencia que siguen planteando la necesidad de establecer los criterios de aplicación del RGPD en este escenario.
Se consagra así, como un elemento fundamental en la normativa de protección de datos, la exigencia de realizar una permanente revisión de los procesos de tratamiento de datos para su adecuación al Reglamento en un contexto dinámico.

Al igual que en el ejercicio anterior, cuestiones clásicas como los tratamientos de categorías especiales de datos, y el rol de los intervinientes en el tratamiento de datos han centrado buena parte de las consultas, así como la adaptación de determinados tratamientos a la situación que se ha producido con la pandemia en distintos ámbitos que, como veremos ha tenido incidencia no sólo directa sino también indirecta y que hace necesaria una revisión del modo de proceder y en consecuencia de aplicar la normativa de protección de datos.

Otro aspecto destacable ha sido la tendencia que se ha observado en los tipos de consultas, y, en consecuencia, de los informes que se han emitido, al haber disminuido las consultas planteadas por los responsables y encargados y aumentar las solicitudes de informe sobre proyectos normativos. Esta tendencia es una manifestación más de la aplicación principio de responsabilidad proactiva por parte de responsables y encargados del tratamiento.

Estrechamente relacionado con ese aspecto, hay que resaltar la aprobación de 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,* que reitera la implicación de los responsables y encargados, a la hora de analizar los riesgos del tratamiento de datos personales y las garantías que permitan mitigarlos y la necesaria intervención del Delegado de Protección de Datos.

Centrándonos en las consultas concretas que se han planteado deben tenerse en cuenta en primer lugar las relativas a los tratamientos de datos relacionados con la pandemia de COVID-19 que

ha dado lugar a los informes que se mencionan a continuación.

El **Informe 13/2021** analiza la adecuación a la normativa de protección de datos del tratamiento referido al cobro del complemento de productividad de los empleados públicos y en concreto a su publicación en la intranet corporativa de la consultante, la CNMC.

Se incide en la posibilidad de que habida cuenta de la actual situación ocasionada por el COVID-19 y considerando que el personal de la entidad consultante presta servicios en modalidad no presencial-, se proceda a la publicación del listado de la productividad individual en la Intranet corporativa, al menos con carácter excepcional. Asimismo, se cuestiona en qué condiciones debería realizarse la publicación y cuáles deberían ser los datos objeto de publicación.

Las cuestiones planteadas en la consulta han sido analizadas por la Agencia en varios informes -por todos los 123/2017, 137/2010, 183/2018 y 36/2019-, en los que se señala la conveniencia de conciliar el derecho de los funcionarios a conocer la asignación del complemento de productividad con el derecho a la protección de sus datos de carácter personal, evitándose la exposición pública de la información, pero sin limitar el acceso a la misma. Se recuerda que, en relación con la publicidad de la productividad de los funcionarios públicos, se ha venido considerando necesario que el acceso a los datos no dé lugar a tratamientos posteriores que puedan resultar contrarios a lo dispuesto en la legislación de protección de datos o genere situaciones en que pueda poner en riesgo los derechos de los empleados. Ello podría lograrse, por ejemplo, estableciendo sistemas que, garantizando el libre acceso a la información y la transparencia exigida por el artículo 23.3 c) Ley 30/1984, de 2 de agosto no permitiesen la reproducción de los datos.

Así, la publicación resulta necesaria para el cumplimiento de una obligación legal aplicable al responsable del tratamiento, concurriendo la base jurídica prevista en la letra c) del artículo 6.1.del RGPD, y estableciéndose dicha obligación en una norma con rango de ley, conforme al artículo 8 de la LOPDPGDD.
Ahora bien, como medio preferente para proceder a dicha publicación, se indica que se realice en un espacio físico de acceso restringido en favor de aquellas personas legitimadas para dicho acceso, y que se adopten las medidas necesarias para evitar su público conocimiento por el resto de los empleados públicos y/o terceros, de forma que suponga la menor injerencia en los derechos y libertades de los interesados. Esta premisa excluye la posibilidad de un conocimiento generalizado de dicho complemento retributivo, como podría ocurrir en el caso de que se procediera a su publicación en internet, en el que el riesgo se incrementaría como consecuencia de la posible indexación por los motores de búsqueda.

En consecuencia, el informe indica que la publicación deberá realizarse en un espacio privado de la intranet de manera que sólo puedan acceder a los datos el personal funcionario, adoptándose las oportunas medidas de seguridad que eviten la reproducción de los datos, así como el acceso indebido a los mismos, teniendo en cuenta lo dispuesto en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Por lo que, sin perjuicio de que corresponde apreciar la necesidad de dicha publicación ante la situación de la pandemia al responsable del tratamiento por aplicación del principio de responsabilidad proactiva (artículo 5.2 RGPD), concluye el informe que la opción de la publicación de la productividad del personal funcionario en la intranet administrativa resulta ponderada y conforme con la normativa de protección de datos.

La publicación de los datos deberá ajustarse a los fines que justificaron su tratamiento, y, tal y como exige el artículo 5 del RGPD, realizarse con pleno respeto a los principios de minimización de datos, limitación del plazo de conservación, e integridad y confidencialidad, de modo que la publicación suponga la menor injerencia en los derechos y libertades de los interesados,

Así la publicación de dichos datos retributivos deberá limitarse a la identificación concreta de las personas afectadas por indicación de su nombre y apellidos, y a la mención a la cuantía percibida y al periodo temporal al que se refiere dicha percepción económica, sin que proceda la publicación del número de su DNI, por aplicación de lo previsto en el apartado 1 párrafo primero de la disposición adicional séptima de la LOPDGDD. Por lo tanto, solo en el caso de coincidencia del nombre y apellidos, podrán publicarse cuatro cifras aleatorias de su documento nacional de identidad. Asimismo, dicha publicación de datos personales en la intranet administrativa del órgano consultante, habrá de ajustarse al estricto cumplimiento de lo dispuesto por el artículo 5.1 b) del RGPD, no pudiendo usarse los datos de carácter personal objeto de tratamiento para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. A su vez, de acuerdo con lo dispuesto en el artículo 5.1 e) del RGPD, la publicación de dichos datos personales en la citada intranet administrativa deberá suprimirse -procediéndose al borrado de los datos publicados-, cuando hayan dejado de ser necesarios o pertinentes para la finalidad que motivó dicha publicación.

Finalmente, el informe pone de manifiesto la necesidad de que por los órganos competentes se impulse la correspondiente modificación normativa que garantice la seguridad jurídica exigible en orden a la mejor interpretación y aplicación del mandato contenido en el artículo 23.3.c) de la Ley 30/1984, de 2 de agosto.

El **Informe 25/2021** tiene por objeto el análisis sobre la adecuación a la normativa de protección de datos de la solicitud de información recibida en la Consejería de Salud del Principado de Asturias (SESPA), por parte de un parlamentario de la Junta General del Principado de Asturias sobre la relación de altos cargos y cargos directivos del citado principado, sus organismos autónomos, entes públicos y empresas públicas a los que se les ha suministrado alguna de las vacunas contra la COVID-19.El informe destaca las implicaciones del principio de responsabilidad proactiva cuyas consecuencias son entre otras, que previo asesoramiento del Delegado de Protección de Datos, corresponde al responsable de tratamiento, SESPA, determinar la base jurídica del tratamiento de datos planteado. A pesar de que teniendo en cuenta lo indicado, no procedería la emisión de informe, “dada la generalidad con la que se están planteando las solicitudes de información de parlamentarios en relación con las personas que han recibido la vacuna contra la COVID-19”, se consideró oportuno, por razones de seguridad jurídica, analizar, con carácter general, el régimen jurídico aplicable a los tratamientos que se derivan de la consulta.

El informe tras analizar las implicaciones del tratamiento de categorías especiales de datos, y el aspecto concreto referido a que la solicitud la realiza un miembro del parlamento autonómico y que el derecho a la información de los diputados forma parte del derecho fundamental reconocido en el artículo 23 de la Constitución (STC 203/2001 de 15 de octubre) y a su vez las preguntas parlamentarias forman parte de la función de control de la acción del Gobierno, señala que el tratamiento de categorías especiales de datos, podría ampararse en el artículo 9.2.g) del RGPD, siempre y cuando concurran todos los requisitos previstos en el mismo, recordando la doctrina del Tribunal Constitucional en Sentencia de 76/2019, de 22 de mayo de 2019, sobre “el interés público esencial”. Y destaca que resulta determinante analizar si dicha norma ha procedido a la identificación de los fines de interés público esencial y la apreciación de la proporcionalidad del tratamiento al fin perseguido, y si la misma ha previsto las garantías adecuadas, teniendo en cuenta que la exigencia general de dichas garantías se refuerza cuando se trata de categorías especiales de datos personales, tal y como resulta del artículo 9.2.g) del RGPD, que se refiere a las “medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado” y del artículo 9.2 de la LOPDGDD, que prevé que dichos tratamientos “deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad” Y que” deberá analizarse si el tratamiento pretendido es, “necesario” y “proporcional al objetivo perseguido”, debiendo tenerse en cuenta

la doctrina sobre el principio de proporcionalidad establecida por el Tribunal Constitucional y que recuerda la Sentencia 14/2003, de 28 de enero".

Concluye el informe señalando que "no corresponde a esta Agencia, sino a la Mesa de las Cámaras la interpretación y aplicación de las normas citadas a efectos de valorar la existencia y suficiencia de las garantías adecuadas que puedan haberse previsto en los correspondientes Reglamentos y la necesidad y proporcionalidad del tratamiento y, en su caso, de los datos concretos que deban ser comunicados en caso de petición. En caso contrario, esta Agencia estaría usurpando las competencias atribuidas al Órgano de Gobierno de una Asamblea Parlamentaria elegida democráticamente, lo que no resultaría ajustado a derecho, tal y como se ha venido indicando en los numerosos informes relacionados con esta cuestión. Por consiguiente, en los supuestos en que, en el ejercicio del derecho de información de los diputados, se soliciten datos de carácter personal, el cumplimiento de la normativa sobre protección de datos personales corresponde, en primer lugar, al órgano administrativo que ostente la condición de responsable del tratamiento asesorado, en su caso, por el delegado de protección de datos y, posteriormente, a la Mesa de la Cámara, de conformidad con el correspondiente Reglamento parlamentario, sin perjuicio del posterior control jurisdiccional."

En el **Informe 32/2021** se plantea la adecuación al a normativa de protección de datos la comunicación por parte del Servicio de Salud de Illes Balears a la Oficina de Prevención y Lucha contra la Corrupción de los datos personales de todos los ciudadanos vacunados sin que éstos estuvieran anonimizados.

Al igual que en el Informe 25/2021 antes referido, se pone de manifiesto que el responsable del tratamiento en cumplimiento del principio de responsabilidad proactiva debería haber aportado un análisis motivado y detallado de las cuestiones planteadas, atendiendo a la naturaleza de la entidad consultante y la entidad requirente de la información, así como a la normativa, jurisprudencia y doctrina aplicable.

No obstante, dado el interés general apreciable en la consulta remitida se entra a analizarla.

- En primer lugar, se analiza la naturaleza y estatus jurídico de la solicitante de la información, la Oficina de Prevención y Lucha contra la corrupción, como una Entidad de Derecho Público, adscrita al Parlamento. Es decir, un órgano auxiliar de los órganos parlamentarios, participando en el control político que corresponde a los mismos, quedando excluida de su competencia las funciones que corresponden a la autoridad judicial y al ministerio fiscal, y estando sujetas sus actuaciones al RGPD y no a la Directiva (UE) 2016/680.

- En segundo término, se aborda ya la consideración de categorías especiales de datos que tienen los datos de salud y los supuestos que permiten su tratamiento, recordando la doctrina constitucional de la apreciación del interés público esencial (STC 76/2019 de 22 mayo), la aplicación del principio de proporcionalidad (STC 14/2003, de 28 de enero) y lo indicado en otros informes de la Agencia (31/2019 y 36/2020).

- Concluye que a pesar de que la lucha contra la corrupción puede considerarse, a los efectos del artículo 9.2.g) del RGPD, como un interés público esencial, el acceso a determinados datos de salud, como los analizados, se considera excesivo y contrario a la normativa sobre protección de datos personales, por varias cuestiones: nada se indica en el requerimiento de información respecto de la finalidad concreta para la que se reclama la información, y el citado precepto requiere que el tratamiento sea necesario, y no se justifica en el requerimiento la necesidad de acceder a los datos personales de las personas vacunadas en relación con la investigación que se está realizando, lo que requeriría la realización del triple juicio de idoneidad, necesidad y proporcionalidad, valorando si la comunicación de datos personales relativos a la salud de determinadas personas es necesaria para el cumplimiento de la finalidad de control de la acción administrativa perseguida, y si dicha finalidad no puede alcanzarse por otros

medios que no requieran la comunicación de dichos datos, como podría ser, por ejemplo, la comunicación de la información agregada (es decir, anonimizada, de forma que no permita la identificación de personas físicas) referida a los distintos grupos de vacunación previstos en los protocolos de vacunación o la no pertenencia a alguno de ellos, indicando el número total de personas que se encontrarían en cada uno de esos supuestos.

Finalmente, el informe que el requerimiento analizado supone un tratamiento masivo de datos personales que, afectaría, al menos, a 108.500 personas, lo que es contrario al principio de minimización de datos y a la doctrina del Tribunal Constitucional y del Tribunal de Justicia de la Unión Europea anteriormente citada.

En el **Informe 29/2021** se aborda otra situación provocada por la pandemia, referida a la cesión por parte de la Comisión Nacional de los Mercados y la Competencia (CNMC) al Ministerio de Educación y Formación Profesional de los números de teléfono de los hogares seleccionados por el Instituto Nacional de Estadística para realizar las entrevistas que forman parte del Programa para la Evaluación Internacional de Competencias de la Población Adulta de la OCDE (PIAAC, por sus siglas en inglés),que forma parte del Plan Estadístico Nacional vigente y cuya gestión en España corresponde al Instituto Nacional de Evaluación Educativa (INEE), ante la imposibilidad, derivada de la situación de pandemia y la necesidad de seguir los protocolos sanitarios recomendados por las autoridades sanitarias de distancia social y minimización de reuniones en lugares cerrados, evitando llevarla a cabo mediante la visita del entrevistador al hogar para realizar una entrevista presencial.

En el informe se resalta la circunstancia de que la comunicación de los números de teléfono por parte de la CNMC a los servicios estadísticos de distintos organismos para la realización de encuestas incluidas en el Plan Estadístico Nacional, ya se ha plantado en numerosas ocasiones, y que el criterio relevante al objeto de determinar la forma en la que procederá dicha comunicación no deriva de la obligatoriedad de la realización de la encuesta por el organismo público correspondiente, sino en la obligatoriedad de su cumplimentación por parte de los afectados. Resultando de aplicación el criterio mantenido en los informes 75/2020 y 78/2020, y por tanto concluye que la comunicación de los números de teléfono por la CNMC al Instituto Nacional de Evaluación Educativa se encuentra amparada por el RGPD siempre y cuando, tal y como ya se señalaba en el Informe 70/2015, el dato sea únicamente utilizado para la realización de la estadística en cuyo ámbito es solicitado. Y se insiste en la necesidad, ya indicada en los informes anteriores, de que se impulse la correspondiente modificación legislativa que garantice la seguridad jurídica y la adecuación de los correspondientes tratamientos de datos personales al RGPD y a la doctrina del Tribunal Constitucional, mediante el establecimiento de las garantías específicas que se estimen adecuadas.

En el **Informe 60/2021** se aborda una situación similar a la descrita en el anterior informe, en el que se plantea por la CNMC la adecuación a la normativa de la solicitud recibida por la Delegación del Gobierno Contra la Violencia de Género de la Secretaría de Igualdad del Ministerio de Igualdad, referida a los números de teléfono móviles y fijos de una muestra de mujeres para poder realizar telefónicamente la Encuesta Europea de Violencia de Género que forma parte del Plan Estadístico Nacional vigente. Se motiva la solicitud en el escenario de pandemia, resaltando la necesidad de realizar las encuestas telefónicamente ante circunstancias como las limitaciones de desplazamientos provinciales e interprovinciales, el posible rechazo a la entrada en los domicilios o la necesidad de garantizar distancias de seguridad.

En el informe, tras analizar lo indicado en otros anteriores sobre supuestos similares (49/2020, 78/2020), se pone especial atención a que la encuesta implica el tratamiento de datos personales incluidos dentro de las categorías especiales de datos y que, en todo caso, sólo serán facilitados voluntariamente. Por lo tanto, para que proceda la comunicación de los números de teléfono de los abonados que están en poder de la CNMC al CIS deberían adoptarse garantías adicionales, además de las genéricas derivadas de la normativa sobre Función Estadística Pública, incluido el secreto estadístico, así como del Código

de Buenas Prácticas de las estadísticas europeas. Sin embargo, no queda acreditada la necesidad de la comunicación de los datos personales correspondientes a los números de teléfono por parte del Ministerio de Igualdad. En consecuencia, se considera que únicamente procederá dicha comunicación, con las garantías señaladas, si se acredita debidamente que la pandemia lo hace estrictamente necesario ante la imposibilidad de llevar a cabo las encuestas presencialmente o si, como consecuencia de la pandemia, la tasa de respuesta de entrevista personal es baja.

Finaliza el informe retirando una vez más, la necesidad de proceder a una modificación legislativa que garantice la seguridad jurídica y la adecuación de los correspondientes tratamientos de datos personales para la realización de encuestas telefónicas al RGPD y a la doctrina del Tribunal Constitucional, mediante el establecimiento de las garantías específicas que se estimen adecuadas, tal y como se puso de manifiesto en el Informe 46/2021, referente al Anteproyecto de Ley General de Telecomunicaciones.

Dejando las cuestiones conexas con la pandemia del COVID-19, a continuación, podemos distinguir otro bloque de informes referidos a los intervinientes en el tratamiento de datos personales, a la consideración de responsables o encargados y en consecuencia a las obligaciones que les incumben.

En el **Informe 70/2021** se aborda la consideración que debe tener, como responsable o encargado del tratamiento, una empresa que presta servicios a una Comunidad de Propietarios, consistentes en la lectura, mantenimiento y conservación de contadores, y emisión de liquidaciones de consumo de agua.

Se recuerda el criterio que se ha seguido en relación con la aplicación de la normativa de protección de datos a las Comunidades de Propietarios, en sus relaciones con terceros prestadores de servicios, señalando que, con carácter general y salvo excepciones, serán considerados encargados del tratamiento. Así se deduce, por ejemplo, de la prestación del servicio que realice el Administrador de Fincas contratado al efecto. Es decir, cuando estos actúan por cuenta de las comunidades de propietarios, están legitimados para tratar y disponer de los datos de los copropietarios que resulten necesarios para la gestión ordinaria de los asuntos de la comunidad, ya que actúan en relación con las comunidades a las que prestan servicios como encargados de tratamiento. Asimismo, las comunidades de propietarios respecto del tratamiento de datos de los comuneros se encuentran legitimados, a los efectos de las causas que recoge el RGPD, en el cumplimiento de una obligación legal en consonancia con el articulado de la Ley de Propiedad Horizontal (LPH).

En el caso concreto de la consulta se está ante un servicio que un tercero presta a la Comunidad de Propietarios y se analiza el contrato que se aporta al efecto y las manifestaciones realizadas, en relación con las Directrices 07/2020 del Comité Europeo de Protección de Datos (CEPD) sobre los conceptos de responsable del tratamiento y encargado en el RGPD. Llegando a la conclusión de que la entidad es encargada del tratamiento derivado de varios elementos que las directrices indicadas consideran fundamental, como es la influencia determinante en el tratamiento; la posibilidad de mantener o modificar los términos del servicio, en el sentido de que la consultante no se encuentra en condiciones de modificar el servicio contratado para cambiar elementos del tratamiento; el tratamiento en sí mismo considerado constituye un elemento clave del servicio, concluyendo que el tratamiento de datos personales es fundamental, y no meramente accesorio, en la prestación del servicio; y respecto del establecimiento de relaciones directas con los titulares de los datos, se indica que los titulares de los datos objeto de tratamiento no tienen una relación jurídica con la consultante, sino que es la Comunidad a la que se le presta el servicio la titular de dicha relación. E incluso la propia literalidad y contenido del contrato, en el sentido de que en él se asignan las responsabilidades y roles en cuanto a responsable y encargado y no existen o, al menos de la información y de las manifestaciones realizadas por la consultante, no se desprende que la realidad del servicio contravenga dichos roles.

En el **Informe 84/2021** se analiza la consideración de responsable o encargado del tratamiento que deben tener los intervinientes en la gestión del negocio de las Instituciones de Inversión Colectiva. (IIC). Este informe matiza el criterio seguido en el Informe 12/2021 a raíz de la aportación de elementos nuevos que han sido objeto de análisis y que en aquel no se pusieron de manifiesto.

En este ámbito operan de un lado, las Sociedades Gestoras de Instituciones de Inversión Colectiva (SGIIC), que, en síntesis, venden suscripciones o participaciones de las IIC a los potenciales inversores, utilizando éstos para efectuar la correspondiente adquisición a las Entidades de Servicios de Inversión (ESI)y cuya compra se canaliza a través de una tercera entidad, aquella que actúa como plataforma de distribución y que será el nexo entre la SGIIC y la ESI.

Existiendo, por tanto, varias relaciones a analizar, la de la SGIIC con la plataforma de distribución, la de la plataforma de distribución con la ESI, y la de la ESI con sus clientes.

Pues bien, se considera de un lado, como responsable del tratamiento en el momento en el que se formaliza la compra de las participaciones a la SGIIC, por cuanto los datos de los inversores necesitan ser tratados por ésta en la medida en que se han convertido parte de la IIC.

Ahora bien, antes de formalizar la compra, serán las ESI las responsables del tratamiento de los datos de los potenciales inversores en la medida en que son clientes de aquella. En efecto, la iniciativa de comprar las participaciones nace en el seno de la ESI, que promociona a través de sus clientes la compra de suscripciones o participaciones. En este estadio, existirá un contrato de servicios de inversión en virtud del cual la ESI va a buscar la mejor opción (participaciones o suscripciones) que sirva a los intereses de sus clientes. Y cuando se formalice la compra entre el potencial inversor y la SGIIC, existirá un contrato de inversión y en ese momento la SGIIC se convertirá en responsable de los datos de "sus nuevos clientes".

En el informe tras un análisis exhaustivo de los contratos entre la SGIIC y la plataforma de distribución, y la ESI y la plataforma de distribución se concluye:

- En primer lugar, que la plataforma de distribución será considerada como una encargada del tratamiento de la ESI, en la medida en que pone a disposición de esta su plataforma tecnológica para posibilitar que los potenciales inversores y clientes de la ESI, puedan adquirir las participaciones.

- En segundo lugar, y sin perjuicio de que la plataforma de distribución tenga un contrato con la SGIIC, su relación no se establece en términos de responsable (SGIIC) y encargado (plataforma de distribución), sino que son dos entidades independientes con autonomía plena, en definitiva, que no se dan los elementos propios de dicha relación de responsable y encargado ya que, en puridad, la plataforma de distribución "no presta un servicio propio de la SGIIC", ni recibe instrucciones sobre cómo llevar a cabo el tratamiento de los datos.

Por último, debe citarse el **Informe 20/2021** que tiene especial relación con el cumplimiento del principio de responsabilidad activa y que tiene como antecedente el informe preceptivo 97/2020 referido al Proyecto de Orden de la Ministra de Asuntos Económicos y Transformación Digital sobre los métodos de identificación no presencial para la expedición de certificados electrónicos cualificados. En aquel informe se echó en falta dadas las implicaciones del tratamiento que pretendía regular el proyecto, el correspondiente análisis de riesgos, y en su caso, evaluación de impacto.

En concreto se indicaba: en virtud del principio de responsabilidad proactiva, al regular en el artículo 5 los requisitos generales de seguridad debería incluirse expresamente la necesidad de realizar el análisis de riesgos para los derechos y libertades de las personas físicas que exige el artículo 24 del RGPD, atendiendo a los principios de privacidad por defecto y desde el diseño contemplado en el artículo 25 del RGPD y la necesidad de realizar

una EIPD conforme al artículo 35, previendo expresamente que, en medidas a implantar como consecuencia del citado análisis de riesgos prevalecerán sobre cualquier otra. Asimismo, dichas medidas deberán revisarse y actualizarse cuando sea necesario, lo que ocurrirá no solo en el caso de que se produzcan cambios en el sistema, como prevé el artículo 5.1. de la Orden, sino en cualquier momento en que se tenga conocimiento de que las mismas no son adecuadas o no son suficientes, como puede ser cuando se tenga conocimiento de vulnerabilidades que puedan dar lugar a brechas de seguridad y para las que no haya solución en ese momento, o por modificaciones en el contexto, los procedimientos organizativos o por los avances tecnológicos. Por esa misma razón, debería hacerse referencia al establecimiento de auditorías de privacidad y revisión continua de las medidas de privacidad encaminadas a la mejora continua del cumplimiento normativo en materia de protección de datos y a la implantación de las medidas correctoras necesarias para mejorar la seguridad de los datos personales. Se trata, en definitiva, de adoptar un modelo de gestión continua del riesgo,(…) Por todas las razones expuestas en los apartados anteriores, se considera necesario una revisión del texto remitido al objeto de garantizar el cumplimiento de la normativa de protección de datos personales, valorando todos los riesgos que la aprobación de la norma puede suponer para los derechos y libertades de los afectados, para la plena efectividad de las previsiones del RGPD y de la LOPDGDD de acuerdo con los criterios jurisprudenciales citados en el presente informe.

El informe se emite favorablemente habida cuenta de que se ha aportado incluido un nuevo apartado en la Memoria de Análisis de Impacto Normativo relativo a la "Evaluación de impacto de riesgos en materia de protección de datos personales" y se han efectuado las oportunas modificaciones en el preámbulo y en el articulado.

Los informes que a continuación se citan, conforman un tercer bloque por cuanto tienen como denominación común que se refieren a tratamientos de datos muy concretos con características particulares que merecen especial atención.

El **Informe 30/2021** se emite a raíz de una consulta surgida en el Grupo de Trabajo formado por la AEPD, la Unidad de Criminalidad Informática de la Fiscalía General del Estado, la Secretaria de Estado de Seguridad del Ministerio del Interior, la Dirección General de Telecomunicaciones y Ordenación de los Servicios de Comunicación Audiovisual de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales del Ministerio de Asuntos Económicos y Transformación Digital las principales Operadoras de Servicios de Telecomunicaciones y la Asociación Española de Banca, y que tiene por objeto analizar los aspectos fundamentales de la estafa conocida como Sim Swapping o duplicación fraudulenta de tarjetas sim, desde una perspectiva multisectorial.

SIM Swapping es el término coloquial a través del que se conoce este tipo de estafa que consiste, en que un tercero ajeno al titular de la tarjeta SIM, solicita a la operadora correspondiente un duplicado de dicha tarjeta SIM (que supone la anulación de la anterior tarjeta SIM), para recibir en dicho duplicado los mensajes de texto SMS que la entidad bancaria envía a sus clientes como medida de seguridad para confirmar determinadas operaciones bancarias.

Este tipo de estafa requiere que previamente el tercero haya conseguido hacerse con las credenciales de la víctima para acceder y autenticarse en el servicio de banca electrónica.

Una vez que el tercero tiene acceso a los servicios de banca electrónica y a la tarjeta SIM de la víctima (tarjeta duplicada), puede operar con total libertad para realizar movimientos en las cuentas corrientes y otros productos financieros de aquella, pues la realización de cualquier operación pasa por el envío de un mensaje SMS de confirmación a la línea de teléfono que el afectado haya proporcionado a la entidad bancaria a esos efectos, y que en este caso, ha sido duplicada y está en poder de dicho tercero.

Teniendo en cuenta lo indicado, la consulta se centra en la adecuación al marco jurídico vigente respecto del acceso por parte de las Fuerzas y Cuerpos de Seguridad del Estado (FCS en lo

sucesivo), a la información de la que disponen las Operadoras de Telecomunicaciones (las operadoras en lo sucesivo) derivado de los servicios que prestan y de las posibilidades de que conforme a la ley puedan mejorar el sistema para la lucha contra este tipo de estafas.

En el informe se analiza la implicación el tratamiento de datos que se da en este tipo de estafas y su investigación por parte de las FCS, para establecer la siguiente conclusión:

- En primer lugar debe indicarse que si bien la STJUE de 8 de abril de 2014, Asunto C-293/2012 invalidó la Directiva 2006/24/CE de 15 de marzo de 2006, por la falta de proporcionalidad que podía suponer la aplicación de sus disposiciones, el Tribunal Supremo en Sentencia núm. 727/2020 de 23 de marzo deja claro que las deficiencias advertidas en la ciada Directiva no se producen en el actual ordenamiento jurídico nacional, y recuerda la plena vigencia de la Ley 25/2007 de 18 de octubre y su coexistencia con los preceptos de la LECrim. Por lo tanto, el acceso a la información sobre el IMEI y el IMSI resultaría conforme a derecho en los cumpliendo los requisitos indicados en la citada normativa, ya estén vinculados a un proceso de comunicación, o simplemente persigan la identificación de su titular al margen de dicho proceso de comunicación.

- En segundo lugar, y en relación con lo anterior, el acceso por parte de las FCS y el Ministerio Fiscal a los datos referidos a la vinculación entre el IMEI del dispositivo dónde se usa la SIM duplicada y la propia SIM salvo mejor criterio de aquellos organismos o instituciones con competencias en este ámbito, no requerirá autorización judicial siempre y cuando la petición no esté vinculada a un proceso de comunicación concreto, en cuyo caso, se aplicaría la Ley 25/2007 de 18 de octubre.

- En tercer lugar, el tratamiento de datos personales de los afectados consistente en la comunicación por parte de las operadoras a las FCS y al Ministerio Fiscal de información sobre las circunstancias de la solicitud de duplicado de la tarjeta SIM y su activación, en el marco de una investigación por la comisión de delitos, se encuentra amparado con carácter general, desde el lado de las operadoras en el artículo 6.1 c) del RGPD, y una vez que la información obre en poder de las FCS y/o del Ministerio Fiscal, se encuentra amparado en 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, todo ello de conformidad con lo dispuesto en el artículo 588 ter m) de la LECrim.

- En cuarto lugar, debe indicarse que la operativa técnica en que se produzca dicha comunicación, en relación con el acceso condicionado por el modo o manera en que las operadoras de telecomunicaciones almacenan los datos de tráfico son cuestiones ajenas a la competencia de la Agencia Española de Protección de Datos.

- Y por último debe indicase que corresponde a las operadoras de telecomunicaciones y a las entidades bancarias cumplir lo dispuesto en el RGPD en tanto responsables del tratamiento de los datos de sus clientes, y en especial establecer medidas para que el tratamiento sea leal, confidencial y se impida el acceso no autorizado por terceros a información personal, de acuerdo con lo indicado en los artículos 5.1f), 24 y 32 del RGPD, y 28.2 de la LOPDGDD, sin perjuicio de lo que corresponda a las entidades bancarias como proveedores de servicios de pago derivado del Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera.

Otro tratamiento que ha requerido un especial análisis, por sus características peculiares y por su trascendencia, es el que se da en el ámbito de los ensayos clínicos. En el **Informe 38/2021** se clarifica la base legitimadora del tratamiento de datos personales que lleva a cabo la figura del monitor en un ensayo clínico cuando accede a los datos personales obrantes en la historia clínica de los sujetos participantes.

Como punto de partida, el informe aborda la consideración (de responsable o encargado del tratamiento) que ha de tener el monitor en un ensayo clínico desde la perspectiva de la normativa de protección de datos.

A tal efecto es necesario observar la normativa que regula la actividad de esté en los ensayos clínicos con medicamentos, el Reglamento (UE) 536/2014 del Parlamento Europeo y del Consejo de 16 de abril de 2014 sobre los ensayos clínicos de medicamentos de uso humano, y también se tiene en cuenta el Real Decreto 1090/2015, de 4 de diciembre, por el que se regulan los ensayos clínicos con medicamentos, los Comités de Ética de la Investigación con medicamentos y el Registro Español de Estudios Clínicos.
Tras el análisis de la misma, se indica en el informe que el monitor ostenta la condición de encargado del tratamiento, en cuanto que trata los datos personales por cuenta del promotor, que es el que tiene la obligación de realizar la monitorización del mismo, siendo el único responsable de la elección del monitor, para lo que "elegirá únicamente un encargado que ofrezca garantías suficientes" (artículo 28.1. del RGPD). En el ejercicio de su función de monitorización, el monitor deberá seguir únicamente las instrucciones del promotor, "de acuerdo con los procedimientos normalizados del promotor" (artículo 40.1.a) del Real Decreto), debiendo suscribirse entre el promotor y el monitor el contrato previsto en el artículo 28.3. del RGPD.

En consecuencia, en cuanto encargado del tratamiento del promotor, la base jurídica aplicable a los tratamientos de datos personales que realice el monitor será la misma que la del promotor. Siendo la monitorización una obligación impuesta al promotor por el Reglamento (UE) 536/2014, la misma será la contemplada en el artículo 6.1.c) del RGPD: "el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento".

Asimismo, el informe recuerda que condición del monitor como encargado del tratamiento del promotor no se ve desvirtuada por la circunstancia de que el promotor únicamente acceda a datos seudonimizados y el monitor acceda a los datos identificativos de la historia clínica del paciente. Ese acceso se produce en cumplimiento de una obligación legal de monitorización del promotor, sin perjuicio de que el promotor no tenga dichos datos en virtud de medidas adoptadas para dar cumplimiento a otros principios del RGPD, como son el de limitación de la finalidad (artículo 5.1.b) y de minimización de datos (artículo 5.1.c), con la consiguiente incidencia en la adopción de las medidas de seguridad en virtud de los diferentes datos personales tratados. En este sentido se señala que el RGPD no considera como criterio determinante para apreciar la existencia de un encargo del tratamiento el que el responsable tenga acceso a los datos, sino que lo que requiere es que las operaciones de tratamiento, entre las que se encuentra, por ejemplo, la recogida, se atribuyan al responsable. El acceso a los datos personales de la historia clínica por parte del monitor se hace por cuenta del promotor y no por cuenta del centro responsable de dicha historia clínica. También se tiene en cuenta que el centro no participa en la elección del monitor ni le puede dar instrucciones respecto al ejercicio de su función, no existiendo una relación jurídica entre el centro y el monitor. El acceso por parte del monitor a los datos de la historia clínica se hace por cuenta del promotor y no del centro, debiendo firmarse el contrato de encargo de tratamiento únicamente con el promotor y no con el centro, sin perjuicio de que este último, en cuento responsable del tratamiento de la historia clínica, deba establecer todas las medidas necesarias para garantizar la seguridad de los datos personales, como puede ser un deber de confidencialidad de conformidad con el artículo 32 del RGPD.

Finalmente, se aclara el papel de otros intervinientes fundamentales en los ensayos clínicos, indicando que el promotor es responsable el tratamiento de los datos para la finalidad de realización de los ensayos clínicos con medicamentos debiendo tomar decisiones sobre los fines y los medios en los términos de las previsiones del Reglamento (UE) 536/2014 y del Real Decreto 1090/2015 que se han expuesto. Previsiones que son específicamente aplicables en relación con las referencias que para esta modalidad de

investigación recoge el artículo 16.3 de la Ley de Autonomía del Paciente cuando contempla los usos de la historia clínica con fines de investigación.

La implicación de las nuevas tecnologías en el tratamiento de datos personales ha y sido y es un elemento fundamental que tradicionalmente ha generado muchas controversias y dudas.

En el **Informe 47/2021** se resuelve una consulta sobre el proyecto "Biometría Seguridad y PBCyFT" presentado por una entidad financiera para su ejecución en el espacio controlado de pruebas del Sandbox Regulatorio Financiero previsto en la Ley 7/2020, de 13 de noviembre, para la transformación digital del sistema financiero, que plantea el tratamiento de datos de reconocimiento facial en el momento del alta de clientes en la oficina o a través de un canal online, con el objetivo de verificar su identidad y así realizar las verificaciones oportunas previstas en la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (PBC/FT), así como del control del fraude.

En el informe se recuerda la dificultad de deslindar los conceptos de identificación y autenticación, cuestión fundamental para valorar si estamos ante un tratamiento de datos biométricos considerados como categorías especiales de datos o no; lo que requiere estar al caso concreto y a las particulares técnicas empleadas en relación con la finalidad perseguida por el tratamiento, así como la necesidad de otorgar la máxima protección a los derechos de los afectados frente al uso de técnicas que puede ser más invasivas para su privacidad y generar mayores riesgos para sus derechos y libertades.

En el supuesto concreto el tratamiento de datos biométricos que se pretende realizar tiene como finalidad cumplir con el deber de identificación establecido en la normativa sobre prevención del blanqueo de capitales y financiación del terrorismo, evitando, de este modo, la posible suplantación de identidad. Por consiguiente, debe concluirse que el proceso de reconocimiento facial empleado implica el tratamiento de datos biométricos con la finalidad de identificar unívocamente a una persona física, por lo que es un tratamiento de categorías especiales de datos sujeto a la regla general de prohibición de los mismos (art. 9.1. RGPD), y cualquier excepción a dicha prohibición habrá de ser objeto de interpretación restrictiva.

Asimismo, se hace referencia a lo indicado en los informes 36/2020, 31/2019 o al 97/2020, en los que se concluía que no existía norma legal en el ordenamiento jurídico español que reuniera los requisitos del artículo 9.2.g) del RGPD, por lo que el tratamiento únicamente podría ampararse en el consentimiento de los afectados siempre que quedara garantizado que el mismo es libre.
Pues bien, tras analizar la obligación de identificación que impone a los sujetos obligados el artículo 3 de la Ley 10/2010 de 28 de abril, y en su caso, el Real Decreto 304/2014, de 5 de mayo, y las exigencias del RGPD, se concluye que dicha regulación no cumple con los requisitos establecidos en el artículo 9.2.g), ya que el legislador no ha previsto el uso de datos biométricos como una medida proporcional para la identificación de las personas físicas, estableciendo las garantías específicas y adecuadas que se derivan de los mayores riesgos que implica el tratamiento de dichos datos.

Por consiguiente, pretendiéndose en el proyecto un tratamiento de datos personales como categorías especiales de datos a los que se refiere el artículo 9.1. del RGPD, puesto que se trata de datos

biométricos dirigidos a la identificación de las personas físicas, es requisito previo que concurra alguna de las circunstancias que levante la prohibición de tratamiento de dichos datos, exigiendo el artículo 9.2. de la LOPDGDD que "Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad." No existiendo, como se ha indicado, norma legal que habilite dicho tratamiento al amparo del artículo 9.2.g) del RGPD.

Por lo tanto, dicha prohibición únicamente podrá levantarse en aquellos casos en que el afectado preste su consentimiento explicito, al amparo de la letra a) del artículo 9.2. del RGPD, debiendo concurrir todos los demás requisitos para otorgar un consentimiento válido que se recogen en la definición del artículo 4.11 del RGPD: "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".

Asimismo, el informe indica que, aunque la ausencia de causa que levante la prohibición del tratamiento de categorías especiales de datos determina, por sí sola, la ilicitud del tratamiento propuesto debe señalarse que tampoco concurre una base jurídica que legitimara el mismo al amparo del artículo 6.1. del RGPD sobre la base del interés público.

Pues, aunque exista un interés público en el ámbito de la prevención del blanqueo de capitales y la financiación del terrorismo, dicho interés no legitima cualquier tipo de tratamiento de datos personales, sino que deberá estarse, en primer lugar, a las condiciones que haya podido establecer el legislador, tal como prevé el propio artículo 6 del RGPD, en sus apartados 2 y 3, y el artículo 8 de la LOPDGDD, tomando en consideración todos los intereses afectados, al objeto de determinar las restricciones que pueden sufrir los intereses particulares como consecuencia de la presencia de dichos intereses generales, lo que debe hacerse a través de una norma con rango de ley.

En el caso del proyecto, no resultaría de aplicación la base jurídica del del artículo 6.1.e) del RGPD en la medida en que la Ley 10/2010 no atribuye competencias, que son propias de las Administraciones Públicas, a las entidades financieras como sujetos obligados al cumplimiento de dicha norma. A lo que hay que añadir que las justificaciones aportadas por la promotora del proyecto, referida a supuestas suplantaciones de identidad, no puede colegirse que las mismas se refieran específicamente al interés público perseguido por la normativa sobre prevención del blanqueo de capitales y financiación del terrorismo, sino más bien a supuestos de fraude en perjuicio de la propia entidad, respondiendo a un interés privado de la misma, lo que no sería admisible, como recuerda, en otro supuesto de aplicación de sistemas de reconocimiento facial, el Auto 72/2021 de la Sección Novena de la Audiencia Provincial de Barcelona de 15 de febrero de 2021. Teniendo en cuenta lo indicado, el informe concluye que el DNI acredita por sí solo y a todos los efectos la identidad y los datos personales de su titular. De este modo, el imponer como obligatoria la identificación mediante reconocimiento facial no se ajustaría a lo previsto en la normativa vigente (ni en lo referido al supuesto de levantamiento de prohibición de tratamiento del artículo 9.2.g) ni tampoco existe legitimación prevista en el artículo 6.1, ambos del RGPD), además de ser desproporcionado y por tanto contrario al principio de minimización.

3.2.2. Informes preceptivos

La AEPD ha continuado trabajando en el objetivo de lograr mayor seguridad jurídica a través de los informes preceptivos sobre disposiciones de carácter general, dirigidos a mejorar la sistemática del ordenamiento jurídico integrando una norma de carácter transversal con las regulaciones sectoriales. Entre las disposiciones informadas en el año 2021 cabe mencionar las siguientes:

- Anteproyecto de Ley Orgánica de enjuiciamiento Criminal.

- Anteproyecto de Ley Orgánica por la que se establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales.
- Anteproyecto de Ley Orgánica de Eficiencia Organizativa del Servicio Público de Justicia.
- Anteproyecto de Ley Orgánica del Mercado de Valores y de los Servicios de Inversión.
- Anteproyecto de Ley orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, para la transposición de directivas en materia de lucha contra el fraude y la falsificación de medios de pago.
- Anteproyecto de Ley Sociedades de Capital.
- Anteproyecto de Ley por la que se adapta al ordenamiento nacional, el Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo, de 14 de noviembre, sobre Eurojust, y se regulan los conflictos de jurisdicción, las redes judiciales de cooperación internacional y el personal dependiente del Ministerio de Justicia en el exterior.
- Anteproyecto de Ley General de Telecomunicaciones.
- Anteproyecto de Ley General de comunicación audiovisual.
- Anteproyecto de Ley por la que se modifica la Ley 13/2011, de 27 de mayo, de regulación del juego.
- Anteproyecto de Ley para la igualdad real y efectiva de las personas trans y para la garantía de los derechos de las personas LGTBI.
- Anteproyecto de ley de medidas de eficiencia digital del servicio público de justicia, por la que se transpones al ordenamiento jurídico español, la directiva UE 2019/1151 del Parlamento Europeo y del consejo, de 20 de junio de 2019, por la que se modifica la Directiva UE2017/1132 en lo que respecta a la utilización de herramientas y procesos digitales en el ámbito del derecho de sociedades.
- Anteproyecto de Ley por la que se modifican diversas normas para consolidar la equidad, universalidad y cohesión del Sistema Nacional de Salud.
- Proyecto de Real Decreto de Ordenación de entidades de crédito.
- Proyecto de Real Decreto sobre el régimen de incompatibilidades de la Guardia Civil.
- Proyecto de Real Decreto por el que se modifica el RD 181/2008, de 8 de febrero, de ordenación del BOE para adaptarlo al Tablón Edictal Judicial Único.
- Proyecto de Real Decreto por el que se establecen los criterios de calidad en medicina nuclear.
- Proyecto de Real Decreto por el que se regula la representación interministerial en la conferencia sectorial del plan nacional sobre drogas.
- Proyecto de Real Decreto por el que se establecen medidas para el control del bienestar animal en los mataderos mediante la instalación de sistemas de videovigilancia.
- Proyecto de Decreto de la Junta de Andalucía por el que se regula el Biobanco.
- Proyecto de Real Decreto por el que se regula el sistema estatal de registros de protección animal.
- Proyecto de Real Decreto por el que se modifica el Reglamento penitenciario aprobado por RD 190/1996, de 9 de febrero.

- Proyecto de Real Decreto por el que se regula el procedimiento para la tramitación de propuestas, sugerencias, quejas y solicitudes de información del personal de la Guardia Civil.
- Proyecto de Real Decreto por el que se regulan los productos sanitarios.
- Proyecto de Real Decreto que regula la organización y funcionamiento de los registros nacionales en materia de reproducción humana asistida.
- Proyecto de Real Decreto por el que se regula la interoperabilidad de los sistemas de peaje en las carreteras españolas.
- Proyecto de Real Decreto sobre inscripción de las personas de nacionalidad española en los Registros de Matrícula de las Oficinas Consulares en el extranjero.
- Proyecto de Real Decreto por el que se regula el Esquema Nacional de Seguridad.
- Proyecto de Real Decreto sobre instrumentos financieros, admisión a negociación.
- Proyecto de Real Decreto por el que se aprueba el reglamento de desarrollo de las potestades y facultades administrativas de la CNMV en relación con los mercados de valores y las empresas de servicios de inversión.
- Proyecto de Real Decreto sobre el régimen jurídico de las empresas de inversión y de las demás entidades que prestan servicios de inversión.
- Proyecto de Real Decreto por el que se modifica el Real Decreto 1275/2011 de 16 de septiembre, por el que se crea la Agencia Española de Medicamentos y Productos Sanitarios y se aprueba su estatuto.
- Proyecto de Real Decreto sobre las funciones de la sanidad de la Guardia Civil y la determinación de la aptitud psicofísica de su personal.
- - Proyecto de Real Decreto por el que se establecen los criterios técnico - sanitarios del suministro control de la calidad del agua de consumo.
- Proyecto de Real Decreto por el que se aprueba el reglamento de organización y funcionamiento interno del Consejo de la Guardia Civil.
- Proyecto de Real Decreto por el que se modifica el Reglamento de control del comercio exterior de material de defensa, de otro material y de productos y tecnologías de doble uso, aprobado por Real Decreto 679/2014, de 1 de agosto.
- Proyecto de Orden por la que se regula el registro electrónico de Apoderamientos en el ámbito de la Administración general del Estado.
- Proyecto de Orden por la que se regula el registro electrónico general en el ámbito de la Administración General del Estado.
- Proyecto de Orden por la que se regula el Registro de funcionarios habilitados en el ámbito de la Administración General del Estado, sus organismos públicos y entidades de derecho público.
- Proyecto de Orden sobre los métodos de identificación no presencial para la expedición de certificados electrónicos cualificados.
- Proyecto de Orden por la que se determinan las escuelas facultadas para impartir formación y especialización y el órgano competente para expedir permisos de conducción de vehículos policiales por personal ajeno.

- Proyecto de Orden por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación.

- Proyecto de Orden por la que se desarrolla el registro de mediadores sociales del ingreso mínimo vital.

- Proyecto de Orden por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Derechos Sociales y Agenda 2030.

- Proyecto de Orden por la que se estable el modelo y las normas reguladoras del expediente de aptitud psicofísico del personal de la Guardia Civil.

- Proyecto de Orden por la que se crea la comisión de formación continuada de las profesiones sanitarias del Instituto Nacional de Gestión Sanitaria, regula composición, funcionamiento y procedimiento de acreditación de actividades formativas.

- Proyecto de Orden por la que se abre procedimiento permanente para la evaluación y acreditación de competencias profesionales, adquiridas por la experiencia laboral o vías no formales de formación, en las Ciudades Autónomas de Ceuta y Melilla, y se formalizan las bases para su desarrollo.

- Proyecto de Orden por la que se regula el Registro electrónico de apoderamientos del Fondo de Garantía Social O.A.

- Proyecto de Orden reguladora de movimiento de medios de pago en el ámbito de la prevención del blanqueo de capitales y de la financiación del terrorismo.

- Proyecto de Orden por la que se regulan determinados aspectos de la autorización de los medicamentos alérgenos de producción industrial y de los graneles de alérgenos de huso humano y veterinario.

- Proyecto de Instrucción por la que se establecen directrices respecto de la función consultiva de la AEPD, con el fin de adecuar la misma a lo previsto en el RGPD la LOPDGDD y el Estatuto de la Agencia.

3.2.3. 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 de los Tribunales Europeos que versen sobre la materia y que por su interés merecen ser destacadas.

Durante el año 2021 se han dictado por la Sala de lo contencioso-administrativo de la Audiencia Nacional, 66 resoluciones[1] , de las cuales:

- 39 fueron desestimatorias de los recursos formulados contra resoluciones de la Agencia (que quedaron plenamente confirmadas) (60 %)

- 3 estimaron parcialmente los recursos (4%)

- 7 estimaron íntegramente las pretensiones anulatorias de las resoluciones de la Agencia (11%)

- 16 inadmitieron los recursos interpuestos contra resoluciones de la Agencia (25%).

Por su parte, el Tribunal Supremo dictó un total de 4 resoluciones, las cuales confirman el criterio de la AEPD.

En cuanto a los sectores de actividad de los recurrentes tanto en la Audiencia Nacional como en el Tribunal Supremo, de 77 resoluciones[2] 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.

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. También se observa un aumento significativo 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.

En cuanto a las estimatorias, y parcialmente estimatorias, debe indicarse que responden a una variada casuística dónde materias como las referidas al ejercicio de los derechos, tanto desde la perspectiva del titular de los datos, como desde las obligaciones del responsable del tratamiento, cobran especial relevancia y, en particular, aquellas que versan sobre la cancelación de antecedentes policiales.

Seguido del sector de banca y seguros, y el sector de las Telecomunicaciones. Tras ellos figura el sector de los sistemas de información crediticia y con el mismo número de resoluciones el sector de distribución y venta, y el de agua y energía. Los restantes sectores como administraciones públicas, asociaciones sindicales, sociedad de la información o publicidad y prospección comercial son los menos significativos cuantitativamente y han sufrido una disminución respecto del ejercicio anterior.

De las materias analizadas por la Audiencia Nacional destacan las siguientes cuestiones:
Comenzando por la aplicación de los principios en el tratamiento de datos, hay que citar **la Sentencia de 5 de mayo de 2021, recaída en el Recurso 1437/2020,** interpuesto contra la resolución de la AEPD que sanciona a una empresa de telecomunicaciones por la vulneración del artículo 6 del RGPD y en la que también se analiza la aplicación de las Circulares de la CMT sobre contratación telefónica y la normativa que debe aplicarse, que está íntimamente relacionada con la diligencia exigible a los operadores. Los hechos son que los datos del denunciante han sido utilizados para, partiendo de una línea de teléfono sobre la que no hay discusión en cuanto a su contratación, activar varias líneas de teléfono adicionales sin que concurriera ninguna base de legitimación para dicho tratamiento. Y con posterioridad los datos son comunicados a un sistema de información crediticia. Por la sancionada se alega, además de las cuestiones de fondo, otras formales o procesales como la suspensión por prejudicialidad penal y la prescripción de la infracción.

Sobre la prejudicialidad penal, la Sala rechaza el argumento recordando la doctrina consolidada de los tribunales en cuya virtud debe darse la triple identidad y lo dispuesto en el artículo 31.1 de la Ley 40/2015, de 1 de octubre, del Sector Público, afirmándose que en el caso analizado no puede apreciarse por cuanto si bien existen tres procedimientos penales en fase de diligencias previas no concurre la identidad del sujeto ya que si bien está personada en la causa la entidad de telecomunicaciones, la acusación se dirige contra una persona física como supuesta suplantadora de la identidad del reclamante, a estos efectos indica que: No existe, por tanto, identidad de sujeto, pues el sujeto infractor es obvio que no sería el mismo.

[1] Únicamente se refiere a Sentencias, quedando por tanto excluidos los Auto que resuelven aquellos procedimientos en los que se ha producido el desistimiento, la caducidad o el archivo por falta de postulación, o tratan de medidas cautelares.

[2] Aquí se incluyen todo tipo de resoluciones (sentencias, autos, providencias, etc. tanto de la Audiencia Nacional como del Tribunal Supremo)

Sobre la prescripción de la infracción se recuerda el cómputo de la comisión de las infracciones que se consideran "continuadas" y en el caso analizado, además de utilizarse los datos para el alta fraudulenta de las líneas de teléfono, con posterioridad se comunicaron al sistema de información crediticia y siguieron constando en los propios sistemas de la entidad de telecomunicaciones con varias deudas pendientes signadas.
Ya sobre el fondo del asunto, se deja claro que no se sanciona por la línea sobre la que no hay discusión pues el tratamiento de esos datos estaba amparado en el artículo 6.2 de la LOPD vigente al momento de dicha contratación, sino que la conducta acreedora del reproche jurídico es el alta de las otras líneas, respecto de la que no se ha podido probar que concurriera ninguna causa que de licitud a ese tratamiento.

Por lo tanto la discusión se traslada a la diligencia prestada por la entidad a la hora de activar las citadas líneas, respecto de lo que se alega que dicha diligencia se cumple cuando se observa lo indicado en las Circulares 1/2009, de 16 de abril de 2009, y 1/2008, de 19 de junio de 2008, ambas de la Comisión del Mercado de Telecomunicaciones, por las que se introduce el consentimiento verbal con verificación por tercero en la contratación de servicios mayoristas regulados de comunicaciones fijas (1/2019) y sobre conservación y migración de numeración telefónica (1/2008). Esta normativa obliga a la intervención de un tercero en el proceso de contratación, que actúa como "verificador", contando la actora con la justificación de la intervención de dicho verificador, por lo que cumplió con todas las exigencias legalmente exigibles para realizar dichas contrataciones, habiendo puesto a disposición de la AEPD las grabaciones de las contrataciones relativas a 4 de las cinco líneas y así como copia del contrato relativo a la última línea objeto de controversia.

Pues bien, la práctica de la prueba reveló que, de los seis audios aportados, dos de ellos pertenecen a la voz de una mujer, siendo que el denunciante es un hombre, además una de ellas no hace referencia a ninguna línea objeto de discusión y la otra ni siquiera identifica el número al que se refiere. Un tercer audio se refiere a un intento de cancelar una portabilidad. El cuarto es relativo a la compra de dos tablets, y el quinto se refiere a una segunda venta a plazos de nuevas tablets y un ipad mini para las restantes líneas. Asimismo, es de destacar que en ninguno se recoge fecha de grabación. Y el sexto se refiere a un cambio de tarifa y no consta la fecha, que es uno de los requisitos exigidos por las Circulares 1/2008 y 1/2009 y que la Sala ha calificado como "dato fundamental" entre otras, en la SAN de 7 de abril de 2017 (Rec. 422/2015).

Por lo que está claro que las citadas grabaciones no pueden amparar el tratamiento de los datos del denunciante. Y en cuanto al contrato aportado, no se reconoce por el reclamante la firma y resulta evidente la discrepancia con la que figura en su DNI.

Finaliza la Sala indicando que como ha señalado reiteradamente (SAN de 23 de abril de 2015, Rec.97/2014, por todas) corresponde a quien realiza el tratamiento acreditar que ha obtenido el consentimiento del afectado, cuando - como aquí sucede- niegue haberlo otorgado, y a tal fin deberá arbitrar los medios necesarios para ello. En esta línea, se expresa el artículo 7 del RGPD. Por tanto, el tratamiento de los datos personales del denunciante no se ajusta al art. 6 RGPD,

Por su parte, **la Sentencia de 11 de junio de 2021**, que resuelve el recurso 322/2020 interpuesto contra la resolución de la AEPD que sanciona a una empresa de telecomunicaciones por la vulneración del artículo 6 del RGPD, es similar a la citada anteriormente en cuanto a hechos y fundamentos de derecho, si bien en este caso es preciso destacar que también se alega la falta de proporcionalidad en la determinación de la cuantía de la sanción por cuanto según afirma remedió la causa que motivaba la reclamación tan sólo dos días después de su origen, y el mismo día que tuvo conocimiento de su existencia. Así como que existió puntual involuntario de un único afectado, y que ha actuado de forma colaborativa y proactiva con la AEPD.

La Sala rechaza estos argumentos recordando la doctrina del Tribunal Supremo sobre el principio de proporcionalidad (STS 12/04/2021 Rec.

5149/2009) en virtud del cual debe existir una debida adecuación entre la gravedad del hecho constitutivo de la infracción y la sanción aplicada, concluyendo que atendida las circunstancias concurrentes no se ha infringido el principio de proporcionalidad en la determinación de la sanción impuesta, que resulta ponderada y proporcionada a la gravedad de la infracción cometida y la entidad de los hechos, y debidamente motivada, sin que se aprecien razones que justifiquen su minoración, máxime teniendo en cuenta la cuantía a la que puede ascender dicha sanción: 20.000.000 € como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

A continuación, procede citar dos resoluciones, la **Sentencia de 22 de junio de 2021- Rec. 1210/2018, y la Sentencia de 5 de noviembre de 2011 -Rec. 1796/2019,** en las que se sanciona a la misma entidad por la vulneración de los principios de licitud y exactitud. Los hechos son que la entidad sancionada, una conocida marca de venta y distribución de productos de belleza a domicilio, reclama el pago de la venta de unos productos a dos supuestas colaboradoras y ante el impago comunica los datos personales de éstas a un sistema de información crediticia -un fichero de morosos-. De los hechos se deduce que un tercero de manera fraudulenta dio de alta en el sistema de distribuidores de la marca a las afectadas y las atribuyo la adquisición de varios productos.

Al igual que en las otras sentencias analizadas, se alegó la prejudicialidad penal, por cuanto existían denuncias ante la jurisdicción penal, siendo desestimada dicha alegación por no darse la triple identidad de hecho, sujetos y fundamentos de derecho, ya que las diligencias se incoan por un ataque informático a los sistemas de la entidad y también por denuncias cruzadas entre la denunciante y la actora.

La Sala resuelve sobre el fondo del asunto refiriéndose a que (…) ha resultado acreditado en las actuaciones y no desvirtuado mediante prueba en contrario, que en los ficheros de Avon Cosmetic se encontraban los datos personales de la denunciante (su nombre, apellidos y número de DNI), asociados a una contratación que realmente no había sido llevada a cabo por la misma. Se trata en definitiva de que la entidad actora inició una relación comercial con una tercera sin control ni supervisión suficiente en cuanto no fue capaz de detectar que realmente, la persona que estaba manifestando su voluntad de contratar, no era quien decía ser. (…)

Finaliza la argumentación de la Sala valorando el elemento subjetivo o culpabilístico, insistiendo en que la culpabilidad de la parte actora no puede considerarse excluida ni atenuada por el hecho de que haya mediado la posible actuación fraudulenta de un tercero, pues la responsabilidad de la parte actora no deriva de la actuación de éste, sino de la suya propia.

La siguiente sentencia también trata sobre el principio de licitud, pero en relación con el tratamiento del dato relativo a la geolocalización y los poderes que el empleador tiene al amparo del artículo 20.3 del Estatuto de los Trabajadores. **La Sentencia de 14 de junio de 2021**, resuelve el Recurso 1770/2019 interpuesto por un particular frente a la resolución de la AEPD de inadmisión.

La entidad procede a la extinción del contrato de trabajo a raíz de la información que se obtuvo por el GPS que llevaba el vehículo de la entidad. Los trabajadores fueron informados de la existencia de dicho sistema, y advertidos de que el vehículo no podía usarse para cuestiones personales, y, por tanto, en fin de semana, que fue lo que motivo el despido. En puridad no se informa de la extinción de la geolocalización en fin de semana, pero quedaba claro que dicho vehículo únicamente se utilizaría para trabajar los días de jornada laboral.

La AEPD inadmite la reclamación en base a que el artículo 20.3 de la Ley del Estatuto de los Trabajadores, así como los artículos 89 y 90 de la LOPDGDD, atribuyen facultades especificas a la empresa que posibilitan la vigilancia y control del desarrollo de la prestación laboral, particularmente, para verificar el cumplimiento por el trabajador de sus obligaciones y deberes. Para

el ejercicio de las citadas funciones de control, los empleadores podrán tratar asimismo los datos obtenidos a través de sistemas de geolocalización, pero con carácter previo habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos.
La Sala no se pronuncia sobre el fondo del asunto pues inadmite el recurso por falta de legitimación al solicitar el recurrente al tribunal la imposición de una sanción lo que contraviene la reiterada doctrina del Tribunal Supremo (por todas la STS de 1 de febrero de 2018 (Rec. 2368/2016).

También relacionado con el principio de licitud en el tratamiento, conviene citar **la Sentencia de 24 de septiembre de 2021** recaída en el Recurso 2435/2019 interpuesto frente a una resolución sancionadora de la AEPD a una entidad financiera cedente de un crédito a una tercera entidad. Si bien los datos del afectado fueron informados a un sistema de información crediticia, aquí no se denuncian ni se analizan si se cumplen los requisitos para dicha inclusión, sino que se aborda el tema de la cesión o comunicación de datos incluidos en la venta de cartera.

El cesionario de los datos y acreedor que incluyó los datos del afectado en el fichero de morosos manifestó que compró una cartera de créditos entre los que estaba uno asociado al denunciante. El cedente para acreditar la deuda y justificar la cesión de los datos aporta un certificado de deuda asociada a una tarjeta de crédito a nombre del denunciante y también impresiones de pantalla de movimientos de dicha tarjeta.

Pues bien, la Sala recuerda la doctrina sobre la validez de la prueba de capturas de pantalla que tanto ha sido invocada y aplicada por la AEPD en sus resoluciones, y que se concreta en que: Sentencia de 9 de abril de 2008 -recurso 235/2006 -, que los pantallazos o reflejos informáticos no acreditan la prestación del consentimiento: "... no se trata más de un simple "pantallazo" informático, que nada acredita ni aporta ninguna información relevante a la hora de poder acreditar el consentimiento del titular de los datos".

Asimismo, por la parte actora se alega que estamos ante un tratamiento legítimo de los datos, fruto de una operación de venta o cesión de créditos contemplada expresamente en el art. 347 y 348 del Código de Comercio.

Frente a lo que la Sala indica que la figura de la cesión de datos personales en relación con el contrato de compraventa y cesión de créditos elevado a escritura pública, al amparo de los mencionados preceptos, es una cuestión que ya ha sido analizada anteriormente " solamente en los supuestos que no consta la existencia de deuda alguna que justifique la cesión de datos se considera que se ha producido una vulneración del artículo 11 de la LOPD tipificada en el artículo 44.4.b) de la citada norma, pues en estos supuestos no se analiza la calidad de los datos sino la falta de consentimiento para su cesión".

Pues bien, concluye la Sala indicando que lo que ha acontecido es que no consta la comunicación de la cesión del crédito a la denunciante, por lo que cabe apreciar la existencia de la infracción por la que ha sido sancionada la parte demandante.

En relación con el tratamiento de datos personales en los sistemas de información crediticia, y que versan sobre los requisitos previstos en los artículos 38 y siguientes del Real Decreto 1720/2007, de 21 de diciembre, o en el artículo 20 de la LOPDGDD, deben citarse la **Sentencia de 2 de julio de 2021** que resuelve el Recurso 415/2020 interpuesto frente a una resolución sancionadora de la AEPD a la entidad responsable del "fichero de morosos" por infracción del articulo 6.1 f) del RGPD, en relación con el articulo 20.1 c) de la LOPDGDD que impone la obligación del bloqueo de los datos del afectado durante el periodo de treinta días por si el afectado ejerce alguno de los derechos tras conocer la inclusión.

Indica la sentencia que la previsión de bloqueo de la información durante treinta días prevista en la citada Ley Orgánica resulta acorde con las previsiones de la información que debe facilitarse cuando los datos personales no se hayan obtenido del interesado recogida en el art. 14 del RGPD. El RGPD permite que una norma de los Estados

Miembros pueda especificar las condiciones generales del presente Reglamento por las que se rige la licitud del tratamiento de datos personales, establecer especificaciones para la determinación del responsable del tratamiento, el tipo de datos personales objeto de tratamiento, los interesados afectados, las entidades a las que se pueden comunicar los datos personales, las limitaciones de la finalidad, el plazo de conservación de los datos y otras medidas para garantizar un tratamiento lícito y leal. Y eso, se ha llevado a cabo por la LOPDGDD, en que se establece el bloqueo de los datos durante del plazo de treinta días en se puede ejercitar los derechos establecidos en los arts. 15 a 22 del RGPD. El tratamiento sin haberse realizado el bloqueo de los datos durante el plazo previsto legalmente resulta ilícito, ya que debe darse prevalencia a los intereses o los derechos y libertades fundamentales del interesado. Pues bien, la sociedad recurrente reconoce en su escrito de alegaciones presentado en vía administrativa, lo siguiente: "Si bien es cierto, que dicha LOPDGDD era de aplicación a partir del día siguiente a su publicación en el BOE, es decir, con fecha 7 de diciembre de 2018, por motivos técnicos y de desarrollo interno en Equifax, no fue factible implementar dichos cambios en nuestros sistemas hasta el pasado 22 de enero de 2019, fecha a partir de la cual el bloqueo de los 30 días quedó efectivamente implementado".

La Sentencia de 10 de septiembre de 2021 que resuelve el Recurso 139/2019 interpuesto contra la resolución sancionadora de la AEPD por inclusión de datos en un sistema de información crediticia sin cumplir los requisitos previstos en el artículo 4.3 de la LOPD y el Real Decreto 1720/2007, de 21 de diciembre.

Así el actor compró una deuda e incluyó los datos del denunciante en un fichero de solvencia patrimonial y los mantuvo en dicho fichero con posterioridad a la petición de cancelación por parte del denunciante, que le participó haber interpuesto una demanda judicial, por lo que la deuda no era cierta ni exigible. La sanción de 60.000 euros impuesta en la resolución impugnada deriva de considerar la AEPD que concurren las agravantes de carácter continuado de la infracción, al estar incluidos los datos en los ficheros de solvencia a sabiendas de la existencia de la demanda, por lo menos desde el 21 de febrero de 2018, fecha en que el denunciante solicitó por primera vez la cancelación de la deuda después de la interposición de la demanda, y hasta el 12 de abril de 2018. También se le aplica la de vinculación de la actividad de la entidad infractora con la realización de tratamientos de datos de carácter personal; el volumen de negocio de la entidad denunciada y la naturaleza de los perjuicios causados a las personas interesadas, siguiendo el criterio de que se trata de un hecho de gran trascendencia y del que se pueden derivar consecuencias muy negativas para el afectado, tanto en su vida profesional como personal (SAN 16/02/2002, entre otras muchas).

Siguiendo con los requisitos para la inclusión en los ficheros de solvencia, las **Sentencias de 20 de septiembre de 2021, Recurso 1669/2019 y la de 11 de noviembre de 2021, Recurso 1979/2019,** tratan del requisito de la existencia de la deuda. En ambos procesos se produce una inclusión en el citado sistema de información y se mantiene a pesar de que se acredita que el deudor abona la deuda lo que determinaría la automática exclusión del fichero de morosos.

En relación con el principio de confidencialidad o deber de secreto (en la terminología de la hoy derogada LOPD), se puede distinguir a grandes rasgos dos bloques perfectamente diferenciados. Las sentencias referidas al tratamiento de datos personales en procesos judiciales y las referidas a la publicación de datos en tablones de anuncios y/o similares.

En cuanto a la aportación de datos personales a procesos judiciales las **Sentencias de 5 de febrero de 2021, Recurso 1045/2019, de 5 de marzo de 2021, Recurso 192/2020, de 30 de abril de 2021, Recurso 586/2021, de 20 de mayo de 2021, Recurso 210/2018 y la de 1 de diciembre de 2021, Recurso 1490/2021,** resuelven recursos interpuestos por particulares que están afectados por diferentes procesos judiciales en los que sus datos personales son aportados por las distintas partes y sirven a dichos procesos. Pues bien, en todos ellos, la Sala

recuerda la doctrina de la concurrencia del interés legítimo como parte del derecho de defensa y de la legitimación en acciones civiles o de otro ámbito jurisdiccional, y que forma parte del núcleo esencial del derecho fundamental previsto en el artículo 24 de la Constitución, y también lo referido al cumplimiento de una obligación legal, cuando los datos son requeridos por mandato judicial. El RGPD, establece en su art. 6.1 los supuestos que legitiman la comunicación de datos personales, como es cuando exista una obligación legal para ello, como puede ser el supuesto de comunicaciones a los Juzgados y Tribunales. A dicho precepto se remite el art. 8 de la LOPDGDD. Por otra parte, ya en la anterior LOPD de 1999, una de las causas que excluía la necesidad de consentimiento para la cesión de datos personales, era que la comunicación que debía efectuarse tuviera por destinatarios a los Jueces o Tribunales -art. 11.2.d) de dicha norma-. Excepción en la que, como dijimos en la Sentencia de 8 de marzo de 2012 -recurso 779/2010-, podemos incluir aquellos supuestos en que se trata de pruebas que, si bien no han sido solicitadas por el Juez o Tribunal, sino aportadas por las partes, con posterioridad, no consta que las mismas hayan sido rechazadas.

En cuanto a la publicación de datos personales con libre acceso de terceros, la **Sentencia de 12 de marzo de 2021** que resuelve el Recurso 959/2020 interpuesto contra la resolución de inadmisión de la AEPD por parte de un particular, trata sobre la publicación de datos personales en el Tablón de Anuncios de la Comunidad de Propietarios. La Sala coincide con el criterio de la AEPD que es acorde con numerosos recursos resueltos por asuntos similares y todos ellos relacionados con datos personales publicados en tablones de anuncios de Comunidades de Propietarios:

Así, en reciente sentencia de 24 de enero de 2020 , argumentábamos lo siguiente: << Por su parte, la Resolución de 13 de enero de 2017 respecto de la que se inadmite el recurso de reposición, argumenta que el Presidente de la Comunidad de Propietarios, como representante de la misma y el Secretario y/ Administrador, como custodio de la documentación de la Comunidad, según el artículo 20 de la Ley de Propiedad Horizontal (LPH) están facultados para el tratamiento de los datos de los miembros para las finalidades previstas en dicha LPH. Señala que, con carácter general, no resulta preciso que en el ámbito interno de la Comunidad, los propietarios consientan el uso de sus datos personales, excepción prevista en los artículos 6.2 y 11.2 de la LOPD y en relación con la morosidad, los artículos 16.2 y 19 de la LPH habilitan la inclusión de los datos identificativos de los propietarios deudores en la Convocatorias de la Junta y sus Actas y añade, que la Ley prevé la instalación de "tablones de anuncios" a los efectos de posibilitar la notificación de los actos de interés de la Comunidad. Entiende dicha Resolución, que, del análisis analizado de los documentos aportados y las circunstancias concurrentes, no se aprecian indicios de infracción. Cabe precisar que la documentación adjuntada a la denuncia versaba sobre la incorporación en las convocatorias y actas de la Junta de la Comunidad de los datos de los vecinos que han interpuesto una demanda judicial contra la Comunidad de Propietarios.>>. (…) << Por todo lo cual, a la vista de las concretas circunstancias concurrentes y tratándose de una notificación efectuada en el ámbito de una relación jurídica existente entre los copropietarios de un edificio en régimen de propiedad horizontal, en la que los copropietarios tienen conocimiento de las cuentas de la Comunidad y de las cantidades adeudas por los comuneros morosos; estando prevista la publicación de la lista de morosos, a efectos de su notificación, por la LPH -artículo 9 h) y circunscrita al ámbito restringido de la Comunidad de Propietarios, en el lugar establecido al respecto, no cabe apreciar vulneración del deber de secreto. Ello, lógicamente, con independencia de la eficacia que dicha notificación pueda tener en el ámbito civil, que es una cuestión que en su caso corresponde valorar a dicha jurisdicción. Criterio el aquí adoptado que por lo demás, es el ya seguido por la Sala en un supuesto similar al presente en la SAN, Sec. 1ª, de 25 de febrero de 2010 (Rec. 166/09), lo que conlleva dejar sin efecto la sanción impuesta>>. Y en sentencia de 1 de abril de 2011, Recur. 222/2010, la Sala se hacía eco de los frecuentes conflictos surgidos en las Comunidades de Vecinos, y declaraba: << La importancia y trascendencia de la normativa de protección de datos y la relevancia de los derechos constitucionales que se encuentran en juego, aconsejan que no

se pongan al servicio de rencillas particulares que deben solventarse en ámbitos distintos que deben tener relevancia solo en el ámbito doméstico que le es propio y no un ámbito como el jurisdiccional. La seriedad que conlleva el ejercicio de la potestad sancionadora aconseja que se pongan en marcha los mecanismos administrativos y jurisdiccionales correspondientes solo cuando se suponga que se ha producido una verdadera violación del derecho fundamental a la protección de datos. Tal circunstancia no concurre en el caso presente.

Por su parte, **la Sentencia de 13 de julio de 2021,** que resuelve el Recurso 1574/2020 interpuesto contra la resolución sancionadora de la AEPD por la vulneración del articulo 5.1 f) del RGPD, trata de la publicación de datos personales en un tablón de anuncios en una cafetería de la entidad sancionada de libre acceso a terceros.

Los hechos son que la Caja Rural es propietaria de un Centro Social dónde hay una cafetería que tiene un tablón de anuncios, dónde se publicó un listado de los socios con nombre y apellidos del denunciante. La cafetería es de acceso público y es punto de reunión de costumbre en el pueblo. El anuncio tiene por objeto poner de manifestó los datos de los expulsados por haber incumplido las obligaciones económicas con la Caja Rural.

Se alega por la actora que la publicación obedece al cumplimiento de una obligación legal, por cuanto la normativa a normativa sectorial aplicable, concretamente en el artículo 22.5 del Real Decreto Legislativo 2/2015, de 15 de mayo, del Consell, y el artículo 17.2 de los Estatutos de la citada Caja Rural, prevé la citada publicación a los efectos de notificar a los afectados la posibilidad de realizar alegaciones en el correspondiente expediente por incumplimiento de la obligaciones económicas.

Pues bien, tras el análisis de los artículos citados se concluye que se prevé dar audiencia a los interesados, pero nada se dice sobre la forma de llevarse a cabo la audiencia, por lo que en ningún caso está legitimado para hacerlo "vía edictos" en un tablón de anuncios en una cafetería, pues el trámite de audiencia debe circunscribirse a los interesados y realizarse con ellos.

También relacionado con la confidencialidad y la exactitud del dato, procede citar dos sentencias que tienen como denominador común que tratan sobre la identificación de los conductores en un procedimiento sancionador de tráfico.

Así en la **Sentencia de 26 de febrero de 2021** que resuelve el Recurso 2202/2019, se sanciona a una entidad que presta servicios de alquiler de vehículos por comunicar los datos de una afectada a la DGT tras el oportuno requerimiento, como conductora de un vehículo que cometió una infracción de tráfico. Lo sucedido es que, en los sistemas de la entidad, figuraba otra cliente con el mismo nombre y apellido que la afectada, pero distinto DNI y también era distinto en número de cliente. La Sala pone de manifiesto que el articulo 5.1 d) del RGPD, impone la necesidad de que los datos personales que se recojan en cualquier fichero sean exactos y respondan, en todo momento, a la situación actual de los afectados, siendo los responsables del tratamiento quien responde del cumplimiento de esta obligación. (…)

Por su parte, **la Sentencia de 20 de diciembre de 2021** que resuelve el Recurso 1447/2020 contra la resolución sancionadora de la AEPD por infracción del articulo 5.1 d) del RGPD, ya que el recurrente reveló datos del afectado a un tercero (la DGT) para identificarlo como autor de una infracción de tráfico; datos que eran inexactos no respondiendo a la realidad puesto que el día en que la infracción fue cometida ya no mantenía relación laboral con el reclamado y no era el conductor del vehículo.

En el ámbito de la videovigilancia se han dictado varias sentencias que están íntimamente relacionadas con otros aspectos como la aportación de las imágenes a procesos judiciales, y que o han sido desestimatorias o que declaran la inadmisibilidad de los recursos, (**Sentencias de 26 de febrero, 16 y 27 de abril y 1 de diciembre todos del año 2021**) siendo de aplicación la doctrina que se acaba de indicar, u otras relacionadas con otros principios generales como el de proporcionalidad. En este sentido la **Sentencia de 23 de noviembre de 2021** que resuelve el Recurso 2269/2019 interpuesto frente a la resolución de archivo de la

AEPD, trata sobre la captación de dos cámaras de videovigilancia que con finalidad de seguridad, inicialmente podían captar vía pública, pero que durante el procedimiento fueron reorientadas y que finalmente ser archivo en la medida en que "no obteniendo imágenes de la acera de enfrente, estaba tutelado el derecho de la denunciante, que no se ve afectada por el dispositivo denunciado"
En lo que respecta al ejercicio de los derechos previstos en los artículos 15 a 22 del RGPD, referidos al derecho de acceso, de rectificación ,de oposición, de supresión, de limitación y de portabilidad, debe indicarse que de las sentencias que resuelven esta materia, se observa claramente dos grupos perfectamente diferenciados. Aquellos que versan sobre el derecho de cancelación de antecedentes policiales, y en su caso, penales, donde el debate jurídico debe centrarse en el grado de motivación o explicación de las causas en virtud de las cuales se deniega la cancelación de los antecedentes. Y los que tratan sobre el denominado derecho de supresión en internet o derecho al olvido; así como otros referidos a tratamientos datos a través de publicaciones, ficheros de acceso públicos, etc..

En cuanto a la cancelación de antecedentes, en la **Sentencia 25 de enero de 2021 Recurso 251/2019,** se resuelve el recurso interpuesto contra la resolución de inadmisión de la AEPD que se confirma en esta instancia judicial, referido a la resolución denegatoria de cancelación de antecedentes policiales del INTPOL de la D.G. Guardia Civil, de 4 de mayo de 2018.

El antecedente policial tiene su origen en unas diligencias policiales de la que se derivaron las Diligencias Urgentes Juicio Rápido 10264/2017 que derivaron en Auto de sobreseimiento provisional y archivo de la causa,

La resolución de la AEPD entiende que la resolución de la DG Guardia Civil está suficientemente motivada y en el recurso de reposición la Agencia analiza las alegaciones del demandante y razona la procedencia de la denegación de su petición, proporcionando así una motivación suficiente del rechazo, indicado que: la denegación del derecho de supresión se encuentra motivada conforme a derecho y amparada en las causas previstas en artículo 33.1 del Reglamento LOPD, ya que se trata de un sobreseimiento provisional acordado por un Juez de Instrucción. Por lo que el mantenimiento de los datos relacionados con la denuncia origen del procedimiento penal es necesario para el efectivo derecho a la seguridad de la víctima de la violencia de género, conforme a la Ley Orgánica 1/2004, de protección integral contra la violencia de género, hasta que, por la Autoridad judicial, se acuerde el sobreseimiento libre y, en todo caso, hasta la prescripción del delito denunciado.

Pues bien, la Sala considera que "El artículo 22.4 LOPD mencionado contiene una regla general –cancelación de los datos "cuando no sean necesarios para las averiguaciones que motivaron su tratamiento"- y varios criterios, a modo de ejemplo, para interpretarla; en este caso es relevante considerar el criterio de la resolución judicial firme, "…en especial la absolutoria, el indulto, la rehabilitación y la prescripción de la responsabilidad"; así, los datos cuya cancelación se solicita, que constan en el fichero policial, tienen su origen en una denuncia que, a su vez, dio lugar a un procedimiento judicial sobreseído provisionalmente poco después. Esta clase de resoluciones (Auto de sobreseimiento provisional) no se mencionan entre las resoluciones judiciales citadas en el criterio legal, que tienen en común el referirse a causas extintivas de la responsabilidad criminal o a la inexistencia de ésta por recaer sentencia absolutoria, o sobreseimiento libre, aunque no se incluya en el texto del precepto, ausencia de responsabilidad que no sucede cuando se trata de un sobreseimiento provisional, aunque la resolución en que se acuerde sea firme, al no haber sido recurrida por ninguna de las partes, incluido el propio denunciado, teniendo en cuenta, además, que el tiempo transcurrido entre la inclusión de los datos en el fichero y la solicitud de cancelación es escaso; así, la resolución administrativa hace una correcta y razonada aplicación de la norma y por ello procede confirmarla"

Muy similar es la **Sentencia de 2 de julio de 2021** Recurso 1495/2020, que confirma la resolución de la AEPD por la que se inadmite una reclamación ante la denegación de cancelación de los antecedentes policiales del fichero INTPOL de la Guardia Civil. También aquí la Sala acoge el criterio de la AEPD y recuerda lo antes indicado sobre la natura-

leza del Auto de Sobreseimiento Provisional como parámetro para la aplicación del artículo 22.4 de la LOPD.

En la **Sentencia de 26 de marzo de 2021**, Recurso 265/2020 se resuelve el recurso interpuesto contra la resolución de inadmisión de la AEPD referido a la solicitud de cancelación los antecedentes policiales del fichero PERSONAS que la Dirección General de la Policía denegó.

El afectado fue condenado como responsable en concepto de autor de un delito de Corrupción de menores, a la pena de prisión, de un año y seis meses, con la accesoria de inhabilitación especial para el derecho de sufragio pasivo. El actor entiende que la resolución de la Dirección General de la Policía no está suficientemente motivada por cuanto realiza una copia literal del artículo 23 de la LOPD.

La Sala considera que no es suficiente la motivación y declara la nulidad de la resolución impugnada, con retrotracción de las actuaciones a fin de que se admita a trámite la reclamación de supresión de datos.

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

La **Sentencia de 7 de mayo de 2021** que resuelve el Recurso 25/2020 interpuesto por la entidad responsable del motor de búsqueda, tiene por objeto una resolución de la AEPD que estima la reclamación de un afectado, consistente en la eliminación de los resultados de búsqueda de tres enlaces de páginas webs de medios informativos dónde recogen noticias sobre un escándalo relacionado con la expedición de títulos universitarios por parte de una universidad presidida y fundada por el reclamante, y que recoge que los periodistas descubrieron que era en un centro de estética dónde se expedían los títulos académicos, en nombre de una “falsa universidad”.

La resolución de la AEPD estima la reclamación por considerar que se tratan de hechos pasados sin que pueda considerarse que tiene incidencia en el presente o que la información pasada adquiera relevancia con hechos actuales y que ya poco pueda contribuir al debate público.

Pues bien, la Sala rechaza el sentido de la resolución al considerar que las informaciones publicadas por los medios de comunicación presentan relevancia e interés público incuestionables pues incluso la Subdirección General de Títulos y Reconocimiento de Cualificaciones del Ministerio de Educación, Cultura y Deporte, se pronunció sobre el tema indicando que el organismo que presidia el afectado no era una institución autorizada como universidad, ni tampoco tenía derecho a extender títulos de licenciado o doctorado.

Se considera que la información se refiere a la vida profesional del reclamante, como presidente de la Universidad Internacional Albert Schweitzer, y no a la vida personal, pues ello es muy relevante para modular la intensidad que ha de merecer la protección del derecho regulado en el art. 18.4 de la Constitución. Así, en la página web de la Albert Schweitzer International University, se dice, entre otras cosas, en relación con el afectado que es presidente fundador de la Universidad Internacional Albert Schweitzer y presidente de la London Diplomatic Academy.

En cuanto al factor tiempo, principal argumento para la estimación de la reclamación por la AEPD, indica la Sala que, sí es cierto que las URL disputadas hacen referencia a informaciones del año 2008, pero lo cierto es que sigue activa la Universidad Internacional Albert Schweitzer, apareciendo en la página web de la misma, el afectado como presidente fundador.

Concluye la Sala: debe prevalecer, frente al derecho a la protección de datos del afectado el derecho a la libertad de información y expresión y el interés preponderante del público en conocer y tener acceso a la citada información, en una búsqueda que verse sobre el nombre del interesado.

La **Sentencia de 21 de mayo de 2021** que resuelve el Recurso 498/2019 interpuesto por la entidad responsable del motor de búsqueda, tiene por objeto una resolución de la AEPD que estima la reclamación de un afectado, consistente en la eliminación de los resultados de búsqueda de 8 enlaces a páginas web referidos a medios de comunicación digitales y blogs, en los que se publican noticias del año 2012 referidas a supuestos abusos sexuales cometidos por el interesado, que se sobreseyeron por Auto de 27 de mayo de 2014 del Juzgado de Instrucción confirmado en apelación por el Auto de la Audiencia Provincial, de fecha 1 de marzo de 2016. La resolución de la AEPD acoge la pretensión del afectado considerando que (…) prevalece el derecho del reclamante al tratarse de datos obsoletos de los que no se ha demostrado la veracidad expuesta en las informaciones de los blogs reclamados y procede la exclusión de sus datos personales a través de una búsqueda en Internet "que verse sobre el nombre de esa persona (…).

Pues bien, la Sala rechaza el sentido de la resolución recurrida y considera que no procede la eliminación de los enlaces en base a que se refiere a la vida profesional del reclamante, sacerdote y psicólogo, y entonces Director Nacional de la ONG "Asociación Internacional del Teléfono de la Esperanza, y no la vida personal. Es más, en el Auto de 1 de marzo de 2016 de la Audiencia Provincial se dice en relación con el afectado, "… que se le podrá exigir responsabilidad en el ámbito de la mala praxis profesional…".

En cuanto al factor tiempo, si bien los enlaces discutidos hacen referencia a la detención del reclamante por el delito de abusos sexuales seguido en el Juzgado de que, por Auto de 27 de mayo de 2014, se decretó el sobreseimiento provisional de la causa, la libertad de información no viene condicionada por el resultado de los procesos penales -Sentencias de la Sala de lo Civil del Tribunal Supremo de 31 de mayo de 2001, recurso 1.230/1996, y de 16 de octubre de 2012 recurso 2.050/2010-.

En consecuencia, afirma la Sala que nos encontramos ante unas informaciones sobre la actividad profesional del reclamante, y ello se deriva de los hechos imputados en el procedimiento penal a aquel. En efecto, en el Auto de la Audiencia Provincial de 1 de marzo de 2016, se dice que se había acreditado que la relación entre aquel y la denunciante "se inició como terapia, de tal manera que el imputado era el terapeuta, que iba a ayudar a la paciente, y ésta confió plenamente en esas palabras". Por otro lado, el cargo que ostentaba el reclamante, Director Nacional de la ONG "Asociación Internacional del Teléfono de la Esperanza", tiene una relevancia profesional. Y añade que no existe constancia de que se trate de datos inveraces, ya que lo que se recoge en las informaciones es la detención del reclamante por un delito de abusos sexuales, y el hecho de que posteriormente se decretara el sobreseimiento provisional de las actuaciones penales por Auto de 27 de mayo de 2014 del Juzgado de Instrucción, confirmado posteriormente por el Auto de 1 de marzo de 2016 de la Audiencia Provincial no condiciona la protección de la libertad de información, (Sentencia de la Sala de lo Civil del Tribunal Supremo de 16 de octubre de 2012 -recurso 2.050/2010-),

La **Sentencia de 21 de julio de 2021** que resuelve el Recurso 217/2021 interpuesto por el afectado, tiene por objeto una resolución de archivo de la AEPD que da por buena la denegación de supresión que realiza la entidad responsable del motor de búsqueda de cinco enlaces de distintos medios de comunicación. Los hechos, son en síntesis que el reclamante se dirigió a la entidad responsable del motor de búsqueda en fecha de 17/06/2020 alegando que es un agente de la Policía Nacional en Canarias, que fue acusado injustamente de detención ilegal y fabricación de pruebas falsas contra cuatro personas que habían sido detenidas en una operación antidroga, habiendo dictado con fecha 19/07/2017 la Sala de lo Penal del Tribunal Supremo sentencia que anulaba de la Sentencia

de 01/02/2016 de la Audiencia Provincial de Las Palmas que era injustamente condenatoria contra él. Sin embargo, a pesar del tiempo transcurrido, en el buscador dicha información sigue apareciendo indexada a su nombre en distintos medios de comunicación sin tener en cuenta el resultado final del procedimiento judicial y que es una información sensible para la reputación personal, social y profesional del reclamante, agente de la Policía Nacional, y obsoleta pues se remonta a 16 años atrás y además desactualizada, pues no recoge el fallo absolutorio de 19 de julio de 2017 de la Sala 2ª del Tribunal Supremo

Frente a ello la Sala confirma la resolución de archivo de la AEPD en base a que los enlaces hacen referencia al demandante policía nacional en Canarias, en relación con su actividad profesional como tal policía nacional, circunstancia que ha sido especialmente destacada por la Sala como muy relevante para modular la intensidad que ha de merecer la protección del derecho regulado en el artículo 18.4 de la Constitución. La Sala ha considerado en varias ocasiones que cuando se trata de noticias sobre un proceso penal referido a la actividad profesional de una persona, como es el caso, tal información, sino resulta obsoleta ni vulnera el principio de calidad de datos, sí tiene la suficiente relevancia, que justifica que prevalezca el interés del público general de dichos datos personales sobre los derechos reconocidos en los arts. 7 y 8 de la Carta Europea de Derechos Fundamentales.

Un aspecto importante a tener en cuenta es que de la lectura de dicha sentencia que aporta el reclamante para justificar su absolución es que no efectúa un pronunciamiento absolutorio sobre el fondo, sino que lo que acuerda el Alto Tribunal es la nulidad de la citada sentencia, ordenando la repetición del juicio con diferentes Magistrados, porque uno de los Magistrados debería haberse abstenido.

La **Sentencia de 2 de noviembre de 2021** recaída en el Recurso 781/2018 interpuesto por el afectado, tiene por objeto una resolución desestimatoria de la AEPD que da por buena la denegación de supresión que realiza la entidad responsable del motor de búsqueda de ocho enlaces de distintos medios de comunicación que considera vulnerar su derecho a la protección de datos y a la intimidad. La Sentencia es contraria a la desestimación que realiza la AEPD, pero por cuestiones formales, es decir, de acuerdo con la LOPD aplicable a la tramitación del procedimiento de Tutela de Derechos, el plazo de 6 meses desde que se inicia el mismo determina el silencio positivo, por lo que se ha de entender estimada la reclamación y, por tanto, el responsable del tratamiento debe conceder el derecho solicitado.

En cuanto al ejercicio de los derechos previstos en los artículos 15 a 22 del RGPD, y en su caso los previstos en la LOPDGDD, al margen del "derecho al olvido", es preciso citar, la **Sentencia de 4 de junio de 2021** que resuelve el Recurso 1862/2019 y que trata sobre la impugnación de la resolución de la AEPD que valida la actuación de la Consejería de Sanidad de la Comunidad de Madrid-Instituto Madrileño de la Salud.

El fondo del asunto se refiere a cómo ejercitar el derecho de acceso, rectificación y supresión. En concreto los hechos son que un afectado ejerce estos derechos en relación con los datos que tuvieran todos los organismos e instituciones de salud pública de la Comunidad de Madrid, y que no habían sido atendidos, derivados de un accidente de tráfico que tuvo el 6 de diciembre de 2017.

La Sala confirma la resolución de la AEPD, por entender que nos encontramos ante una solicitud de acceso, supresión y rectificación realizada de forma genérica, y en ningún momento el actor ha aportado un listado de los centros sanitarios de la Comunidad de Madrid a los que quería dirigir su solicitud, insistiendo en querer tener todo lo concerniente a su persona de todos los centros existentes. En este sentido, se le contestó por el responsable del tratamiento, que debía subsanar en el plazo de diez días lo siguiente:

- Concreción del órgano ante el que desea ejercer sus derechos.
- Enumeración de los ficheros a los quiere acceder.

- Enumeración de los ficheros de los cuáles se requiere la cancelación, indicando a qué datos se refiere y acompañando documentación justificativa de lo solicitado.

- En el supuesto de solicitar la rectificación, adjuntar los documentos que acrediten y justifiquen la corrección.

El Tribunal entiende que dicha petición de subsanación encuentra respaldo en el art. 13.1 de la Ley Orgánica 3/2018, de 5 de diciembre, que dispone: "… Cuando el responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud". Por tanto, se ha atendido la reclamación habida cuenta, que el ejercicio de los derechos se realizó de manera genérica, como también se hace en la demanda. No debemos olvidar de la posibilidad que le concede al responsable del tratamiento el art. 12.5 del RGPD, que dispone: "Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá: a) cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o b) negarse a actuar respecto de la solicitud".

La **Sentencia de 14 de junio de 2021** recaída en el Recurso 1061/2018 trata sobre la impugnación de la resolución de la AEPD que inadmite una reclamación contra la actuación del Servicio Canario de Salud, que trata sobre la rectificación de los datos de salud del reclamante obrantes en su historial clínico.

Se solicita por el afectado que "se condene a la Administración a cancelar los datos del diagnóstico de enfermedad mental de bipolaridad, bien por error de diagnóstico, bien por prescripción, y calificativo de persona peligrosa". Añade que los datos que contiene el historial clínico son erróneos e inexactos, por lo que tiene derecho a su cancelación de acuerdo con lo dispuesto en la LOPD y en la Ley 41/2002, de 14 de noviembre, ignorando la antigüedad de los datos que, de ser superior a cinco años, tendrían que ser cancelados.

La Sala confirma el criterio de la AEPD tras analizar la explicación que otorga el Servicio Canario de Salud señalando que la conservación de los datos tiene como finalidad prestar la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo cinco años, de lo que no cabe deducir que, en este caso, en que no se ha determinado la fecha de inclusión de los datos en la historia clínica, pasados cinco años han de cancelarse o suprimirse. Y menos aún que en el ámbito de los procedimientos previstos en la normativa de protección de datos se puedan discutir el acierto o la precisión de valoraciones o apreciaciones de los facultativos que pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas. En conclusión, la desestimación por el Servicio Canario de Salud de la solicitud formulada por el recurrente es ajustada a la normativa de protección de datos personales.

La **Sentencia de 15 de junio de 2021** que resuelve el Recurso 146/2019, interpuesto por una particular frente a la resolución de la AEPD de inadmisión. Los hechos son que la AEPD considera que la entidad ha atendido el derecho ejercido de oposición y supresión por la reclamante sobre las publicaciones que sobre su persona aparecen en cinco enlaces de un sitio web dedicado a publicar información proveniente del Boletín Oficial del Registro Mercantil derivados de su condición de administradora única de dos empresas. La Sala confirma el criterio de la AEPD indicando que ha resultado probado en las actuaciones, y no desvirtuado mediante prueba alguna en contrario, que la página web analizada se limita a exponer y hacer accesible la información publicada sobre cualquier sociedad en los boletines oficiales y disponible para cualquier ciudadano en el Registro Mercantil.

Por tanto, el tratamiento de los referidos datos personales por parte del responsable, al existir un interés público en tener acceso a la información mercantil de ambas sociedades, información mercantil que incluye los datos de su adminis-

tradora, se adecua a lo previsto en el artículo 6 apartado f) del RGPD. Y si bien es cierto que la recurrente ejercitó, además del derecho de supresión , los derechos de limitación y oposición al tratamiento de los mismos datos personales, se desprende de la lectura los preceptos afectados la mayor amplitud y contundencia del derecho de supresión, por lo que en cierto modo abarcaría los otros dos, especialmente cuando se considera improcedente, de modo claro y categórico, el ejercicio de tal derecho de supresión, lo que conlleva la inadmisión de los otros dos derechos ejercitados.

La **Sentencia de 5 de noviembre de 2021** que resuelve el Recurso 691/2018 interpuesto frente a la resolución de inadmisión de la AEPD planteada por un afectado contra la denegación de cancelación ante una entidad financiera.

Los hechos son que consideró que sus datos se incluyeron indebidamente en la Central de Información y Riesgos del Banco de España (CIRBE) por parte de ABANCA. CIRBE comunica a la afectada que la información se corresponde con un crédito hipotecario ante el que el demandante aparece como garante solidario y que la operación aparece impagada y con saldo deudor, a 29 de septiembre de 2014, de 14.946.960,40 de dólares que, al parecer, ha sido reclamado ante los tribunales del Estado de México, sin que de todo ello se haya realizado notificación o requerimiento alguno. ABANCA por su parte, manifestó que no era posible la cancelación al ser el riesgo objeto de reclamación ante los tribunales de México.

La Sala considera que el CIRBE no es un fichero de solvencia patrimonial y no le son de aplicación las normas específicas ni los requisitos previstos en la normativa de protección de datos para este tipo de ficheros; es un servicio público y por ello no está regulado por el artículo 29 de la LOPD, lo que no excluye la aplicación del resto de la LOPD. Ello no excluye que los datos que se le declaren a esta entidad no deban ser exactos, pues como dice el artículo 60 de la Ley 44/2002, "los datos declarados a la CIR por las entidades obligadas serán exactos y puestos al día, de tal forma que respondan con veracidad a la situación actual de los riesgos y de sus titulares en la fecha de la declaración".

Así es preciso tener en cuenta que consta en el expediente la respuesta detallada proporcionada por la entidad bancaria, así como copia del contrato de crédito hipotecario y estado de la deuda y su evolución. En este caso el nombre y NIF del demandante figuran en la documentación proporcionada por la entidad bancaria al CIRBE, asociados al contrato de crédito hipotecario que parcialmente se ha aportado con la demanda, en la que se menciona repetidamente al actor como obligado solidario, cuya simple negativa, no refrendada por la presentación de denuncia policial, judicial o protesta ante el banco, u otra reacción ante esa supuesta suplantación de su personalidad o simple coincidencia del nombre y dos apellidos con los de otra persona, carece de fuerza para dudar sobre la exactitud del dato en este aspecto. Y, en cuanto al resto de cuestiones que plantea sobre las cláusulas del contrato o la liquidación de intereses o ausencia de notificación del conocimiento de la reclamación judicial en México, no tienen incidencia en este ámbito de la protección de datos, como señala la Resolución impugnada, y no se ha producido infracción de los artículos 16 LOPD y 33 de su Reglamento de aplicación.

En cuanto a la infracción del artículo 5.4 LOPD referente al cumplimiento de la obligación de informar en la recogida de datos, los datos proporcionados por las entidades bancarias a la CIRBE lo son en cumplimiento de una obligación legal (artículo 60, Segundo de la Ley 44/2002), por lo que le sería de aplicación la excepción prevista en el mismo artículo 5.5.

Y finalmente, en cuanto a la vinculación con el consentimiento, la Sala recuerda que hay que conjugar las disposiciones generales contenidas en la LOPD con las específicas de la Ley 44/2002, cuyo artículo 60 quinto, excepciona la necesidad de contar con el consentimiento del titular cuyos datos han sido facilitados la CIRBE.

Por su parte, como se ha indicado antes, el Tribunal Supremo dictó un total de 4 resoluciones, confirmando todas ellas el criterio de la AEPD, de las que conviene destacar las siguientes:

La **Sentencia de fecha 18 de febrero de 2021**, que resuelve el Recurso de Casación 232/2021 tiene por objeto la imposición de una sanción a una entidad financiera por vulneración del artículo 4.3 de la LOPD, si bien el interés casacional es el derivado de la aplicación del artículo 85.3 de la LPACAP en relación con los artículos 24 y 103 CE, a fin de esclarecer si la renuncia a acciones o recursos a la que se refiere el citado precepto abarca únicamente a la vía administrativa, o también a la vía judicial.

La Sala dice que la renuncia o el desistimiento que se exigen en el referido precepto para poder beneficiarse de las reducciones en el importe de la sanción se proyectan única y exclusivamente sobre las acciones o recursos contra la sanción a ejercitar en la vía administrativa y no en la judicial. Y esa claridad hace innecesaria la utilización de cualquier otro método de interpretación (in claris non fit interpretatio), (por todas, baste citar la STS n.º 1582/2020, de 23 de noviembre, RCA 4333/2019).

Ahora bien, una cosa es que en tales casos subsista la posibilidad de impugnar en la vía jurisdiccional contencioso-administrativa la resolución sancionadora, y otra distinta que el sujeto que se haya visto beneficiado por la reducción de la sanción tenga que asumir, como contrapartida lógica, que se incremente la dificultad para impugnar con éxito en la vía judicial contencioso-administrativa la resolución sancionadora, porque esa será la consecuencia natural de haber reconocido voluntariamente su responsabilidad en aplicación de los principios de buena fe y de vinculación a los propios actos, que exigen a todos los sujetos que intervienen en el procedimiento la debida coherencia en sus comportamientos procesales.

Por lo que para que dicha impugnación pueda tener éxito tendrá que proporcionar al juzgador una sólida explicación que justifique cumplidamente el motivo por el que, habiendo asumido primeramente su responsabilidad por la infracción cometida -que conlleva el reconocimiento de la concurrencia de los elementos objetivo y subjetivo de la infracción, es decir, de su participación en los hechos tipificados y de su culpabilidad-, después, en vía judicial, sostiene la inexistencia de la infracción, negando la concurrencia de los mencionados elementos constitutivos de la infracción y evidenciando así un comportamiento procesal notoriamente contradictorio.

La **Sentencia de 28 de febrero de 2021**, recaída en el Recurso de Casación 244/2021 que confirma el criterio de la AEPD y que versa sobre el derecho de supresión ejercido frente a una confesión religiosa.

Se analiza qué datos son susceptibles de conservación por la confesión religiosa Testigos de Jehová al analizar la procedencia en la contestación que ofrecen a un afectado que tras de ser expulsado de dicha congregación solicita la supresión de sus datos.

La AEPD considera que podrían conservarse los datos referidos al nombre, fecha de bautismo y fechas de des asociación, y no todos aquellos que pretende justificar la congregación como son además de los indicados, el nombre de la congregación, la fecha de nacimiento y el sexo. Todo ello encaminado para satisfacer su interés legítimo y no solo en el procedimiento de readmisión. Así, las alegaciones de la confesión religiosa son, en síntesis, que tienen el derecho de determinar caso por caso, que datos personales conservará de exmiembros que solicitan la supresión de sus datos, cuanto tales datos sean necesarios para sus finalidades religiosas y para el cumplimiento de sus intereses y actividades legítimas. Asimismo, sostienen que se vulnera el derecho a la libertad religiosa (autonomía y autoorganización de la confesión). Y esgrimen los siguientes argumentos para conservar los datos:

- Nombre de la congregación: son los ancianos de la misma congregación los que deben readmitir. Los expulsados a veces no recuerdan el nombre de la congregación. Hay 150.000 en España.

- Fecha de nacimiento: para mejor identificación, coincidencia de nombre y evitar el Re-bautismo.

- Sexo: identificar mejor a la persona, hay extranjeros que por el nombre no se deduce este aspecto.

La Sala parte de que a diferencia de la LOPD que reconocía una excepción a la exigencia de consentimiento expreso y por escrito en favor de las Iglesias, Confesiones o Comunidades religiosas, respecto de los datos de carácter personal de "sus asociados o miembros", sin ninguna referencia expresa respecto de quienes habían abandonado la confesión religiosa y ya no reunían, por tanto, esa condición de asociados o miembros, la regulación del RGPD excluye de forma expresa de la prohibición de tratamiento de datos especialmente protegidos el tratamiento por las asociaciones y organismos religiosos de los datos no solo de los miembros actuales sino también de los miembros "antiguos". Y si bien el RGPD no es de aplicación, al menos debe citarse a título interpretativo pues ambas partes los han citado las disposiciones del RGPD como fundamento de sus respectivas pretensiones.

La Sala coincide con las apreciaciones de la sentencia impugnada en el sentido de que la conservación por la Confesión religiosa de los datos personales de su exmiembro sobre los que versa este recurso no supera el juicio de proporcionalidad, atendiendo los datos personales cuya conservación ha sido admitida por la resolución de la AEPD que se encuentra en el origen de este recurso, especialmente el nombre y apellidos que, desde luego, es el dato idóneo y necesario para la identificación de quien ha dejado de ser miembro de la Confesión religiosa en el caso de una eventual e incierta solicitud de readmisión. Asimismo, debe estimarse que la combinación del nombre propio y los dos apellidos del exmiembro son suficientes en este caso, por sí solos, para su identificación en la eventualidad de que en el futuro solicite la readmisión en la Confesión religiosa, sin que sea, por tanto, exigible la fecha de nacimiento. Lo mismo sucede con el dato del sexo si se pretende utilizar para una mejor identificación. Y respecto del nombre de la congregación a la que pertenece el exmiembro, se llega a la conclusión de que existen otras medidas más moderadas o, si se quiere, menos restrictivas o invasivas del derecho fundamental a la protección de datos, como el apuntado tanto por la resolución de la AEPD como por la sentencia impugnada, que aluden a la simple solicitud o pregunta al exmiembro de este dato del nombre de la congregación a la que pertenecía, en la hipótesis de que solicite su readmisión, a fin de dar respuesta a dicha solicitud.

Finalmente, también se rechaza la pretensión referida a que la conservación de los datos personales no quede limitada al supuesto de que medie una nueva petición de ingreso del afectado en base a un interés legítimo de usar los datos para otras finalidades más allá de la readmisión, pues dicha pretensión se hace en abstracto sin justificar a que otras finalidades pue responder dicha conservación.

En consecuencia fija la siguientes doctrina que presenta interés casacional: una Confesión religiosa tiene el derecho a la conservación de los datos personales de quien abandonó la confesión que sean necesarios para sus fines religiosos, ante una solicitud inicial de supresión total de los mismos, en los términos que resultan del artículo 9.2.d) del RGPD, y los concretos datos a los que alcanza este derecho de conservación son los que, en cada caso, superen el juicio de proporcionalidad que exige el cumplimiento de los tres requisitos o condiciones de idoneidad, necesidad y proporcionalidad en sentido estricto.

La **Sentencia de 13 de diciembre de 2021** que resuelve el Recurso de Casación 1456/2021 que aborda un caso de suplantación de identidad para la obtención de un microcrédito y que tuvo como consecuencia que, ante el impago del mismo, los datos del suplantado se incluyeran en un fichero de información crediticia. Se concreto el interés casacional en relativo a la formación de jurisprudencia consiste en interpretar la normativa de protección de datos de carácter personal vigente a efectos de aclarar si la intervención fraudulenta de un tercero, que suplanta la identidad de otra persona en una contratación online, permite excluir la infracción del necesario consentimiento inequívoco para el tratamiento de los datos personales que exige el artículo 6 LOPD (actual artículo 6 LOPDGDD) al entender que la empresa

contratante actuó con diligencia suficiente y en la creencia de que contrataba con el verdadero titular de tales datos.

La Sentencia analiza el deber de diligencia de la entidad sancionada y considera que aun existiendo, y aplicándose, las medidas previstas por la empresa (registro en la plataforma; validación del DNI: con verificación de doble factor de 2 algoritmos que garantizan tanto la veracidad del número y la letra del documento como que el solicitante tiene en su poder el DNI, por original o copia; validación del número de teléfono móvil a través de un código PIN, validación de datos bancarios y validación de la tarjeta de crédito/débito aportada por el solicitante); y pese a la adopción de tales medidas, se podría haber cometido el delito de suplantación de identidad, de estafa y/o de uso indebido de documento verdadero.

La fase del procedimiento de contratación del préstamo denominada "validación de datos bancarios", que consiste en verificar si la cuenta bancaria "es real" y está asociada efectivamente a una cuenta bancaria, es también irrelevante desde el punto de vista del respeto a las obligaciones impuestas por la normativa de protección de datos, pues sólo asegura el buen fin del préstamo, esto es, que el importe prestado se dirigirá a una cuenta abierta y activa, pero nada aporta en cuanto a que el titular de esa cuenta sea precisamente la persona que figura en el DNI utilizado. Dice la Sala que ninguna de las medidas adoptadas por la recurrente está destinada a acreditar que la persona que solicita el microcrédito coincide con el titular del DNI aportado.

El Supremo concluye que no puede recaer sobre la empresa contratante la responsabilidad de impedir que se produzca un hecho ilícito o delictivo como es la utilización fraudulenta de un DNI por parte de quien no es su titular. Pero lo que sí es exigible es la diligencia necesaria para que no se le pueda reprochar el incumplimiento de sus obligaciones en materia de protección de datos de carácter personal -tanto en lo que se refiere a la exigencia de consentimiento del interesado como en lo relativo al principio de veracidad y exactitud de los datos- la implantación de medidas de control tendentes a verificar que la persona que pretende contratar es quien dice ser, esto es, que coincide con el titular del DNI aportado

Fijando la siguiente doctrina: la intervención fraudulenta de un tercero, que suplanta la identidad de otra persona en una contratación On line, no excluye que la empresa contratante, que lleva a cabo el tratamiento de los datos personales, haya podido incurrir en infracción por falta del necesario consentimiento inequívoco que exige el artículo 6 de la Ley Orgánica 3/2018, de 5 de diciembre, pues aquella intervención fraudulenta de un tercero no implica por sí misma que la empresa contratante haya actuado con diligencia suficiente.

Finalmente, en el ámbito de la justicia europea, se han dictado resoluciones por el Tribunal de Justicia Europeo (TJUE) entre las que cabe citar la **Sentencia de 22 de junio de 2021,** recaída en el Asunto C-439/2019, que interpreta el alcance del concepto de "infracciones penales" del artículo 10 del RGPD, al abordar lo relativo al tratamiento de datos referidos a infracciones de tráfico de acuerdo con la normativa de Letonia. Así, puede decirse que el concepto de "infracción penal" no depende su contenido según lo que sea delito en cada Estado miembro, sino que es un concepto autónomo de derecho de la UE, según tres criterios: la calificación jurídica de la infracción en Derecho interno, el segundo la propia naturaleza de la infracción y el tercero la gravedad de la sanción que puede imponerse al interesado. Incluso en el caso de infracciones que el Derecho nacional no califique de «penales», tal carácter puede derivarse, no obstante, de la propia naturaleza de la infracción de que se trate y del grado de severidad de las sanciones que esta pueda implicar (véase, a este respecto, la sentencia de 20 de marzo de 2018, Garlsson Real Estate y otros, C 537/16, EU:C:2018:193, apartados 28 y 32).

La calificación de las infracciones de tráfico que pueden implicar la atribución de puntos como «infracción penal», en el sentido del artículo 10 del RDPD, encaja asimismo con la finalidad de esta disposición. En efecto, la comunicación al público de datos personales relativos a infracciones de tráfico, incluidos los puntos impuestos

por su comisión, puede, habida cuenta de que tales infracciones constituyen un atentado a la seguridad vial, provocar la desaprobación de la sociedad y conllevar la estigmatización del interesado, en particular, cuando esos puntos ponen de manifiesto cierta gravedad o cierta frecuencia de dichas infracciones. De ello se deriva que las infracciones de tráfico que pueden implicar la atribución de puntos están comprendidas en el concepto de «infracciones» contemplado en el artículo 10 del RGPD.

En consecuencia, concluye que el artículo 10 del RGPD debe interpretarse en el sentido de que se aplica al tratamiento de datos personales relativos a puntos impuestos a conductores por infracciones de tráfico.

Por lo tanto, si bien el Tribunal no dice que con carácter general las infracciones administrativas se igualen a las infracciones penales, sí que se amplía en gran medida el espacio de estas.

3.3. Tecnológicos

La División de Innovación Tecnológica (DIT) se crea a principios del año 2016, como Unidad de Evaluación y Estudios Tecnológicos (UEET), formando parte de la Unidad de Apoyo de la Dirección. El objeto era disponer de una unidad que diera soporte a responsables, encargados y DPDs para la aplicación del principio de Responsabilidad Proactiva del Reglamento General de Protección de Datos (RGPD) y estudiase el estado del arte de los nuevos tratamientos de datos que involucraban el uso de tecnologías disruptivas.

De esta forma, la Agencia Española de Protección de Datos (AEPD) seguía el ejemplo de otras autoridades como la CNIL francesa, que dispone de una Dirección de Tecnologías e Innovación, o el ICO británico, que dispone de una Dirección Ejecutiva de Innovación y Política Tecnológica, entre otros.

Desde sus inicios, en el contexto del impulso del principio de Responsabilidad Proactiva, la DIT ha impulsado la creación de materiales y recursos de ayuda a responsables, encargados y DPDs en la aplicación práctica del principio de responsabilidad activa.

En julio de 2020, la antigua UEET toma su denominación actual y, en el recientemente aprobado RD 389/2021 por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos, la DIT viene depender directamente de la Presidencia de la AEPD asumiendo las siguientes competencias:

- Asesorar a la dirección de la AEPD, así como a sus distintas unidades, sobre los temas tecnológicos que tienen relevancia en la protección de datos de carácter personal. Analizar las implicaciones y alternativas del estado de arte de la tecnología y generar el conocimiento necesario para anticiparse a los cambios de la misma.

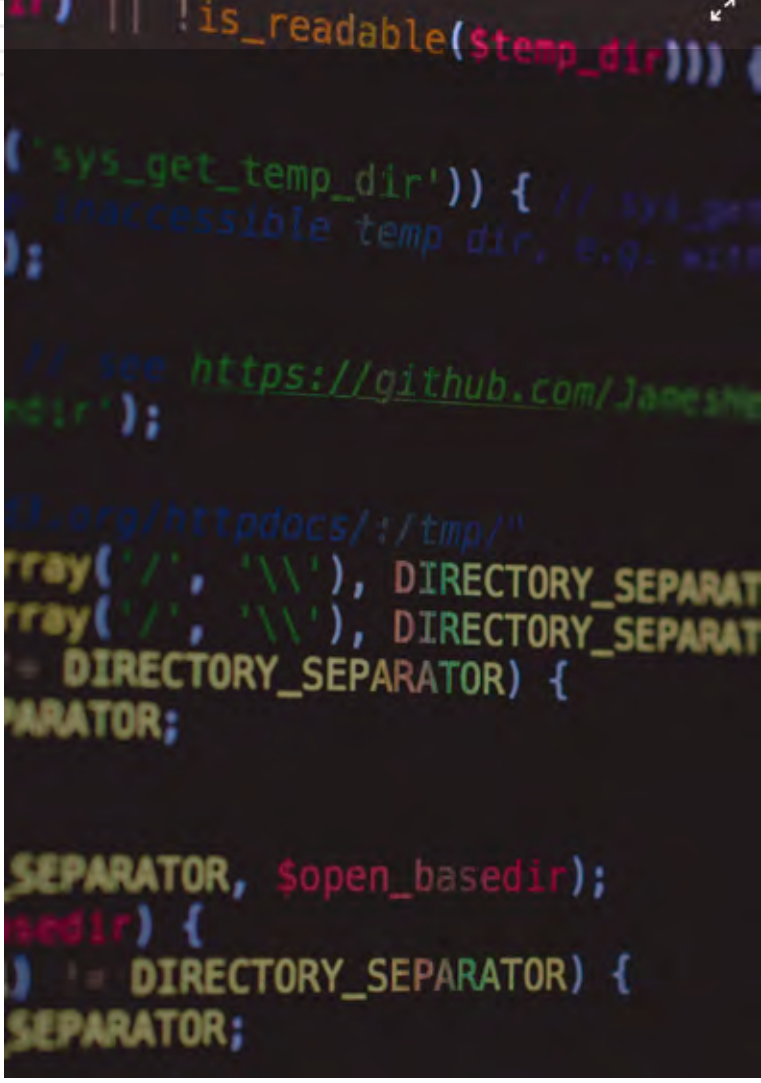
- Impulsar la protección de datos como un factor de confianza y garantía de calidad en beneficio del desarrollo económico de la sociedad con el objeto de promover la sensibilización de responsables y ciudadanos. Este punto incluye el desarrollo y mantenimiento de herramientas de ayuda para el cumplimiento por parte de los mismos y la elaboración de guías que impulsen el cumplimiento de aspectos específicos del principio de responsabilidad activa del Reglamento (UE) 2016/679 en el ámbito tecnológico, según su artículo 57.1. b) y d).

- Impulsar las medidas que garanticen la compatibilidad del desarrollo tecnológico con la privacidad asegurando los derechos de los ciudadanos según lo previsto en el artículo 57.1.i) del Reglamento (UE) 2016/679; en particular: el asesoramiento a emprendedores y desarrolladores tecnológicos, la realización de estudios de prospección tecnológica, informar y asesorar a los proyectos tecnológicos con implicaciones en el derecho a la protección de datos de las personas, participar en proyectos tecnológicos de ámbito internacional de interés público sobre la base del derecho de la Unión Europea o de los Estados Miembros y promover la colaboración con las Universidades con el fin de impulsar la protección de datos en proyectos y contenidos curriculares jurídicos y técnicos.

- Gestionar el Registro de brechas de seguridad para facilitar a los responsables el cumplimiento de lo previsto en el artículo 33 del Reglamento (UE) 2016/679. Analizar y clasificar las brechas de seguridad y, en su caso, proponer motivadamente a la dirección la iniciación de una investigación cuando aprecie indicios de la comisión de una infracción.

- Emitir informes, recomendaciones y dictámenes sobre las consultas previas relativas a la Evaluación de Impacto para Protección de Datos realizadas por los responsables conforme al artículo 36 del Reglamento (UE) 2016/679, en virtud de lo previsto en su artículo 57.1.l).

- La elaboración de una lista positiva y, en su caso, otra negativa de tratamientos que requieren la realización de evaluaciones de impacto según lo previsto en el artículo 57.1.k del Reglamento (UE) 2016/679.



A la fecha, la DIT consta de siete miembros, todos funcionarios: un nivel 30, cuatro niveles 28 (dos de ellos recién incorporados), un nivel 26 y un auxiliar. El perfil de los funcionarios del grupo A1 y A2 es tecnológico, aunque con profundos conocimientos en protección de datos, tecnologías y gestión de la responsabilidad proactiva.

Las actividades más destacadas de la DIT durante el año 2021 se describen a continuación:

3.3.1. Elaboración de guías y modelos, estudios y notas técnicas

Buena parte de las áreas de actividad en las que se encuentra implicada la DIT es la elaboración de guías, modelos, estudios y notas técnicas. Estas están enfocadas a responsables, encargados y DPDs, en las que se vierten recomendaciones de carácter técnico con relación a actividades concretas en las que existe un tratamiento de datos personales:

- Nueva versión de la 'Guía para la Gestión del riesgo y evaluación de impacto de datos para tratamientos de datos personales', que aúna y actualiza las dos guías publicadas en 2018.

- Actualización de la 'Guía de notificación de brechas de datos personales'.

- La guía de 'Requisitos para Auditorías de Tratamientos que incluyan IA'.

- La nota técnica 'Diez malentendidos relacionados con la anonimización', publicado en colaboración con el Supervisor Europeo de Protección de datos.

- Hoja de ruta para garantizar la conformidad con la normativa de protección de datos.

Estos recursos, junto con los anteriormente publicados, acumulaban un total de más de 140.000 descargas de usuarios directamente desde la página web de la AEPD, además de hacerse accesible a través de listas de distribución de DPDs.

A lo largo de 2021 también se ha participado con contenido relativo a la aplicación práctica de la responsabilidad proactiva del blog de la AEPD con las siguientes publicaciones desde el 1 de diciembre de 2020 al 30 de noviembre de 2021:

- IoT: Riesgos del Internet de las Cosas en el hogar y recomendaciones para un uso seguro
- IoT (II): Del Internet de las Cosas al internet de los cuerpos
- IoT (III): Domótica IoT
- Anonimización y seudonimización
- Anonimización y seudonimización (II) la privacidad diferencial
- Cifrado y Privacidad (V): la clav como dato personal
- Privacidad en reuniones online
- Teletrabajo y protección de datos en el ámbito digital
- Brechas de seguridad: Ransomware y gestión del riesgo
- Identificación en sevicios de pago online
- Htpps: Cifrado en la web

En colaboración con el Supervisor Europeo de Protección de Datos, han sido publicadas las traducciones al castellano de la 'Guía para evaluar la proporcionalidad de los tratamientos en políticas y medidas legislativas' y la 'Guía para Evaluar la Necesidad de los tratamientos en políticas y medidas legislativas'.

Están en progreso material adicional de soporte a responsables, encargados y DPDs con relación a la aplicación efectiva y eficiente de la responsabilidad proactiva y tecnologías como la Inteligencia Artificial, IoT, Blockchain y 5G.

3.3.2. Notificaciones de brechas de datos personales

El artículo 33 del RGPD establece la obligación y condiciones para que el responsable del tratamiento notifique a la autoridad de control competente toda brecha de datos personales. El artículo 34 establece las condiciones por las que será obligatorio la comunicación de una brecha de datos personales al interesado.

No es obligatorio notificar todas las brechas de datos personales, dado que el RGPD prevé una excepción a esta obligación cuando, conforme al principio de responsabilidad proactiva, el responsable pueda garantizar que es improbable que la brecha de datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas.

Las notificaciones de brechas de datos personales ante la Autoridad de Control son parte de la responsabilidad proactiva de los responsables, o encargados en su caso. Las notificaciones y comunicaciones de brechas tienen el objetivo de crear una sociedad más resiliente, proteger de forma efectiva los intereses de los sujetos de los datos y demostrar diligencia en los tratamientos de datos. La notificación de brechas realizada de acuerdo con el RGPD no implica la imposición de una sanción. Al contrario, una notificación y comunicación en tiempo y forma, en el caso de que la Autoridad de Control inicie actuaciones previas de investigación, es una evidencia de la diligencia de la organización a la hora de ejecutar eficazmente la obligación de responsabilidad proactiva requerida por el RGPD. Sin embargo, el no cumplir con las obligaciones de notificación y comunicación a los interesados sí está tipificado como infracción.

En determinados casos, tras la notificación de una brecha es necesario trasladar la notificación de la brecha de datos personales a la Subdirección General de Inspección de Datos para que estudien la existencia de una potencial vulneración de la normativa de protección de datos. El traslado de todas y cada una de las brechas notificadas a los servicios de inspección iría en contra del espíritu

del artículo 33 del RGPD, que es el de construir una sociedad más resiliente ante los incidentes de seguridad que afecten a datos de carácter personal mediante el intercambio de información entre responsables y las autoridades competentes y el fomento de una cultura de responsabilidad proactiva.

La AEPD publica en *la sección sobre brechas de datos personales de su página web*, resúmenes mensuales sobre la evolución de la notificación, las características de las brechas, la tipología de entidades afectadas, además de cifras sobre la comunicación de incidentes a los interesados. Cada informe incluye al principio una sección destacando aspectos relevantes detectados mediante el análisis de las notificaciones de brechas notificadas, proporcionando a las organizaciones información valiosa que puede contribuir a su resiliencia.

En el año 2021, las brechas de datos personales causadas por ciber incidentes de origen externo-malintencionado siguen teniendo el mayor protagonismo.

Dentro de este tipo de incidentes el ransomware es el más repetido, y siguen en aumento los casos en los que el cifrado de los datos y/o los sistemas va precedido de una exfiltración de información y su puesta a la venta en internet/darkweb. Los responsables y encargados de tratamiento deben tomar conciencia del riesgo que estos ataques plantean, y que apliquen medidas técnicas y organizativas apropiadas para afrontarlos. Es fundamental intentar evitar su materialización y tener capacidad para su detección temprana, para evitar o minimizar la exfiltración de datos personales, protegiendo su confidencialidad, además de evitar la pérdida de su disponibilidad. Además, la rápida evaluación de las consecuencias permite tomar acciones para minimizar el impacto sobre los derechos y libertades de las personas cuyos datos personales se hayan visto afectados.

En resumen, las actividades realizadas en torno a la gestión de la notificación de brechas de datos personales se pueden resumir de la siguiente forma:

- 1.647 notificaciones de brechas de datos personales se han gestionado durante el periodo entre el 1 de enero de 2021 y el 31 de diciembre de 2021.
- Publicación de nuevo formulario estructurado para la notificación de brechas de datos personales que facilita el cumplimiento de la obligación de notificar brechas de datos personales a la autoridad de control.
- Puesta en producción de herramienta interna de tramitación de notificaciones de brechas personales, que permite reducir los plazos de tramitación y de respuesta a los responsables del tratamiento.
- Seguimiento y evaluación de los criterios para el traslado a inspección de notificaciones de brechas de datos personales.
- Mantenimiento de la sección sobre brechas de datos personales con, entre otros, la publicación en la página web de la AEPD de los informes mensuales sobre brechas notificadas a la AEPD con un análisis sobre su tipología, además de agrupar todo el material de interés sobre brechas de datos personales.
- Publicación de la nueva guía sobre “Notificación de Brechas de Datos Personales” de la AEPD.
- Establecimiento de canal de traslado de notificaciones de brechas que sean de la competencia de una Autoridad de Control Autonómica
- Mantenimiento del canal de notificaciones de brechas de datos personales de la Sede Electrónica de la AEPD.

- Seguimiento del contrato para el desarrollo de un sistema de gestión de brechas que facilite la comunicación con el responsable y la gestión de las brechas de datos personales.

3.3.3.Evaluaciones de impacto y consultas previas

Con relación a las tareas relativas al análisis de las consultas previas relacionadas con la Evaluación de Impacto para Protección de Datos, durante 2021 se han remitido a la AEPD y gestionado un total de tan solo dieciocho solicitudes de consulta previa. Teniendo en cuenta la obligación a dicha consulta cuando una evaluación de impacto muestre que el tratamiento entrañaría un alto riesgo si no se toman medidas para mitigarlo, y la expansión de servicios basados en tecnologías disruptivas, surgen dudas de si los responsables y encargados del tratamiento están adecuadamente asesorados con respecto al cumplimiento de esta obligación.

Relacionado con el tema de las consultas previas, la DIT ha tenido una participación muy activa en los protocolos de pruebas (sandbox) establecidos en el artículo 8.3 de la Ley 7/2020, de 13 de noviembre, para la transformación digital del sistema financiero con la emisión de un total de 8 informes sobre proyectos de diversa índole.

La DIT presta también soporte al canal del DPD participando en aquellas consultas de índole técnico que se reciben, elaborando un total de nueve respuestas.

Con carácter general, el número de consultas previas recibido, y la calidad de las evaluaciones de impacto en protección de datos realizadas por los responsables, se evidencia un intento de cumplimiento meramente formal de los requisitos que exigen los artículos 35 y 36 del RGPD sin dar respuesta al enfoque de riesgos que exige el principio de responsabilidad activa del RGPD. Las consultas previas presentadas se han limitado a un análisis de riesgo de cumplimiento normativo y no, como establece el RGPD, una gestión en los riesgos que los tratamientos de datos personales implican para los derechos y libertades de los interesados. Los responsables, en la documentación presentada, han evidenciado desconocimiento de las guías, recomendaciones, instrucciones e informes publicados por la AEPD. En general, se advierte cierta confusión entre lo que es un informe de carácter jurídico y la documentación de un proceso de gestión de los riesgos que exige análisis, toma de decisiones y ejecución de acciones para implementar medidas y garantías. Finalmente, se advierte una ausencia del DPD tanto en sus obligaciones de asesoramiento (art.35.2), como de supervisión de la aplicación de la EIPD (art.39.1.c RGPD).

El RGPD hace alusión al término riesgo en numerosas ocasiones (artículos 4.24, 23.2.g, 24.1, 25.1, 27.2.a, 30.5, 32, 33, 34, 35, 36, 39.2, 49.1, entre otros). Los riesgos para los derechos y libertades de los interesados necesariamente deben identificarse y evaluarse en el marco adecuado para su gestión que, previamente, debe de haberse establecido. La gestión del riesgo es una disciplina que constituye uno de los pilares de la gestión de cualquier organización y, en ningún caso, la gestión del riesgo para los derechos y libertades de las personas físicas debe contemplarse como un elemento aislado del resto de procesos de una organización sino como un elemento más a gestionar de manera global por los responsables. Interpretar que el riesgo en materia de protección de datos, para dar respuesta a los requisitos que exige el RGPD, puede limitarse a un simple ejercicio de cumplimiento formal de las obligaciones de la normativa de protección de datos es contrario al espíritu al Working Paper 218 *(WP218)* relativo a la Declaración sobre el papel de un enfoque basado en el riesgo en el marco legal de la protección de datos y contrario al propio espíritu del RGPD.

Sin embargo, este no es el único malentendido en la aplicación de los requisitos del RGPD con relación a la EIPD. En muchas de las consultas previas presentadas se aprecia confusión entre el principio de proporcionalidad y el principio de minimización de datos, haciendo una interpretación que está lejos de lo que señala el considerando 4 del RGPD. Del mismo modo, el principio de necesidad del tratamiento también se viene a reducir al análisis de necesidad de llevar a cabo

la EIPD frente a la necesidad a la que el propio tratamiento, en sus finalidades y las distintas opciones de implementación, que tendría como objetivos dando respuesta a un adecuado balance riesgo-beneficio que dicho tratamiento pudiera tener para los sujetos de los datos.

Desde la DIT se ha impulsado las iniciativas necesarias para dotar a responsables y encargados de recursos de ayuda a fin de paliar las deficiencias y errores de interpretación que han venido observando desde la entrada en vigor del RGPD, publicando a lo largo de 2021, la nueva *Guía de análisis de riesgos y evaluaciones de impacto en protección de datos*, una *lista de verificación formal del contenido de la documentación de la EIPD*, además de la herramienta *Evalúa-Riesgo* junto con un documento de *tablas* o anexos que permite a los responsables abordar los retos planteados por el RGPD para dar respuesta a las obligaciones que el RGPD establece en su enfoque de riesgos.

Otro de los problemas observados es la entrada en la AEPD de consultas previas por canales distintos al canal de consultas previas de la sede electrónica. Debe de tenerse en cuenta que los plazos señalados en el artículo 36 del RGPD son muy limitados y la entrada de consultas previas por canales externos al canal de consultas previas implica una gestión adicional de cada consulta que reduce considerablemente los plazos desde el punto de vista material. En este sentido, la Instrucción 1/2021, en general, viene a plantear requisitos mínimos a tener en cuenta con relación a la evaluación de impacto que debe de acompañar a la solicitud de consulta previa además de incluir la exigencia de utilizar el canal de consultas previas, evitando así, demoras innecesarias que reduzcan materialmente los plazos de respuesta.

3.3.4. Cooperación con asociaciones y otras entidades

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

- Autoridades Autonómicas de Protección de Datos en aspectos tecnológicos.
- Secretaría General de Administración Digital, (SGAD) en consultas sobre temas de regulación tecnológica.
- Secretaría de Estado de Digitalización e Inteligencia Artificial, a la que se han atendido sus consultas sobre temas tecnológicos con trascendencia en protección de datos.
- INCIBE, con relación a la coordinación en la comunicación de brecha de seguridad
- Consejo Superior de Investigaciones Científicas (CSIC), en la revisión de guías y notas técnicas
- Centro para el Desarrollo Tecnológica e Industrial (CDTI) Comisión del seguimiento del Convenio de Colaboración y en la revisión de guías.
- Comité Técnico de Normalización CTN-71 sobre Tecnologías Habilitadoras Digitales y en el Subcomité Técnico SC42 sobre Inteligencia Artificial y Big Data, como vocales.
- Universidad Carlos III-IMDE A Networks en temas de consultas tecnológicas.
- Universidad de Alcalá de Henares en el marco de una extensión del proyecto para estudiar técnicas de gobernanza en Blockchain y propuesta de elaboración de un convenio de colaboración.

- Universidad Nacional de Educación a Distancia (UNED), en la revisión de guías y como miembros del Advisory Board proyecto UNED Forensic GDPR.

- Universidad Nebrija: Convenio entre la Agencia Española De Protección de Datos y la Universidad Antonio de Nebrija sobre la realización de prácticas por parte de los alumnos de títulos propios de máster y máster oficiales.

- Fundación Éticas: colaboración el desarrollo de guías de auditorías de aplicaciones de Inteligencia Artificial

- Grupo OdiseIA, en colaboración en temas de Inteligencia Artificial.

- Asociación Profesional de Cuerpos Superiores de Sistemas y Tecnologías de la Información de las Administraciones Públicas (ASTIC), en la revisión de guías.

- Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información (AUTELSI) en la revisión de guías.

- Asociación Women in a Legal Word, en la revisión de guías y preparación de un Protocolo de Colaboración.

- Observatorio de Bioética y Derecho-Cátedra UNESCO de Bioética. Universidad de Barcelona, en la preparación de un Protocolo de Colaboración.

En relación con la participación en iniciativas internacionales de carácter tecnológico en protección de datos, las acciones más reseñables son las siguientes:

- Participación en el Subgrupo de Tecnología del Comité Europeo de Protección de Datos, entre otras cosas, participando como co-revisores en la guía de Blockchain y la guía de anonimización (pendientes de publicar), presentando la iniciativa AppCensus de IMDEA.

- Colaboración con el Supervisor Europeo de Protección de Datos, que se ha materializado en la publicación en común de una nota sobre equívocos en anonimización y se está trabajando en una herramienta conjunta de análisis de cookies.

- Definición del Componente 5 (Protección de Datos) del proyecto Twinning EU Support to E-Governance and digital economy in Ukraine y asunción del rol de Component Leader del proyecto.

- Participación en el grupo de Inteligencia Artificial de la Conferencia Internacional.

- Colaboración con la Universidad de las Naciones Unidas en el campo de Blockchain, con la que se ha firmado un nuevo MOU de colaboración.

- Colaboración con la Red Iberoamericana como revisores de los documentos publicados sobre Cloud Computing.

- Colaboración con la Autoridad Brasileña de Protección de Datos, con la que se ha firmado un MOU de colaboración.

- Colaboración con la asociación internacional Biometric Institute en la elaboración de una guía de buenas prácticas sobre biometría.

- Colaboración con la Escuela Politécnica Federal de Lausana, a través de la científica Carmela Troncoso, en la elaboración conjunta sobre la nota técnica "Recomendaciones para el despliegue de aplicaciones móviles para el control del acceso a espacios públicos".

- Asesoramiento a la Fundación Internacional y para Iberoamérica de Administración y Políticas Públicas (FIIAPP) en proyectos internacionales de protección de datos.

- Asesoramiento a grandes corporaciones tecnológicas (MICROSOFT, GOOGLE, AMAZON) y sector financiero (BDE).

- Colaboración con Agencia Europea para la Gestión Operativa de Sistemas informáticos de Gran Magnitud en el Espacio de la Libertad, Seguridad y Justicia (eu-LISA)

Finalmente, colaboración con la División Internacional de la AEPD en la participación española en acciones puntuales internacionales.

En cuanto a la obligación de asesorar a la Dirección de la AEPD, así como a sus distintas unidades, sobre los temas tecnológicos que tienen relevancia en la protección de datos, desde su creación la DIT participa de forma regular en las actividades e iniciativas de la AEPD.

Tales actividades son muy numerosas y listarlas sería prolijo, por lo que se destaca:

- Participación de miembros de la DIT como ponentes en diversos foros internacionales, como el BvD DPO Spring Congress 2021 en Alemania, el euLISA Webinar Privacy and data protection by design, o el Seminario RIPD 2021 (webinario) sobre Protección de datos ante la disrupción tecnológica: Computación en Nube e Inteligencia Artificial.

- Participación de miembros de la DIT como ponentes en diversos foros realizados en España con ámbito internacional y nacional, como II CONGRESO INTERNACIONAL: "Dinero Digital y Gobernanza TIC en la UE: nuevos estándares jurídicos y tecnológicos" de la Universidad de Alicante, II Jornada Protección de Datos Personales IAPP-UFV, Jornadas de Digitalización del Consello Económico e Social de Galicia, II Congreso Internacional "Dinero Digital y Gobernanza TIC en la UE" o Tres ponencias en el curso de la UIMP "Privacidad Innovación e Igualdad".

- Otra formación dirigida a otras instituciones y administraciones públicas (AECID, Ministerio de Justicia, de Inclusión, de Universidad, de Transporte, de Educación, de Política Territorial, Ayuntamiento de Madrid, etc.)

En cuanto a la formación interna, la DIT ha impartido:

- Curso interno introductorio al análisis de aplicaciones móviles
- Curso interno sobre cookies
- Curso interno sobre responsabilidad proactiva
- Curso interno de formación en el RGPD impartido a través de la plataforma del INAP a distintos Ministerios

- Realización de un videotutorial práctico sobre herramientas de la AEPD para el tercer sector

- Desde la DIT se viene dando soporte al canal INFORMA con relación a las consultas de índole técnica de los responsables, en general consultas relacionadas con aspectos sobre evaluaciones de impacto, análisis de riesgos, medidas de seguridad, tecnologías, tratamientos biométricos, notificaciones de brechas, etc.

- Asesoramiento técnico a la Dirección de la AEPD, al Gabinete Jurídico en la elaboración de informes y al resto de unidades de la AEPD.
- Colaboración en la preparación de intervenciones públicas de la Dirección de la AEPD.
- Asesoramiento técnico a la SGPA en la promoción de códigos de conducta.
- Asesoramiento técnico en la elaboración en guías y recomendaciones de otras unidades de la AEPD.
- Participación en los comités internos de la AEPD como: Comité de Coordinación, Criterios, Clasificación documental, Indicadores, Coordinación STIC, Coordinación Informática, Comité de Seguridad, Grupo Igualdad, Grupo para uniformizar las comunicaciones con intervinientes en los procedimientos electrónicos y CANOA.

3.3.5. Mantenimiento y desarrollo de herramientas

Para ayudar a responsables, encargados y DPDs en el cumplimiento de las obligaciones relativas a la responsabilidad proactiva se han publicado durante el año 2021 las siguientes herramientas:

- *COMUNICA-BRECHA* para asesorar a los responsables sobre su obligación de comunicar a los interesados una brecha de datos personales.
- *EVALÚA-RIESGO* para permitir la identificación y evaluación del riesgo para los derechos y libertades de los interesados.

Además del mantenimiento efectuado en las herramientas ya publicadas por la AEPD en años anteriores, se ha desarrollado el Website Evidence Collector, una herramienta interna, para su uso por la SG de Inspección, que está siendo adoptada por otras autoridades de protección de datos.

El *conjunto de herramientas ya disponibles para responsables y encargados* (FACILITA, FACILITA-EMPRENDE, GESTIONA-RGPD, EVALÚA-RIESGO COMUNICA-BRECHA) han tenido más de 79.000 ejecuciones desde el 1 de diciembre de 2020 hasta el 30 de noviembre de 2021.

3.3.6. Ciclo innovación y protección de datos. Mujer y Ciencia

En el marco de los compromisos de la Agencia en materia de responsabilidad social y sostenibilidad, especialmente en el ámbito de la tecnología y la protección de datos, así como con la igualdad de género, la AEPD ha celebrado a lo largo de 2021 un ciclo de seis debates (webinarios) sobre "Innovación y protección de datos. Mujer y ciencia", ya en su segunda temporada, con el que se ha continuado con los debates rigurosos sobre temas de actualidad.

El ciclo se reinició el 22 de junio con la ponencia "Innovación, protección de datos y transformación digital. Interfaz cerebro-computador y protección de datos" a cargo de Doña Yasna Bastidas Cid, ingeniera de telecomunicaciones e investigadora, cuya trayectoria profesional está vinculada con la construcción de sistemas y el desarrollo de metodologías que contribuyan a reforzar las garantías de privacidad en sus diseños y galardonada con el premio de Investigación en protección de datos Emilio Aced 2020, por la Agencia Española de Protección de datos.

Continuó el 3 de noviembre, con la doctora Doña Marta Beltrán Pardo presentando la ponencia "Identidad, biometría y privacidad". La doctora Beltrán Pardo es profesora e investigadora en la Universidad Rey Juan Carlos y profunda conocedora del mundo de la ciberseguridad y de las implicaciones que, para las personas, puede suponer el uso de la tecnología biométrica.

El ciclo del año 2021 se cerró el 24 de noviembre con la ponencia de Doña María López Escorial "Innovación, protección de datos y transformación social. Pobreza, emprendimiento social y negocios inclusivos", profesora del IE Business School desde 2002 y consultora independiente especializada en innovación social, principalmente el desarrollo de soluciones empresariales para

combatir la pobreza, y fomentar el emprendimiento social y los negocios inclusivos.

El ciclo ha contado con una amplia participación, especialmente desde el ámbito de las Autoridades Iberoamericanas de Protección de Datos, a quienes se ha dirigido. Los webinarios del Ciclo, tanto de la primera como la segunda temporada están accesible en la página web de la Agencia. La tercera temporada ya está previsto que se inaugure el 16 de marzo de 2022.

3.3.7. Otras acciones de impulso a la responsabilidad

Otras acciones realizadas por la DIT con el objeto de impulsar el cumplimiento del principio de responsabilidad activa del RGPD, en el marco del asesoramiento a emprendedores y desarrolladores tecnológicos con la finalidad de informar y asesorar en proyectos tecnológicos con implicaciones en el derecho a la protección de datos de las personas han sido el desarrollo y actualización de secciones de la página web de la AEPD:

- Actualización del espacio web *Innovación y Tecnología,* agrupando los contenidos tecnológicos por temáticas, en sus dos versiones en castellano e inglés.
- Actualización de *obligaciones del responsable.*
- Mantenimiento del espacio *Lucha Contra la Violencia de Género y la Violencia Digital* con una actualización publicada el 25 de noviembre.
- Mantenimiento del espacio *Brechas de datos personales.*
- Mantenimiento del espacio dedicado a la *Videovigilancia.*

Por otra parte, los miembros de la DIT han participado en actividades de formación externa e interna, así como divulgación en temas de protección de datos.

Desde la DIT también se viene dando soporte al canal de Atención al Ciudadano con relación a las consultas de los responsables de índole técnica, en general consultas relacionadas con aspectos sobre evaluaciones de impacto, análisis de riesgos, medidas de seguridad, tecnologías, tratamientos biométricos, notificaciones de brechas, etc.

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

4. Al servicio de los ciudadanos

4.1. Adaptación de la actividad consultiva de la AEPD al RGPD: La Instrucción 1/2021 de la AEPD

La Agencia tiene encomendada entre sus funciones, la de atender a las consultas y preguntas de los ciudadanos y DPDs de la forma más eficiente y efectiva posible, conforme con el esquema de funciones establecido por el RGPD.

Las medidas que introdujo la pandemia se mantuvieron durante este año, lo que siguió condicionando el marco de la atención a los ciudadanos, de manera que aunque se reanudó la atención presencial, mediante la solicitud de cita previa, el número de personas atendidas en esta modalidad aún está lejos del registrado antes de la pandemia. También se ha constatado un descenso en el número de las consultas escritas, fruto principalmente de la revisión y actualización de su sistema de registro. Este descenso se ha visto ampliamente compensado por el incremento registrado en las consultas de las preguntas frecuentes (FAQs), que proporcionan información de elevada calidad y que se someten a un continuo proceso de revisión y actualización.

Con la finalidad de adaptar la actividad consultiva de la Agencia al esquema de funciones previsto por el RGPD para las autoridades de protección de datos, y de impulsar el principio de responsabilidad proactiva, se aprobó a finales de 2021 la Instrucción 1/2021, de 2 de noviembre, por la que se establecen directrices respecto de la función consultiva de la Agencia.

Esta Instrucción introduce cambios sustanciales en la práctica consultiva de la AEPD que tienden a hacer esta actividad más eficiente y efectiva. Se incluyen el Canal Consulta y el Canal del DPD. De una parte, el “Canal Consulta” se enfoca para informar a los ciudadanos sobre los derechos de protección de datos y, de otra, el “Canal del DPD” se centra en la atención de las consultas de éstos, convirtiendo a los DPDs en interlocutores cualificados con la Agencia, según prevé el propio RGPD. Los responsables y encargados del tratamiento, de conformidad con el principio de responsabilidad proactiva, deben encontrar el asesoramiento individualizado en sus propios DPDs y consultores especializados.

El Canal del DPD también está disponible para las organizaciones y asociaciones representativas de responsables y encargados del tratamiento que presten servicios de asesoramiento a sus miembros, en particular cuando éstos son pymes y micropymes, sobre las que la AEPD puede considerar el desarrollo de las acciones de información o difusión adecuadas a sus necesidades específicas y ayudarles a cumplir con sus obligaciones en materia de protección de datos.

4.2. Mejora de la información de consulta en la web

La adaptación al sistema consultivo fijado en el RGPD se complementa con una mejora de los materiales informativos, de consulta y de ayuda al cumplimiento de la normativa aplicable disponibles en la web. De esta forma, el conocimiento y la información sobre la protección de datos se obtiene de forma más fácil y rápida; y se hace accesible a una comunidad de visitantes de la web, mucho mayor que la de aquellos que de manera individual acuden a los canales de consulta de la AEPD, para lo que se requiere certificado electrónico.

Siguiendo esta estrategia, se acometió, en primer lugar, la reforma integral del catálogo de preguntas frecuentes (FAQs) de la web. De forma inmediata, se ha iniciado ya una mejora de la accesibilidad a las FAQs en la web, sus mecanismos de búsqueda y la reestructuración del actual catálogo de FAQs, de acuerdo con las materias más frecuentes de consulta. Esta reforma continuará en 2022 a través de un programa presentado a la Comisión Europea para su cofinanciación. La Agencia proyecta disponer de una amplia base de datos actualizada y fácil comprensión de FAQs, disponibles también en versión inglesa, que podrá ser accesible y consultada por un amplio grupo de ciudadanos de toda la UE, en la medida que estamos regulados por la misma pieza de legislación, el RGPD, y tenemos los mismos derechos.

El primer paso en esta reforma integral, que ha sido la mejora de la aplicación informática de soporte y la implantación de un motor de búsqueda por palabras, ha producido ya un aumento importante de las visitas a las FAQs y una disminución en el número de preguntas individuales recibidas. Se ha iniciado un proceso de mejora del conocimiento y, consecuentemente, del empoderamiento de los ciudadanos para ejercitar sus derechos de protección de datos, con vocación de continua mejora. Los esfuerzos a corto y medio plazo que sin duda requerirá la mejora de las FAQs redundarán a largo plazo en la consecución de los objetivos esenciales de la AEPD.

4.3. Educación y menores

En el gráfico se muestran por categorías las 1.789 consultas recibidas y tramitadas por la Unidad de Educación y Menores durante el año 2021.

El mayor número de consultas en 2021 han sido planteadas por progenitores, en concreto un 54% del total, también cabe incidir que, tomadas de manera agrupada, las consultas realizadas por responsables de empresas y organismos públicos que tratan datos de menores de edad, como pueden ser clubs deportivos o entidades locales, docentes de centros educativos, tanto de infantil, primaria, secundaria, bachiller, Universidades y alumnos, generalmente universitarios, se llega a un segundo bloque con un 25% del total de consultas recibidas y tramitadas por esta Unidad.

Destaca que la mayoría de las cuestiones planteadas han dejado de referirse a los tratamientos de datos de los alumnos para el ejercicio de la función educativa, que se lleva a cabo por los centros educativos, como pasaba el curso pasado, y se puede apreciar que la comunidad educativa ha asimilado de manera gradual la utilización de plataformas de gestión educativa y se ha acostumbrado a su utilización, tanto como base de comunicación entre familias, alumnos y docentes, como para trasladar la comunicación de las calificaciones de los alumnos a las familias. En estos colectivos se ha constatado un aumento de consultas en relación con el tratamiento de datos personales que realizaban los responsables del tratamiento y que se derivaba de la vacunación contra la COVID, tanto de los alumnos como de los docentes y personal administrativo y de servicios que presta sus servicios a los responsables.

Por otro lado, nuevamente se registra un número considerable de consultas con la utilización de la imagen de los alumnos en actividades extraescolares, o no relacionadas propiamente con la función educativa, y que los centros educativos o las empresas e instituciones quieren difundir a las familias, perfiles de Redes Sociales, aplicaciones de videoconferencia, o difundiendo el

contenido de imágenes en streaming. En estos casos, la consulta más frecuente se refiera a cómo se debe trasladar la información a las familias y a los docentes, ya que se generan dudas en cuanto a su correcto uso y a las medidas de seguridad que se deben tomar para su utilización. Con la finalidad de facilitar a las familias un instrumento para resolver sus dudas se ha elaborado una relación con los datos de contacto de los *Delegados de Protección de Datos de las Consejerías de Educación de las CCAA,* a quienes se pueden trasladar las consultas relacionadas con los tratamientos de datos personales de los centros públicos. También se ha incrementado el número de consultas de progenitores en relación con la contratación de actividades deportivas realizadas por menores en las que el responsable del tratamiento quiere difundir imágenes de los menores.

Destaca el aumento significativo del número de consultas de ciudadanos en las que se solicita información para interponer una reclamación ante la AEPD por presunta vulneración de la normativa de protección de datos, superando el 15% del total de consultas recibidas. A este respecto, se ha tratado de informar convenientemente a los consultantes sobre la cuestión planteada, ya que en numerosas ocasiones no se corresponde con situaciones en que se vayan a admitir reclamaciones ante la Agencia, sino que son tratamientos de datos personales cuya legitimación está amparada, en la mayoría de los casos, por alguna norma legal o por un contrato firmado por los progenitores y, por tanto, la causa de la legitimación no es el consentimiento de los interesados o de sus padres o tutores legales. Como ejemplos, se pueden citar la publicación en las webs de centros educativos de los listados de alumnos admitidos o excluidos, o la comunicación de datos de alumnos por parte de centros educativos a empresas externas que van a desarrollar clases extraescolares.

La Unidad de Educación y Menores recibe consultas tanto a través de la *Sede electrónica* de la AEPD y de la dirección electrónica del *Canal joven*, como por canales específicos de consulta a disposición de la ciudadanía, en este caso por WhatsApp y teléfono que, en su conjunto, han experimentado un incremento de un 28,5% frente a las consultas recibidas en 2020 y de un 19% frente a las de 2019.

Así mismo y como viene ocurriendo en estos últimos años, hay que indicar que desde el Canal Prioritario de la AEPD, en su apartado específico para menores (14 a18 años), se han derivado a la Unidad de Educación y Menores, un total de 44 reclamaciones, en las que se solicitaba la retirada de contenido sensible publicado en internet, pero que *no cumplían los requisitos de admisión establecidos en este Canal*, así se han podido articular como consultas e informar a los ciudadanos en 28 casos, el resto fueron objeto de archivo, pues, entre otras cuestiones, no se facilitaron datos de contacto suficientes para poder ofrecer una contestación.

Acciones dirigidas a la formación y sensibilización en el entorno educativo y de menores

Jornada sobre Protección de datos y adicciones tecnológicas

24 de marzo

El 24 de marzo, se organizó conjuntamente con la Delegación del Gobierno para el Plan Nacional sobre Drogas y la colaboración del Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF), la Dirección General de Bilingüismo y Calidad de la Enseñanza de la Consejería de Educación y Juventud de la Comunidad de Madrid y el INJUVE, una jornada online y en streaming para afrontar desde una perspectiva multidisciplinar la cuestión de la adicción a las tecnologías y sus consecuencias, y plantear un marco de actuación conjunta e intentar facilitar a los implicados, ya sean jóvenes, padres, profesores y otros colectivos que participen en la vida de los menores, una información general sobre la materia.

La jornada contó con la participación de expertos y de organizaciones involucradas en el bienestar del menor con ANAR, la CEAP y la Cruz Roja Juventud.

Curso NOOC, Menores y seguridad en la Red, 2ª edición
del 14 al 23 de marzo

En colaboración con el Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF), del 14 al 23 de marzo se ha desarrollado en la plataforma educativa online del INTEF la *segunda edición del curso Menores y seguridad en la Red* (NOOC -Nano Open Online Course-) dirigido a la comunidad educativa, especialmente a los padres, a las familias y a los docentes, tutores y equipos directivos de centros educativos. El NOOC contó con un total de 1.580 alumnos inscritos, de los cuales el 37.5% han sido docentes y el 62.5% no docentes, muestra del interés que tienen las familias por la protección de datos y la seguridad de los menores en Internet y Redes Sociales.

Curso Tutorizado sobre Protección de Datos, privacidad y derechos digitales en los centros educativos, desarrollado por INTEF y en que colabora la AEPD.

Siguiendo con la colaboración que se viene manteniendo con el INTEF, del 14 de septiembre al 16 de noviembre, se ha desarrollado la segunda edición del curso *Protección de Datos, privacidad y derechos digitales en los centros educativos*, dirigido al profesorado y a los equipos directivos de los centros educativos.

Campaña de difusión de las iniciativas 'Lo paras o lo pasas' y 'Las redes soiales no son un juego'

Se ha difundido a los centros educativos de secundaria, bachiller y formación profesional, tanto públicos como privados del territorio nacional, las campañas *'Lo paras o lo pasas'* y *'Las redes sociales no son un juego',* para dar a conocer a la comunidad educativa las consecuencias de la difusión irresponsable de información sensible a través de Internet, y el *Canal prioritario* de la Agencia para poder solicitar la retirada de fotografías, vídeos o audios de contenido sexual o violento en Internet sin el consentimiento de las personas que aparecen en las imágenes publicadas.

Premio a las Buenas Prácticas Educativas en Privacidad y Protección de Datos Personales para un Uso Seguro de Internet por los Menores 2021

Se convocó y difundió entre los centros educativos, tanto públicos como privados del territorio nacional, la nueva edición del *Premio a las Buenas Prácticas Educativas* en Privacidad y Protección de Datos Personales para un Uso Seguro de Internet por los Menores, que premia a los centros educativos por los proyectos que hayan desarrollado para concienciar y fomentar el buen uso de Internet y a las personas y entidades que se hayan destacado por la labor en este ámbito.

Infografías

En este ámbito de actuación se han elaborado las siguientes infografías con la finalidad de dar conocer aquellos aspectos que más se demandan en el ámbito del tratamiento de datos de menores:

- **Quién es quién en los centros educativos,** para ayudar a entender los *distintos roles que se establecen en un centro educativo* en relación con los tratamientos de datos personales tanto de alumnos, familias y docentes.
- **Información sobre consentimiento para tratar datos personales de menores de edad,** *sobre recogida del consentimiento para el tratamiento de datos personales de menores de edad.*
- **Cuáles son tus derechos de protección de datos,** *sobre derechos reconocidos en la normativa de protección de datos.*

4.4. Comunicación

En el gráfico se muestran por categorías las 1.789 consultas recibidas y tramitadas por la Unidad de Educación y Menores durante el año 2021.

4.4.1. Redes Sociales

La AEPD lanzó el 28 de enero de 2018 *su cuenta oficial en Twitter*, cumpliendo así con su objetivo de estar presente en el entorno de las redes sociales para difundir las iniciativas puestas en práctica y que los ciudadanos interesados puedan conocerlas de forma directa.

Al finalizar 2021, la cuenta de Twitter de la AEPD contaba con casi 33.000 seguidores, con una media de 136 seguidores nuevos a la semana. Durante 2021 se publicaron en el perfil más de 1.000 tuits, registrando más de 13.000 menciones y 3,7 millones de impresiones.

Con este canal de comunicación, la Agencia persigue varios objetivos: dar a conocer la labor que desempeña la AEPD, promoviendo la sensibilización entre los ciudadanos en relación con la protección de sus datos, y difundir las guías, materiales y herramientas de cumplimiento que la Agencia pone a disposición de los profesionales, las empresas y las administraciones públicas. Por otra parte, esta cuenta representa un instrumento esencial para conocer cuáles son las inquietudes en esta materia por parte de los diferentes colectivos, tanto de quienes tratan datos como de aquellas personas cuyos datos son objeto de tratamiento.

Las publicaciones más destacadas en Twitter en 2021 están relacionadas con la entrega de los Premios Protección de Datos; el curso online gratuito 'Menores y Seguridad en Red, organizado por la Agencia y el Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado; el uso del certificado de vacunación para acceder a establecimientos; y el lanzamiento del Pacto Digital para la Protección de las Personas.

4.4.2. 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 2021 el blog de la Agencia ha recibido más de 340.000 visitas únicas, frente a las 223.000 de 2020. Entre los posts que han despertado un mayor interés se encuentran los relacionados con las *Brechas de seguridad de datos personales: qué son y como actuar; Elaborar el registro de actividades de tratamiento, IoT (III) Domótica. Internet de las Cosas: riesgos y recomendaciones, IoT (II): Del Internet de las Cosas al Internet de los Cuerpos y Privacidad en reuniones online.*

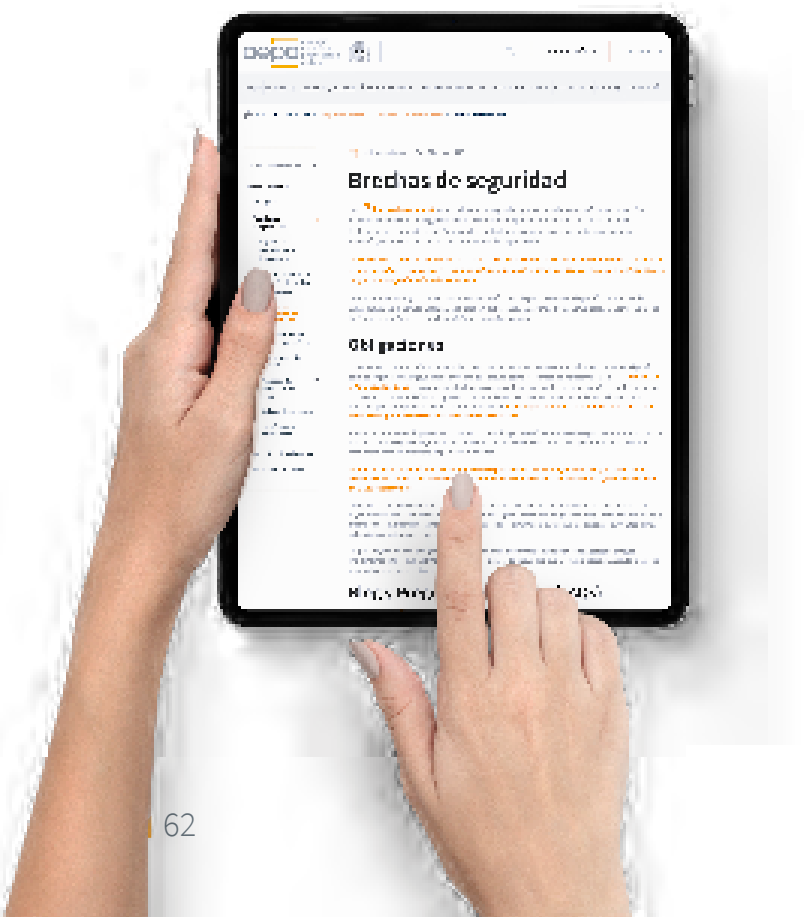
4.4.3. Canal de Yotube

Durante 2021 el Canal de YouTube de la Agencia albergó 37 nuevos vídeos. En cuanto a los resultados obtenidos, el año se cerró superando los 4.500 suscriptores en el canal de YouTube de la Agencia, obteniendo casi 140.000 visualizaciones y más de 6.000 horas de visualización. Esta cifra supone un incremento de suscriptores de un 28% respecto a 2020. 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.

La Agencia Española de Protección de Datos (AEPD) renovó en marzo de 2021 *su catálogo de vídeos en los que ayuda a configurar las opciones de privacidad y seguridad* de los principales sistemas operativos, navegadores web, redes sociales y aplicaciones más utilizadas (sistemas operativos Android e iOS; el navegador web Firefox; las redes sociales Facebook, Instagram y Twitter; la aplicación de mensajería instantánea WhatsApp; los navegadores Chrome y Edge; la aplicación de mensajería instantánea Telegram y la red social Tik Tok).

Los vídeos se inician con una breve introducción explicando qué es y para qué se utiliza cada servicio. A continuación, realizan un detallado repaso 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.

Estos vídeos han recibido casi 17.000 de visualizaciones, acumulando más de 700 horas de visualizaciones



4.4.4. Espacio 'Protegemos tu privacidad' de Radio 5

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 166 piezas temáticas, en las que un experto de la Agencia o la propia conductora del programa ofrece consejos y recomendaciones. De ellas, 47 corresponden al año 2021.

4.4.5. Relaciones con los medios

Los medios de comunicación tienen una gran importancia en lo que a protección de datos se refiere tanto por su contribución 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 2021, la Agencia atendió casi 600 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 más de 700.000 visitas únicas.

Las cinco notas de prensa más consultadas de 2021 han sido las siguientes:

- *La AEPD publica una guía sobre protección de datos y relaciones laborales*
- *'Lo paras o lo pasas', iniciativa para fomentar el uso del Canal Prioritario*
- *La AEPD actualiza su Guía sobre el uso de cookies con las nuevas directrices del Comité Europeo de Protección de Datos*
- *Comunicado de la AEPD en relación con la toma de temperatura por parte de comercios, centros de trabajo y otros establecimientos*
- *La AEPD lanza un Pacto Digital con el respaldo de las principales organizaciones empresariales, fundaciones, asociaciones de medios y grupos audiovisuales*

Asimismo, en relación con notas de agenda informativa publicadas en la web, la Agencia publicó en 2021 más de 80 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 la redacción de las notas de prensa de las reuniones plenarias que periódicamente celebra el Comité Europeo de Protección de Datos (CEPD).

4.5. Agenda institucional

Durante 2021, la Agencia participó en numerosas reuniones, jornadas, foros, congresos, seminarios web, actos y presentaciones, en calidad de organizadora o invitada. El objetivo de la Agencia en estos actos es fomentar una cultura de protección de datos entre ciudadanos y organizaciones, así como continuar siendo un punto de referencia para el análisis de las implicaciones de la normativa de protección de datos en la actividad de distintos ámbitos. Además, la Agencia ha incrementado desarrollando iniciativas para visibilizar su *Canal prioritario* para solicitar la retirada de contenidos de carácter sexual o violento que se publican en internet sin el consentimiento de las personas afectadas. De nuevo, muchos de estos actos y webinarios han seguido celebrándose en formato digital como consecuencia de la Covid-19. La relación completa de la agenda institucional de la AEPD puede consultarse en la siguiente *sección web.*

Dentro del ámbito del sector público, la AEPD ha participado diversas jornadas, seminarios, reuniones y conferencias, como el Día de Internet Segura 2021 'Una Internet mejor comienza contigo: más conectados, más seguros', un evento promovido por la red INSAFE/INHOPE con el apoyo de la Comisión Europea y organizado por el INCIBE; la jornada digital sobre adicciones tecnológicas organizada junto con la Delegación del Gobierno para el Plan Nacional sobre Drogas, en colaboración con la Consejería de Educación y Juventud de la Comunidad de Madrid, el Instituto Nacional de Tecnologías Educativas y Formación del Profesorado (INTEF) y el INJUVE; o el webinario 'Los riesgos derivados de las nuevas tecnologías y el acoso', dirigido a la Carrera Fiscal y enmarcado en el espacio 'Viernes formativos de la Fiscalía General del Estado'.

Además, la AEPD ha participado en la conferencia 'Acceso a nuevas fuentes de datos con fines estadísticos', organizada por el Instituto Nacional de Estadística; el curso de Verano de la Universidad de Málaga 'El Reglamento General de Protección de Datos: tres años de aplicación'; la VI edición del Congreso Internacional de Transparencia; la Jornada de formación "La Violencia de Género a través de las Redes Sociales" organizada por el Ayuntamiento de Almuñécar, el Centro de Municipal de Información a la Mujer y la Subdelegación del Gobierno de Granada; el VII Curso sobre Igualdad de Género, organizado por el área de Derechos Humanos e Igualdad de la Policía Nacional; la Jornada: 'Ciber-violencia sobre mujeres y niñas', organizada por la Subdelegación del Gobierno en Almería; la Jornada 'La violencia de género. Derechos y recursos', organizada por la Unidad contra la Violencia sobre la Mujer de la subdelegación del Gobierno de España en Granada en colaboración con Granada la Unidad de Igualdad y Conciliación de la Universidad de Granada; la Jornada informativa 'Ciberviolencia de género', organizada por la Mancomunidad Río Monachil de Granada o el Pleno del Consejo

para la Eliminación de la Discriminación Racial o Étnica, organizado por el Ministerio de Igualdad.

En el plano del sector privado, la AEPD ha participado en diferentes jornadas, foros, congresos, debates, conferencias, desayunos de redacción y webinarios a lo largo de 2021, como la jornada dedicada a la privacidad de los datos aplicados al marketing business to business, organizada por la Asociación de Marketing de España (MKT) y la Federación de Empresas de Publicidad y Comunicación (FEDE); *el XIII Foro de la Privacidad ISMS Forum;* el I Congreso de la Infancia y Adolescencia, organizado por los Ilustres Colegios de Abogados de Madrid y Barcelona y la Plataforma Familia y Derecho; el Congreso Internacional de Derecho Digital de Enatic; el primer debate de la Asociación Madrileña de la Abogacía de Familia e Infancia (AMAFI); la XIV Conferencia Anual de las Plataformas Tecnológicas de la Investigación Biomédica y el XVIII Foro de Seguridad y Protección de Datos de Salud organizado por SEIS.

Asimismo, la AEPD ha participado en el webinario de AMETIC, Adigital y CEOE 'Impacto en la economía española, visión empresarial'; las II Jornadas Contra el Maltrato 'Tolerancia Cero', organizadas por la Fundación Mutua Madrileña y Antena 3 Noticias; las Jornadas sobre Ciberseguridad 'Seguridad de cuentas y privacidad'; el Encuentro gallego de ciberseguridad CIBER.gal; la XXIII Jornada Internacional de Seguridad de la Información, organizada por ISMS Forum o el desayuno de redacción 'El factor humano en la ciberseguridad: formación y talento para protegerse de un mundo conectado', organizado por Cinco Días en colaboración con Abanca.

Dentro de este ámbito, la AEPD ha mantenido reuniones de trabajo con la Confederación Española de Organizaciones Empresariales (CEOE) o el Instituto de Contabilidad y Auditoría de Cuentas (ICAC) y se ha reunido con representantes de empresas como Google o Vodafone.

Además, ha mantenido reuniones de carácter institucional con representantes de departamentos ministeriales, como la celebrada con la secretaria de Estado de Presupuestos y Gastos del Ministerio de Hacienda y Función Pública, María José Gualda Romero, y con el subsecretario de Justicia, José Miguel Bueno Sánchez o la celebrada con el director general de Transformación Digital de la Administración de Justicia, Aitor Cubo. Asimismo, la Agencia ha celebrado un Seminario de Coordinación de Autoridades junto a la Autoridad Catalana de Protección de Datos, la Agencia Vasca de Protección de Datos y el Consejo de Transparencia y Protección de Datos de Andalucía, en el marco de cooperación institucional entre la AEPD y las autoridades autonómicas de protección de datos.

La Agencia también ha participado en dos reuniones como parte del Grupo de Trabajo de Adicciones a las Nuevas Tecnologías junto con representantes de la Delegación del Gobierno para el Plan Nacional sobre Drogas, el Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado, el Instituto de la Juventud y la Consejería de Educación y Juventud de la Comunidad de Madrid. Igualmente, ha mantenido reuniones con representantes de asociaciones, como la Asociación de Editores de Libros y Contenidos Educativos (ANELE) y la Asociación Española de Fundraising.

En este ámbito, la Agencia ha participado en la Sesión online organizada por la Asociación Profesional Española de Privacidad (APEP) sobre el Día Europeo de Protección de Datos; en el del foro de los Delegados de Protección de Datos de la European Banking Federation (EBF DPO Forum); en el Séptimo Congreso Internacional de Responsabilidad Social, organizado por el Foro ResponsabilizaRSe; en el coloquio organizado por la Asociación de Diplomados en Altos Estudios de la Defensa Nacional (ADALEDE); la jornada digital organizada por la Asociación de Directivos y Profesionales de Relaciones Laborales (ADIRELAB) para presentar la *Guía de Relaciones Laborales de la AEPD* y la Jornada Ciudadanía Conectada sobre 'Derechos de la infancia y mediación parental en el contexto digital', organizada por Pantallas Amigas.

La AEPD también ha participado en diversos actos enfocados a fomentar el conocimiento de

la normativa de protección de datos, así como a facilitar el uso de herramientas desarrolladas por la Agencia. Así, destaca la jornada 'Recursos y herramientas de la AEPD', dirigida a fundaciones y entidades del Tercer Sector. En el mes de junio, la AEPD presentó la *'Gestión del riesgo y evaluación de impacto en tratamientos de datos personales',* en un acto en el que también dio a conocer *EVALÚA_RIESGO RGPD*, el prototipo de una herramienta que ayuda a identificar factores de riesgo de los tratamientos de datos personales. Además, la AEPD organizó y celebró el seminario 'Privacidad, sostenibilidad e innovación', enmarcado en las Actividades de Verano 2021 de la Universidad Internacional Menéndez Pelayo (UIMP) de Santander.
Por otra parte, la Agencia ha organizado y celebrado un nuevo ciclo de debates digitales para analizar diversos aspectos relacionados con la innovación y la protección de datos desde la perspectiva de la mujer en el campo de la ciencia y la tecnología, que se detallan en otro apartado de esta Memoria.

En el ámbito internacional, la Agencia ha seguido participando en las reuniones digitales plenarias y los Subgrupos del Comité Europeo de Protección de Datos (CEPD) y ha intervenido en eventos y mantenido encuentros y reuniones como la celebrada como parte del Grupo Permanente de Autoridades Nacionales de Protección de Datos de la Red Iberoamericana de Protección de Datos (RIPD); el webinario 'Estrategias de las Autoridades de Protección de Datos para luchar contra la violencia digital en Iberoamérica con un enfoque de género' de la RIPD; la reunión digital con el viceministro de Tecnologías de la Información y Comunicación de Ecuador, Félix Chang Calvache; la reunión digital del Comité Ejecutivo de la Red Iberoamericana de Protección de Datos (RIPD); el VIII Congreso Internacional de Protección de Datos Personales, organizado por la Superintendencia de Industria y Comercio (SIC) de Colombia y la Red Iberoamericana de Protección de Datos Personales; la Jornada de Seminarios Especializados en materia de Protección de Datos personales en la Ciudad de México 2021, organizada por el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (INFO CDMX); el Comité Ejecutivo de la Red Iberoamericana de Protección de Datos (RIPD); la 43ª Global Privacy Assembly, organizada por el Instituto Nacional de Trasparencia, Acceso a la Información y Protección de Datos Personales (INAI); la reunión de trabajo con una delegación del Senado de Chile, compuesta por su presidenta, Ximena Rincón, y otros miembros de dicha Cámara; el XIX Encuentro de la Red Iberoamericana de Protección de Datos Personales (RIPD) y la visita institucional del consejero del Consejo para la Transparencia de Chile, Bernardo Navarrete Yáñez.

Asimismo, la AEPD y la Autoridad Nacional de Protección de Datos de Brasil (ANPD) han suscrito un memorándum de entendimiento en el marco de un proyecto de cooperación mutua para desarrollar iniciativas dirigidas a promover la difusión del derecho a la protección de datos de carácter personal y crear un espacio de intercambio de conocimientos y mejores prácticas que permitan fortalecer las capacidades técnicas de ambas partes relacionadas con la aplicación de la normativa de protección de datos personales.

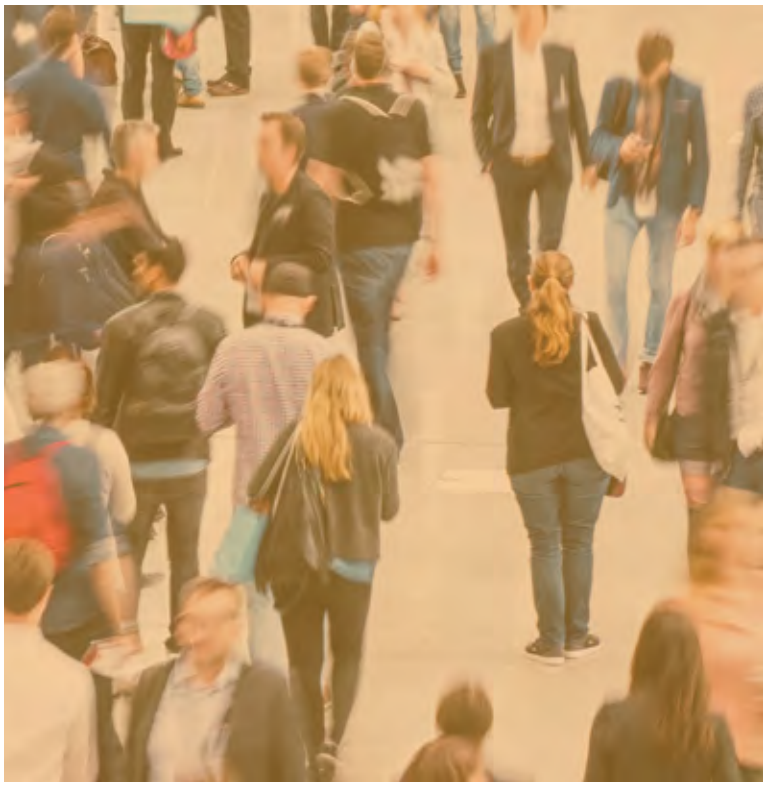
Por otra parte, la AEPD ha continuado desarrollando iniciativas para dotar de mayor visibilidad a su Canal Prioritario. En este sentido, ha acogido el 'I Foro Privacidad, Innovación y Sostenibilidad' con motivo del Día internacional de la Protección de Datos, donde se presentó públicamente el *Pacto Digital para la Protección de las Personas,* una iniciativa de la Agencia que promueve un gran acuerdo por la convivencia en el ámbito digital con el doble objetivo de fomentar el compromiso con la privacidad en los modelos de negocio de empresas y organizaciones, y de concienciar a los ciudadanos de las consecuencias de difundir contenidos sensibles en internet. Meses después, la Agencia celebró tres reuniones de seguimiento de este pacto, en la que participaron organizaciones empresariales; fundaciones y asociaciones, y asociaciones de medios y grupos audiovisuales adheridos inicialmente a la iniciativa, al objeto de compartir información acerca del estado del Pacto Digital y las acciones desarrolladas por las entidades adheridas para la difusión del mismo.

La Agencia también se reunió con representantes de Facebook para analizar el funcionamiento y la respuesta al envío de medidas cautelares derivadas del Canal prioritario, así como con representantes de Tik Tok con el fin de informar acerca del Canal prioritario de la Agencia.

Asimismo, ha impulsado un Grupo de Trabajo para la adopción de medidas de protección a los menores que eviten el acceso a páginas web de contenido para adultos. En la reunión participaron representantes del Ministerio del Interior (Secretaría de Estado de Seguridad), Ministerio de Educación y Formación Profesional, la Dirección General de Telecomunicaciones y Ordenación de los Servicios de Comunicación Audiovisual del Ministerio de Asuntos Económicos y Transformación Digital, INJUVE, INCIBE y la Fiscalía de Delitos Telemáticos.

Por otra parte, ha mantenido una reunión con representantes del Instituto Andaluz de la Mujer (IAM), en el marco de la Comisión de Seguimiento del Protocolo General de Actuación suscrito en 2020 entre la Agencia y el Instituto, con el fin de colaborar en la atención de las mujeres cuyos datos se han obtenido y difundido de forma ilegítima, especialmente en el caso de imágenes, vídeos o audios de contenido sensible. Asimismo, ha participado en una reunión digital con representantes del Consejo Audiovisual de Andalucía, con el objetivo de intercambiar información e iniciativas orientadas a la protección de los menores en relación con el acceso a contenidos audiovisuales que perjudiquen su desarrollo físico, mental y moral, y en concreto, a contenidos pornográficos.

La Agencia también ha celebrado reuniones dirigidas a la búsqueda de vías de colaboración con entidades como la Fundación 29 de Febrero y el Instituto de las Mujeres.
Dentro del capítulo de comparecencias oficiales, la directora de la AEPD, Mar España, compareció ante la Comisión para la auditoría de la calidad democrática, la lucha contra la corrupción y las reformas institucionales y legales del Congreso de los Diputados, con el objetivo de realizar un análisis de las medidas necesarias para reforzar



la imparcialidad e independencia de autoridades independientes y organismos de regulación; ante la Comisión de Asuntos Económicos y Transición Digital del Senado, para explicar el Pacto Digital para la Protección de las Personas, así como ante la Comisión Constitucional del Congreso de los Diputados, para presentar la Memoria de la Agencia correspondiente a 2020.

Igualmente, cabe mencionar la firma entre la directora de la AEPD y la presidenta de Women in a Legal World, Marlen Estévez, de un protocolo general de actuación para la promoción de la presencia femenina en materia de tecnología y privacidad, así como la reunión con la directora de la Oficina del Alto Comisionado para la Pobreza Infantil del Gobierno de España, Carmen Gayo.
Finalmente, el Consejo Consultivo de la Agencia de Protección de Datos -órgano colegiado de asesoramiento a la dirección de la Agencia – mantuvo reuniones digitales el 1 de julio y el 17 de diciembre de 2021 para exponer y analizar la actividad de la institución.

4.6. Infografías

La AEPD publicó en 2021 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 este sentido, se han publicado las siguientes infografías:

- *Riesgos de internet de las cosas en el hogar y recomendaciones para el uso seguro de internet de las cosas.*
- *Quién es quién en el tratamiento de datos personales en tu centro educativo*
- *Cuáles son tus derechos de protección de datos*
- *Las redes sociales no son un juego*
- *Lo paras o lo pasas*
- *Un solo clic puede arruinarte la vida*

4.7. Actividades de divulgación

4.7.1. Actividades de divulgación

La AEPD continuó en 2021 con su compromiso de fomentar la cultura de protección de datos entre los ciudadanos y organizaciones a través de diferentes acciones de divulgación. La presencia física de los medios de comunicación a los actos que se recogen a continuación tuvo que reducirse como parte de las medidas de control de la COVID-19, si bien se optó por una invitación para seguirlo en streaming cuando fue posible.

Presentación del Foro Privacidad, Innovación y Sostenibilidad
28 de enero

Con motivo del Día Internacional de Protección de Datos el 28 de enero, la AEPD celebró el I Foro de Privacidad, Innovación y Sostenibilidad, un acto retransmitido en streaming en el que presentó el Pacto Digital para la Protección de las Personas, un proyecto que promueve un gran acuerdo por la convivencia ciudadana en el ámbito digital y que se lanzó con la colaboración de las principales organizaciones empresariales, fundaciones, asociaciones de medios de comunicación y grupos audiovisuales, que ya se han adherido al mismo.
El acto fue inaugurado por el Ministro de Justicia, Juan Carlos Campo, y la clausura corrió a cargo de la Fiscal General del Estado, Dolores Delgado. Asimismo, tras la presentación del Pacto por parte de la Directora de la AEPD, Mar España, y la intervención de Itziar de Lecuona, de la Cátedra UNESCO de Bioética, se celebraron dos mesas redondas.

En la primera de ellas, centrada en el sector empresarial, participó el vicepresidente de CEOE, Miguel Garrido; el presidente de CEPYME, Gerardo Cuerva; el presidente del Círculo de Empresarios, John de Zulueta; el presidente de la Cámara de España, José Luís Bonet; el presidente de la Asociación Española de Fundaciones, Javier Nadal; y el presidente de la Plataforma del Tercer Sector y de la Plataforma del Voluntariado, Luciano Poyato.

La segunda de las mesas, que analizó el papel de los medios de comunicación en la prevención de la violencia digital, contó con la participación del Presidente de la Federación de Asociaciones de Periodistas de España, Nemesio Rodríguez; el Presidente de la Asociación de Medios de Información, Antonio Fernández-Galiano; el Presidente del Club Abierto de Editores, Arsenio Escolar; el Director de Asuntos Regulatorios y Asuntos Institucionales de Atresmedia, Miguel Langle; el Director General Corporativo de Mediaset, Mario Rodríguez, y la directora de protección de datos y privacidad de la Corporación RTVE, Cristina Hernández.

Jornada digital sobre adicciones tecnológicas

24 de marzo

En el marco de los compromisos en materia de Responsabilidad Social y Sostenibilidad, especialmente en el ámbito de las actuaciones orientadas a los menores y al ámbito educativo, la Agencia Española de Protección de Datos y la Delegación del Gobierno para el Plan Nacional sobre Drogas, en colaboración con la Consejería de Educación y Juventud de la Comunidad de Madrid, el Instituto Nacional de Tecnologías Educativas y Formación del Profesorado y el INJUVE, organizaron una jornada digital sobre adicciones tecnológicas con el objetivo de fomentar entre los niños y jóvenes un uso responsable de las TIC, dar visibilidad a las consecuencias que este tipo de adicciones produce en los ámbitos escolar, familiar y social, y abrir un debate sobre la prevención, detección y recursos disponibles.

La jornada fue inaugurada por el delegado del Gobierno para el Plan Nacional sobre Drogas, Joan Villalbí, y contó con la participación del profesor de la Universidad de Santiago de Compostela, Antonio Rial Boubeta, que ofreció una ponencia sobre la 'Tecnología y nuevas adicciones en la infancia y la adolescencia (salud, convivencia y responsabilidad social)'.

Asimismo, se abordaron las 'Adicciones tecnológicas en el ámbito familiar y escolar' en una mesa redonda que contó con representantes de la Viceconsejería de Organización Educativa de la Comunidad de Madrid; la Universidad de Deusto; la Fundación ANAR; el área de Salud de Cruz Roja juventud y CEAPA, bajo la moderación del subdirector del Registro General de la AEPD, Julián Prieto Hergueta. Finalmente, la jornada fue clausurada por la directora de la Agencia de Protección de Datos, Mar España.

Entrega de los Premios Protección de Datos

7 de abril

La Agencia celebró el acto de entrega de los 'Premios Protección de Datos 2020' en las categorías de Comunicación, Investigación, Proactividad y buenas prácticas en el cumplimiento del Reglamento y la LOPDGDD, Buenas prácticas educativas y Buenas prácticas de protección en internet de la privacidad de las mujeres víctimas de violencia por razón de género. 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. Las iniciativas premiadas se recogen con detalle en un apartado posterior.

Seminario de la UIMP 'Privacidad, Sostenibilidad e Innovación'

7, 8 y 9 de julio

La Agencia impartió del 7 al 9 de julio el seminario 'Privacidad, Sostenibilidad e Innovación', enmarcado en las Actividades de Verano 2021 de la Universidad Internacional Menéndez Pelayo (UIMP) de Santander. El curso analizó la aplicación práctica del modelo de cumplimiento y supervisión del RGPD, y las importantes novedades en las bases jurídicas del tratamiento de datos, especialmente respecto del consentimiento y el interés legítimo; en la tramitación de reclamaciones, así como en la promoción de sistemas de autorregulación a través de códigos de conducta. Y también en la aplicación del Reglamento a nuevas tecnologías, como la inteligencia artificial, el big data, las redes 5G, el internet de las cosas o el blockchain. Ello ha exigido una respuesta que garantice una aplicación coherente de la norma en el ámbito de la Unión por parte del Comité Europeo de Protección de Datos.

Asimismo, se abordó la sentencia del Tribunal de Justicia de la Unión Europea sobre el denominado caso Schrems 2, así como la interrelación entre el Reglamento y la normativa reguladora de la publicidad online y de las cookies y otras

tecnologías similares serán temas que también se tratarán durante el seminario.
En el ámbito de la pandemia de COVID-19, también se trataron las iniciativas relacionadas con la emisión de certificados interoperables para garantizar la libre circulación dentro de la Unión Europea, la finalidad de dichos tratamientos a nivel europeo y sus posibles usos secundarios por parte de los Estados miembros.

4.7.2. Campañas de difusión

'Un solo clic puede arruinarte la vida' - Canal prioritario

Para continuar con la difusión del *Canal Prioritario*, el 28 de enero de este año la Agencia presentó la campaña *'Un solo clic puede arruinarte la vida'* dentro del Pacto Digital para la Protección de las Personas. Esa campaña fue declarada de servicio público por la CNMC y está dirigida a concienciar de los riesgos de reenviar o difundir contenidos sensibles, como fotografías o vídeos de carácter sexual o violento. Más del 90% de la población de 16 a 74 años utiliza Internet de manera frecuente y casi el 65% de ellos interactúa en redes sociales como Instagram, Facebook, Twitter o YouTube, según datos del Instituto Nacional de Estadística. De entre esos miles de clics que permiten la comunicación, informarse o estar en contacto con amigos o familiares, la campaña pone el foco en un clic que tiene consecuencias mucho más graves que el resto, un reenvío de contenidos sensibles sin el permiso de las personas cuya imagen, voz u otros datos personales aparecen en ellos; un clic que, con la intención de hacer daño o por desconocimiento, contribuye a la difusión de contenidos sexuales, violentos o de ciberacoso.

Para llevar a cabo la promoción de esta campaña se contó con el apoyo de todas las entidades adscritas al Pacto Digital, haciendo referencia especial por su difusión a la campaña llevada a cabo por las tres principales cadenas de televisión en España: Atresmedia, Mediaset y RTVE, cuya emisión se realizó de forma gratuita. Como ejemplos del importante impacto que ha tenido esta campaña se puede citar la emisión del

vídeo-spot en televisión por parte de las cadenas de ámbito nacional anteriormente mencionadas (exento de cómputo publicitario pues se trata de un anuncio en el que puede apreciarse características y valores de interés público y que, a su vez, carece de valor comercial) del 28 de enero a 7 de febrero, y obtuvo más de 63 millones de impactos.

Campaña con el Instituto Andaluz de la Mujer

El Instituto Andaluz de la Mujer (IAM) en colaboración con la AEPD lanzaron el 26 de enero la campaña contra la ciberviolencia de género #PuedesPararlo con el objetivo de dar a conocer el Canal Prioritario. El lanzamiento de esta campaña, cuya cartelería y pegatinas se difundieron a través de los cerca de 800 entes municipales de Andalucía, es una de las acciones que se derivan del protocolo general de actuación entre la Agencia Española de Protección de Datos y el Instituto Andaluz de la Mujer. Este protocolo surgió con el fin de articular la colaboración entre ambas instituciones para la mejora de la atención a las mujeres cuyos datos se hayan obtenido y difundido ilegítimamente a través de internet, en particular imágenes, vídeos o audio con datos sensibles.

El Instituto Andaluz de la Mujer imprimió 40.000 carteles y 30.000 pegatinas que repartieron entre los 785 ayuntamientos de Andalucía y los Centros Provinciales de la Mujer, con el objetivo de llegar a los puntos de interés como los Centros Municipales de Información a la Mujer, los centros educativos, los centros de salud, las dependencias municipales o los mercados.

Consejos y recomendaciones a menores - Clan TV

Con motivo de la celebración del Día internacional de Protección de Datos, el canal de televisión Clan TV, de RTVE, volvió a emitir los vídeos realizados junto con la Agencia para difundir entre los menores el valor de la privacidad en Internet y la importancia de luchar contra el ciberacoso. La campaña cuenta con seis vídeos editados a partir de materiales de la AEPD disponibles en la web Tudecideseninternet.es y en ellos se abordan cuestiones como el ciberacoso, la dependencia tecnológica o la huella digital, ofreciendo consejos y recomendaciones.

'Lo paras o los pasas'

La campaña 'Lo paras o lo pasas', lanzada a mediados de abril, continuó con las acciones de difusión del Canal Prioritario. Con esta iniciativa la Agencia se dirige a todas las personas que en algún momento pueden ver publicado un contenido de este tipo, aunque inicialmente no lo grabasen ellos. Al ver ese vídeo o fotografía cada persona debe decidir qué hacer: si se convierte en cómplice o si va a actuar para parar la cadena. El objetivo es transmitir que cualquiera puede denunciar ante la Agencia la publicación de ese tipo de contenidos en páginas web y que no sólo tiene una responsabilidad la persona que inicialmente decide publicar un contenido de carácter sexual o violento sin el permiso de la persona que aparece en las imágenes sino todos aquellos que contribuyen a su difusión a través de diferentes vías. En el caso de que las imágenes sensibles se hayan subido a alguna red social o estén públicamente accesibles en un sitio web, los ciudadanos pueden acudir al canal.

Para ampliar la difusión de #LoParasOLoPasas la Agencia Española de Protección de Datos contó con la colaboración de la actriz Ana Milán, que planteó en sus redes sociales qué harían sus seguidores si ven publicado un vídeo de carácter sexual grabado sin el consentimiento de la mujer que aparece en el mismo. Con más de dos millones y medio de impresiones y más de medio millón de interacciones, esta campaña se ha convertido en la acción más viral que ha realizado la Agencia hasta el momento, siempre con el objetivo de acercarse al terreno en el que los jóvenes son más activos, el de las redes sociales.

Además, los carteles que conforman la iniciativa se han remitido a todos los institutos, así como a los Consejeros de Educación de las Comunidades Autónomas.

'Las redes sociales no son un juego'

La Agencia lanzó a primeros de septiembre la iniciativa *'Las redes sociales no son un juego – Si compartes contenido sexual o violento perdemos todos'* para poner el foco en la publicación en redes sociales de este tipo de contenidos y transmitir que todas las personas pueden denunciar en el Canal prioritario su publicación. Esta campaña se llevó a cabo a través de las redes sociales, contando con el apoyo para difundirla de las entidades adheridas al Pacto Digital. Asimismo, el cartel realizado también se envió a los centros educativos.

4.7.3. Premios

Premios concedidos por la AEPD

La Agencia entregó el 7 de abril de 2021 los 'Premios Protección de Datos 2020' en las categorías de Comunicación, Investigación, Proactividad y buenas prácticas en el cumplimiento del Reglamento y la LOPDGDD, Buenas prácticas educativas y Buenas prácticas de protección en internet de la privacidad de las mujeres víctimas de violencia por razón de género.

En la categoría de Comunicación, la AEPD entregó el premio principal a la periodista Begoña

Vázquez de la Paz, del programa ‘La Aventura del Saber’ de Televisión Española, por su reportaje ‘Seguridad en el mundo digital’, dedicado al *Canal Prioritario* de la AEPD y la *página ‘AseguraTic,’* y en el que se ofrecen claves para el uso responsable de las nuevas tecnologías y se explican los riesgos derivados de un mal uso de internet, especialmente para los más jóvenes. Asimismo, el jurado concedió el accésit a Maldita.es por el proyecto ‘Maldita Tecnología’, en el que se abordan cuestiones sobre privacidad, uso de datos, ética de la tecnología y derechos digitales.

En la categoría de ‘Investigación en protección de datos personales Emilio Aced’ el jurado concedió el premio, ex aequo, Álvaro Feal Fajardo, por 'Angel or Devil? A Privacy Study of Mobile Parental Control Apps', y a Yasna Vanessa Bastidas Cid, por ‘Neurotecnología: Interfaz cerebro-computador y protección de datos cerebrales o neurodatos en el contexto del tratamiento de datos personales en la Unión Europea'. El primer trabajo, en el que también han participado Paolo Calciati, Narseo Vallina-Rodríguez, Carmela Troncoso y Alessandra Gorla, estudia las aplicaciones de control parental con impacto internacional, analizando el problema de la recolección y envío de datos en Android y estableciendo recomendaciones de cumplimiento. El segundo trabajo analiza el nacimiento de los neuroderechos humanos, y cómo protegerlos en el futuro.

Asimismo, el jurado otorgó un accésit a Darío Lopez Rincón por su trabajo 'Protección de datos en el sector de los videojuegos: análisis de su adaptación al RGPD y LOPDGDD desde el punto de vista de los videojuegos de gran presupuesto o «triple A»', que aborda el impacto en los derechos a la protección de datos de los menores con relación al tratamiento de sus datos en los videojuegos.

Respecto al Premio a la Proactividad y Buenas Prácticas en el cumplimiento del Reglamento Europeo de Protección de Datos y la Ley Orgánica de Protección de Datos Personales y Garantía de los derechos digitales, en la modalidad de empresas, asociaciones y fundaciones, el jurado entregó el premio, ex aequo, a Paloma Llaneza González y Hugo Albornoz, por el trabajo 'Consent Commons: una iconografía para la protección de datos y la transparencia’, y a la Fundación 29 de Febrero por el trabajo 'Healthdata29: Guía legal y repositorio para fomentar la compartición de datos de salud'. El primero de los trabajos premiados es un proyecto de implantación gratuita que desarrolla un sistema de iconos que facilita la comprensión de las condiciones y bases del tratamiento para empresas y organismos públicos, mientras que el segundo es una iniciativa que tiene por objeto fomentar la compartición de datos de salud anonimizados con fines de investigación, a través de una guía legal y un repositorio.

En el apartado de entidades del sector público, se entregó el premio al Instituto Nacional de la Seguridad Social (INSS) por el trabajo 'La gestión de la privacidad en el INSS: Haciendo realidad el enfoque 360º', que hace una exposición de la proactividad, las buenas prácticas adoptadas y los mecanismos de control establecidos por la entidad.

El jurado entregó un accésit a la Diputación de Tarragona por el trabajo 'Adaptación de las entidades locales de Tarragona, a la normativa de protección de datos, papel que desempeña la Unidad de Secretaria Intervención (USIM) de la Diputación de Tarragona', un proyecto que realiza un análisis de las actividades de tratamiento comunes, el proceso de implantación de administración electrónica común e informa de los procesos de formación de los empleados públicos y los cargos electos, entre otros aspectos.

En la categoría 'Premio a las Buenas prácticas educativas en privacidad y protección de datos personales para un uso seguro de internet', el jurado otorgó el premio en la modalidad dirigida a centros de enseñanza de Educación Primaria, ESO, Bachillerato y Formación Profesional, a Profesores de Almendralejo Soc. Coop. Enseñanza CC Ruta de la Plata por 'Abordaje sistémico del valor de la privacidad en la enseñanza escolar', un proyecto en el que se trabaja este derecho fundamental con alumnos, profesores y padres; se da a conocer la figura del DPD y se ofrecen guías de formación específicas para etapas educativas desde infantil hasta secundaria.

En la modalidad de compromiso de personas, instituciones, organismos, entidades, organizaciones y asociaciones, públicas y privadas, el premio recayó en la Fundación Canaria Yrichen por el 'Proyecto Ayudantes TIC', que fomenta el uso responsable de las tecnologías y el aprendizaje entre iguales, persigue el desarrollo de una cultura de ciberconvivencia segura y saludable y ofrece orientación familiar individualizada.

Finalmente, en la categoría de 'Buenas prácticas en relación con iniciativas del ámbito público y privado dirigidas a una mayor protección en internet de la privacidad de las mujeres víctimas de violencia por razón de género', el jurado premió el trabajo de Miriam Pascual Martín, por su trabajo 'No más películas. Toma el mando y protege tus datos para frenar la violencia de género'. En él se presentan múltiples intervenciones en varios ámbitos dirigidos a alumnos de Grado Medio de FP, entre las que destacan los recursos utilizados y la perspectiva racional y emocional para abordar este problema, y se promueven diversas acciones de concienciación para evitar la violencia digital compartiendo recursos con la comunidad educativa.

Premios recibidos por la AEPD

Como puede consultarse en otros apartados de esta Memoria, la Agencia ha realizado una importante labor de concienciación tanto entre aquellos que tratan datos como entre la ciudadanía. Este trabajo le ha supuesto la concesión de tres nuevos premios durante 2021, que se suman a los 15 que ya le habían sido concedidos por instituciones y organizaciones públicas y privadas desde el año 2017. El detalle de todos ellos puede consultarse en *esta sección de la página web de la AEPD.*

Acto de entrega del 'Premio Ciudadanía', del Ministerio de Política Territorial y Función Pública

La AEPD fue galardonada con el Premio Ciudadanía en la XIII edición de los 'Premios a la Calidad e Innovación en la Gestión Pública', otorgado por el Ministerio de Política Territorial y Función Pública. La Agencia obtuvo el premio por su iniciativa "Del plan estratégico al plan de sostenibilidad y responsabilidad social: Menores y uso responsable de Internet, canal prioritario, web de ayuda para las víctimas de violencia de género, prevención del acoso digital en el ámbito laboral y código ético de la AEPD". El 'Premio Ciudadanía' tiene por objeto reconocer la calidad e impacto en la ciudadanía de iniciativas singulares de mejora en los sistemas de relación con los ciudadanos o que reviertan en una mayor transparencia, participación, rendición de cuentas o integridad en la provisión de los servicios públicos.

• 'Premios Nacionales de Informática y Salud 2020' de SEIS

La Agencia Española de Protección de Datos (AEPD) fue galardonada, ex aequo, con el Premio a la Mejor iniciativa en materia de Ciberseguridad, privacidad y protección de datos en el ámbito sanitario en los XXVI Premios Nacionales de Informática y Salud 2020 de la Sociedad Española de Informática de la Salud (SEIS). El galardón se

concedió tanto a la Agencia Española de Protección de Datos, como a la Autoridad Catalana de Protección de Datos, la Agencia Vasca de Protección de Datos y el Consejo de Trasparencia y Protección de datos de Andalucía.

En particular, la Sociedad Española de Informática de la Salud reconoce su contribución en el tratamiento de los datos sensibles en situación de pandemia, donde la seguridad y la privacidad de los datos ha requerido un tratamiento especial. "Para afrontar este reto con las mayores garantías posibles y de una manera unificada, ha sido fundamental el papel desarrollado y el liderazgo ejercido por las Autoridades de Protección de Datos", destaca SEIS.

Trofeo Extraordinario Seguridad TIC de la revista Red Seguridad

La directora de la Agencia fue galardonada por la revista Red Seguridad con el Trofeo Extraordinario de la 14ª edición de los Trofeos de la Seguridad TIC, unos premios que reconocen la labor de profesionales, empresas y organismos dedicados a la ciberseguridad. Este reconocimiento ha sido concedido a la directora "por su importante labor al frente de la AEPD, destacando su profesionalidad y saber hacer".

Los premios cuentan con siete categorías: Innovación, Empresa de Seguridad TIC, Institución pública, Trayectoria profesional, Captación y divulgación, Trofeo al centro educativo y Trofeo extraordinario. Este último se concede a la persona, entidad o colectivo que más se haya destacado por sus valores humanos, acciones meritorias o labor extraordinaria en pro del desarrollo y difusión de la cultura de la Seguridad en Tecnologías de la Información y las Comunicaciones.

El jurado de estos premios es el Comité Técnico Asesor de Red Seguridad, compuesto por representantes de las principales asociaciones del sector, varios organismos y profesionales independientes, que deliberan sobre las candidaturas recibidas y formulan su veredicto.

4.8. Acceso a la información pública y transparencia

La transparencia forma parte de los valores de la Agencia. La Agencia dispone de su propia Unidad de Información y Transparencia (UIT) que prepara las resoluciones tras recabar datos de las unidades operativas de la Agencia que pueden proporcionar la información que se solicita. La Agencia ha desarrollado protocolos internos de tramitación que permiten tramitar las solicitudes de acceso de forma ágil y precisa. Las resoluciones de acceso a la información pública son resoluciones razonadas, jurídicamente sólidas y se resuelven en un tiempo de tramitación significativamente menor al plazo máximo legal de un mes. Siguiendo su compromiso de actuación transparente y responsable, el 97% de las resoluciones sustantivas adoptadas por la AEPD han concedido el acceso a la información solicitada, como se desprende de los datos expuestos en esta Memoria. Las resoluciones son ampliamente aceptadas, siendo el nivel de litigiosidad inferior al 3%.

El número de solicitudes de acceso a la información pública se ha incrementado ligeramente respecto al año anterior. La mayor parte de las peticiones se refieren a expedientes y resoluciones sancionadores. También se han solicitado y se ha facilitado el acceso a informes de la AEPD, relaciones de puestos de trabajo, e información sobre contratos de la AEPD.

La UIT de la AEPD participa en el grupo de trabajo del Comité Europeo de Protección de Datos encargado del 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 UITs de la AGE, para coordinación de criterios, convocado y dirigido por la Dirección General de Gobernanza Pública.

En aplicación de su compromiso de actuación transparente, la AEPD publica en su web las resoluciones denegatorias o parcialmente denegatorias, para el conocimiento general de los razonamientos y motivación de su actuación *https://www.aepd.es/es/la-agencia/transparencia/resoluciones-de-transparencia*

5. Ayuda efectiva a las entidades

5.1. Primeras impresiones del canal del DPD: consultas jurídicamente complejas que hacen reflexionar a la AEPD y a los DPDs sobre las zonas grises del RGPD

El canal de consulta para los DPD, "Canal del DPD", operativo desde noviembre de 2020, se encuentra en el ámbito de la Instrucción 1/2021. La Instrucción indica que las consultas al Canal del DPD deben ir acompañadas de un informe del DPD en cuestión, en el que se analice el tratamiento sobre el que se consulta y se examinen los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del mismo.

En el segundo semestre del año se ha constatado que el tipo de consultas presentadas revisten una mayor complejidad jurídica y plantean cuestiones que no están perfectamente delimitadas, o lo que podríamos llamar zonas grises del RGPD. Así, por ejemplo, se han planteado consultas sobre la determinación del establecimiento principal en la UE de un grupo corporativo cuyo establecimiento principal de toma de decisiones ha quedado fuera de la UE (Reino Unido). También se han planteado cuestiones relativas al tratamiento de datos relacionados con la vacunación para combatir la COVID y sus implicaciones en la esfera laboral. Igualmente, en el sector de la salud se han planteado consultas sobre la base de legitimación de tratamientos que afectan a los organismos que gestionan donaciones de sangre.

La delimitación de las figuras de responsable y encargado en supuestos de tratamientos en la prestación de servicios sanitarios también sigue siendo recurrente. Las cuestiones relacionadas con la obligación de atender a requerimientos tributarios y el tratamiento de datos a través de sistemas de videovigilancia, tanto en espacios públicos como privados, son también cuestiones sobre las que los DPDs continúan planteando dudas. Por otro lado, el tratamiento de datos a través de sistemas de reconocimiento facial es otro de los temas que más se ha planteado en el último semestre del año.

En otro orden de cosas, destaca que se han recibido numerosas consultas (también en el Canal Consulta de atención a los ciudadanos) que afectan a tratamientos de entidades locales y se observa con preocupación la ausencia de cualidades de los DPDs para asistir a esas entidades y supervisar el cumplimiento de la normativa.

El canal DPD proporciona asistencia en la medida de los recursos disponibles en las Entidades Locales menores, por lo que, dado el gran número de municipios en España, sería conveniente organizar actuaciones de sensibilización más generales e impulsar iniciativas como las adoptadas por las algunas Diputaciones provinciales, como las de Zaragoza y Cádiz, que proporcionan, de forma centralizada desde la estructura de la Diputación, servicios de DPD a todos los municipios de la provincia que lo necesiten.

5.2. Inscripción de Delegados de Protección de Datos

Durante el año 2021 se recibieron un total de 19.142 comunicaciones de alta, baja y modificación de los datos de contacto de los delegados de protección de datos de entidades pertenecientes al sector público y al sector privado.

El número total de entidades que a 31 de diciembre han comunicado los datos de contacto de su DPD, en cumplimiento de lo estipulado en el artículo 37.7 del RGPD y el artículo 34.3 de la LOPDGDD, se ha incrementado en más de un 25% durante 2021, llegando al número total de 82.249 entidades.

El número total de DPD comunicado por las Administraciones Locales se ha incrementado en más de 19% durante este año con respecto al año anterior, llegando a un total de 3.997 responsables que han comunicado los datos de contacto de su DPD, este sector es el que más se ha incrementado dentro del colectivo de responsables o encargados que tienen potestades públicas.

5.3. Certificación de DPD conforme al Esquema AEPD – DPD

La voluntad de proporcionar seguridad a los responsables y encargados que han de designar un DPD motivó a la AEPD el desarrollo de un Esquema de certificación de DPD en julio de 2017.

La experiencia acumulada durante el funcionamiento del Esquema durante este tiempo fue poniendo de manifiesto determinados aspectos susceptibles de mejora, lo que dio lugar a sus sucesivas actualizaciones y revisiones, siendo la de más envergadura la llevada a cabo en 2020, en la adopción de la versión 1.4 del Esquema. A lo largo de 2021 se ha seguido revisando el Esquema y fruto de una reunión con las Entidades de Certificación, en la que propusieron aspectos de mejora, se elaboró una Nota Técnica (1/2021) que tuvo en cuenta la aportación de ENAC y de las Entidades de Certificación.

En cuanto al desarrollo del Esquema, durante el año 2021 finalizó el proceso de acreditación de una nueva entidad de certificación: ITANSA Certificaciones S.L., con la que ya son ocho las entidades de certificación acreditadas, constatándose una cierta estabilización en cuanto a su número, si bien hay dos entidades que se encuentran en proceso de acreditación y una entidad más que ha solicitado la documentación para poder iniciarlo.

Se recibieron 52 consultas de las Entidades de Certificación respecto a diversas cuestiones de desarrollo del Esquema, a las que se les dio respuesta.

Continua el constante seguimiento de las disposiciones y criterios que se adoptan en protección de datos, lo que tiene como consecuencia la revisión y actualización de las preguntas de las pruebas para obtener la certificación.

Aunque la pandemia supuso una ralentización de los exámenes, durante el año 2021 se ha recuperado el ritmo anterior, aunque se produjeron 16 cancelaciones por diversos motivos.

El número de exámenes que se realizaron durante 2021 fue de 82, a los que se presentaron 586 candidatos, de los que se han certificado 175, con lo que a finales de año el número de DPD certificados con arreglo al Esquema era de 789.

Se ha continuado con el desarrollo y mantenimiento de la aplicación para generar exámenes, y se ha añadido una funcionalidad para poder generar exámenes en formato adecuado para personas que padecen de dislexia.

También se han llevado a cabo 12 procesos de auditoría de cumplimiento del Esquema o de seguimiento del mismo, algunos de los cuales eran la finalización de procesos ya iniciados el año 2020, pero que se retrasaron debido a la pandemia. Las auditorias continuaron haciéndose por medios telemáticos por el mismo motivo. También se han incrementado las actividades de seguimiento del cumplimiento del Esquema, tanto de las Entidades de Certificación como de las Entidades de Formación,

Finalmente, el máster en 'Derecho de las Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información' de la Universidad Carlos III de Madrid obtuvo el reconocimiento de la AEPD como programa que da a acceso a las pruebas para obtener el certificado de DPD. Continúan en curso de gestión las solicitudes de reconocimiento de los másteres de otras dos universidades.

5.4. Códigos de Conducta

Durante este año 2021, en la línea de años anteriores, 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.

Durante 2021 se han realizado las siguientes actuaciones en relación los proyectos de código de conducta:

Códigos Nacionales

- **a)** Reuniones como con los promotores de códigos de conducta:

  - Unió Catalana D'Hospitales
  - Associació Catalana de Recursos Asistencials (ACRA)
  - Colegio Oficial de Farmacéuticos de Sevilla
  - Farmaindustria
  - Asociación Nacional de Entidades de Gestión de Cobro (ANGECO)
  - Asociación Nacional Para la Investigación de Marketing, Económica y Social (Antes ANEIMO y AEDEMO)
  - Unión Española de Entidades Aseguradoras y Reaseguradoras (UNESPA)
  - Consejo Andaluz de Colegios de Administradores de Fincas
  - PwC, Deloitte, EY y KPMG promotores Código de conducta de las firmas de servicios multidisciplinares
  - Código de conducta del Servicio Lista Robinson (ADIGITAL)
  - Código de conducta sobre la Atención del ejercicio de derechos y la resolución de conflictos (ADIGITAL)
  - Código de Conducta con la iniciativa Consent Commons

- **b)** Se inadmitió el proyecto de código de conducta del Grupo Acta Hoteles.

- **c)** Se denegó la aprobación del código de conducta del sector infomediario, presentado por la asociación multisectorial de la información (ASEDIE), cuya resolución ha sido objeto de recursos contencioso administrativo que se encuentra pendiente.

Códigos de conducta transaccionales

- **a)** En el marco del mecanismo de coherencia del RGPD en la tramitación de los códigos promovidos por:

  - La Autoridad de Control de Francia, código EUCLOUD
  - La Autoridad de Control de Bélgica, código CISPE

- **b)** Como Autoridad de Control correvisora del proyecto de código de conducta promovido por la Federación Europea de la Industria Farmacéutica sobre investigación científica (EFPIA), que regula el tratamiento de datos en el ámbito de los ensayos clínicos y el cumplimiento de obligaciones en farmacovigilancia, cuya autoridad líder es la Autoridad belga.

- **c)** En el marco de las denominadas por el Comité Europeo de Protección de Datos "sesiones informales" en la revisión de otro proyecto de código transnacional en el sector sanitario, promovido por EUCROF, Federación Europea de Organizaciones de Investigación por Contrato (CRO), como prestadores de servicios en la investigación clínica, en su condición de encargados del tratamiento.

5.5. Formación y difusión

En 2021, como consecuencia de la pandemia causada por la COVID, se ha continuado con la formación y difusión online en la mayoría de los casos. En formato online se han impartido cursos sobre protección de datos con un temario actualizado, además de formación interna, a empleados públicos de los siguientes organismos:

- Ministerio de Educación y Formación Profesional
- Ministerio de Política Territorial y Función Pública
- Ministerio de Transportes, Movilidad y Agenda Urbana
- Ministerio de Justicia
- Ministerio de Sanidad
- Ministerio de Universidades
- Ministerio de Inclusión, Seguridad Social y Migraciones
- Agencia Española de Cooperación Internacional para el Desarrollo
- Agencia Estatal de Seguridad Ferroviaria
- INAP, han recibido formación 420 empleados públicos
- Instituto Asturiano de Administración Pública "Adolfo Posada", en tres ediciones

Asimismo, se ha impartido formación y participado en acciones formativas en:

- La Asociación de Marketing de España y la Federación de empresas de Publicidad y Comunicación
- Federación Europea de Banca
- INCIBE, en el marco de la red INSAFE /INHOPE
- La Federación de Empresarios de Albacete (FEDA) con ámbito de difusión a toda la Comunidad de Castilla-La Mancha, a través de la colaboración con la Confederación de Empresarios de Castilla-La Mancha (CECAM)
- Asociación de Directivos/as de Relaciones Laborales (ADIRELAB)
- La Universidad de Salamanca, "X Fórum de expertos y jóvenes investigadores en derecho y nuevas tecnologías"
- Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México
- Universidad de Alicante
- Escuela Diplomática, curso selectivo acceso a la carrera diplomática
- Ayuntamiento de Madrid
- Ayuntamiento de Pontevedra
- ISMS Forum (comunidad de DPD)
- I Encuentro gallego de ciberseguridad (Ciber.gal)

Sobre violencia digital y de género para la difusión del Canal Prioritario:

- Ministerio de Justicia

- Asociación de periodistas de la provincia de Alicante
- Subdelegación del Gobierno de Granada: Centro de Información a la Mujer del Valle de Lecrín y de Monachil, Ayuntamiento de Almuñécar
- Subdelegación del Gobierno en Almería.

Se ha impulsado, junto con la Secretaría General, la organización y el desarrollo de la formación interna en protección de datos y transparencia, en especial para las nuevas incorporaciones.

5.6. Transferencias internacionales

Durante 2021 la Agencia Española de Protección de Datos, como autoridad de control líder, aprobó las normas corporativas vinculantes para la transferencia internacional (BCR, por sus siglas en inglés) de los grupos KUMON y COLT TECHNOLOGY SERVICES.

En ambos casos, las BCR, como herramienta para aportar garantías para las transferencias internacionales de datos dentro de las compañías del grupo, recogían las garantías para dichas transferencias cuando el grupo multinacional actúa tanto como responsable de sus tratamientos como en calidad de encargado para los tratamientos de sus clientes.

En la tramitación de estas BCR la Agencia contó con la opinión favorable del Comité Europeo de Protección de Datos.

Así mismo, la AEPD ha actuado como autoridad líder en la tramitación de las BCR de tres grupos multinacionales que se encuentran en distintas fases del procedimiento coordinado para su aprobación, y ha mantenido reuniones con entidades interesadas en disponer de BCR para las transferencias de datos entre sus compañías.

Igualmente, la AEPD es correvisora en la tramitación de ocho proyectos de BCR lideradas por autoridades de protección de datos de otros Estados miembro.

6. La potestad de supervisión

6.1. Resultados

El análisis de los resultados de la potestad de supervisión desarrollada por la Subdirección General de Inspección de datos (SGID en adelante) arroja una primera conclusión por encima de todas: el aumento sin precedentes de las reclamaciones recibidas y de la carga de trabajo por las actuaciones derivadas de ellas.

El número de reclamaciones presentadas en la Agencia, 13.905, con un aumento del 35% con respecto al año anterior, supera con creces el número que se recibió en 2018, primer año de plena aplicación del RGPD, donde el efecto por la difusión de los nuevos derechos y obligaciones del Reglamento europeo supuso la recepción de una cifra de reclamaciones récord hasta ese momento, de 13.005 reclamaciones.

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 a través de las actuaciones y procedimientos que se regulan en la LOPDGDD, y supletoriamente en la regulación del procedimiento administrativo común que establece la LPACAP, incluyendo una primera fase de análisis previo de admisibilidad, para posteriormente desarrollar la fase de traslado al responsable o encargado y decidir sobre la admisión a trámite, realizar en su caso actuaciones previas de investigación, y finalmente iniciar procedimiento sancionador o procedimiento de ejercicio de derechos. Esta tramitación, con finalización en una u otra de las fases indicadas, ha llevado a resolver 14.098 reclamaciones en 2021, lo que supone una tasa de resolución del 101% frente a las reclamaciones recibidas, por tanto, respondiendo al desafío que ha supuesto el alto volumen de reclamaciones recibidas este año, e incluso reduciendo ligeramente el número de reclamaciones pendientes frente al volumen con el que se inició 2021.

A las reclamaciones recibidas en la Agencia se suman otro tipo de entradas que inician actuaciones, 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 seguridad en las que debe valorarse su investigación por la SGID. También se crea en años recientes el canal prioritario para la retirada de contenidos sensibles, que incluye un acceso para que menores de 14 a 18 años puedan comunicar la existencia de fotografías, vídeos o audios de contenido sexual o violento en Internet. Todo ello, junto a las actuaciones realizadas por propia iniciativa, suman cerca de 900 entradas adicionales en 2021, distintas de lo que es una reclamación, que también son el origen de las actuaciones y los procedimientos descritos anteriormente.

Además de las nuevas tecnologías y los cambios normativos, la tendencia creciente de las reclamaciones también es un reflejo de la creciente preocupación de la ciudadanía por los tratamientos derivados de sus datos personales y la necesidad de control sobre los mismos. En el *último estudio* sobre privacidad elaborado por el CIS en 2018, el 76% de los ciudadanos manifestaba mucha o bastante preocupación por la protección de datos. Según la *encuesta* sobre uso de tecnologías de información y comunicación en los hogares del INE para el año 2021, en los tres últimos meses un 81% de los usuarios de Internet realizaron acciones para gestionar el acceso a su información personal en Internet.

En este mismo sentido se manifiesta el Parlamento Europeo a través de la Resolución de 25 de marzo de 2021, sobre el informe de evaluación de la Comisión acerca de la ejecución del Reglamento General de Protección de Datos dos años después de su aplicación (2020/2717(RSP)), al poner de manifiesto que "desde el inicio de la aplicación del RGPD, ha aumentado enormemente el número de reclamaciones recibidas por las autoridades de control; que ello demuestra que los interesados son

más conscientes de sus derechos y desean proteger sus datos personales de conformidad con el RGPD".

También se debe destacar, en este contexto de aumento de reclamaciones, la eliminación de barreras para el acceso a la Agencia que significa la apuesta por la Administración electrónica desde el año 2007, con la ley 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos, y posteriormente con la ley 39/2015, del procedimiento administrativo común de las Administraciones Públicas. Junto al progresivo aumento de ciudadanos que cuentan con los medios tecnológicos necesarios, facilita la presentación de reclamaciones, de forma ágil y rápida, sin necesidad de desplazamientos ni esperas. En 2021, el 72% de las reclamaciones se recibieron a través de la sede electrónica de la AEPD.

Merece la pena resaltar que, además de las competencias que tiene la Agencia derivadas del RGPD y de la LOPDGDD, la Ley 9/2014 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 están aprobando nuevas leyes que también facultan a la Agencia y, en particular, a la SGID a utilizar estos procedimientos. Entre ellas, y además de 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, durante el año 2021 se han aprobado dos más: 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 y 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. Esto redunda en un incremento de la entrada y sobre todo en reclamaciones que vienen de ámbitos normativos diferentes con peculiaridades en cada uno de ellos que conviene distinguir a la hora de realizar los procedimientos.

Todo ello contribuye a una tendencia progresiva de aumento de las reclamaciones que no parece en ningún caso transitorio ni circunstancial, como se deduce del estudio del marco temporal 2007-2021, y que pone el foco sobre los organismos de control y su capacidad para atender a todas las reclamaciones recibidas.

El aumento en la entrada y la mayor dificultad que esta presenta, por tratarse en muchos casos de temas novedosos y de cuestiones en las que es necesario llegar a un consenso con las autoridades de control de otros países, produce una tensión en la estructura y en los recursos de la SGID que no se ha visto correspondida con un paralelo aumento del personal, tendencia que no está limitada a 2021, sino a lo largo de la última década y media, donde se ha producido una transformación paulatina en el ámbito de la protección de datos, tanto por motivos tecnológicos como normativos, que ha supuesto un aumento en volumen y complejidad del trabajo necesario de supervisión y control. De esto da una muestra evidente la siguiente figura, que toma de base el año 2007 para reflejar el incremento de reclamaciones y entradas que generan nuevos casos, frente al personal asignado a la SGID. Mientras las reclamaciones han seguido una clara tendencia creciente (en 2021 supone un 471% del volumen de 2007), el personal con el que cuenta la SGID apenas ha sufrido variaciones, salvo el ligero crecimiento de los dos primeros años del período.

Conviene traer a colación de nuevo la citada Resolución del Parlamento Europeo, de 25 de marzo de 2021, en la que ha señalado "la importancia de que las autoridades de control de la Unión, así como el CEPD, dispongan de suficientes recursos financieros, técnicos y humanos para poder hacer frente rápida, pero exhaustivamente a un número cada vez mayor de casos complejos y que requieren una gran cantidad de recursos, y para coordinar y facilitar la cooperación entre las autoridades nacionales de protección de datos, hacer seguimiento adecuadamente de la aplicación del RGPD y proteger los derechos y libertades fundamentales".

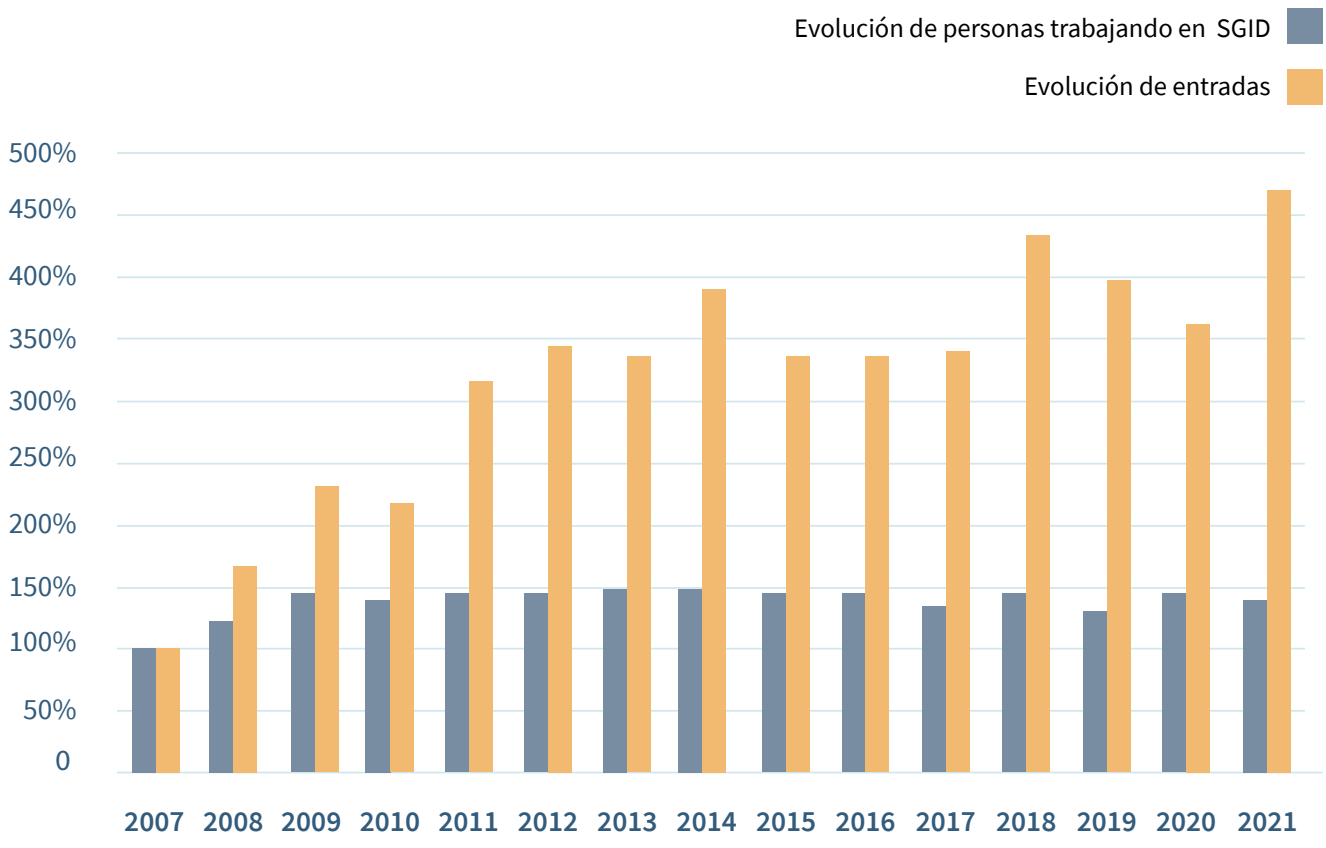
Si uno de los puntos más significativos de 2021 en cuanto a su evolución está en la entrada de reclamaciones, el segundo podríamos destacarlo

en el final del procedimiento de reclamación: las resoluciones del procedimiento sancionador. La apertura del procedimiento sancionador no representa el cauce más común de resolución de reclamaciones; por el contrario, la búsqueda de soluciones en fases tempranas es mucho más frecuente, especialmente por medio del trámite del traslado de la reclamación al responsable o encargado, tal y como está establecido en la LOPDGDD. No obstante, cuando existen responsabilidades que deben ser depuradas en un procedimiento sancionador la apertura del procedimiento deviene necesaria. En este sentido, en 2021, las resoluciones en procedimiento sancionador han crecido un 49%. La complejidad de los tratamientos estudiados y la relevancia y alcance de las infracciones se demuestra en el incremento de las multas impuestas en resolución definitiva, cuyo importe medio se ha triplicado con respecto al año anterior, y cuyo importe global ha aumentado un 337%.

La mayor complejidad y entidad de los casos resueltos también ha generado un aumento de la litigiosidad, creciendo los recursos administrativos un 18%, y los recursos ante la jurisdicción contencioso-administrativa, un 87%.

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 ha observado una ligera ralentización en la recepción de nuevos casos. No obstante, se ha visto compensado con un aumento en el número de decisiones de procedimientos participados por la Agencia, y la necesidad de concluir un proceso complejo de consenso y resolución que puede durar varios años. En el siguiente apartado se revisarán algunos de ellos.

Evolución comparativa del número de entradas y del personal de la SGID (2007-2021)



A todo esto, hay que añadir 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 EEMM, 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).

Hasta fechas recientes, existían las siguientes agencias o grandes sistemas de información: Europol; Eurojust; Sistema Información del Mercado Interior (IMI); Sistema de Información Aduanera; Sistema de Información de Visados (VIS); Sistema de Información Schengen (SIS II); y Eurodac. Sin embargo, recientemente se han ido incorporando otros cuatro ámbitos que comparten estas mismas características: Sistema de Información y Autorización de Viajes (SEIAV), más conocido como ETIAS, por sus siglas en inglés; Sistema Entrada/Salida (EES); Fiscalía Europea (EPPO); y Sistema de Información de Antecedentes Penales para no ciudadanos de la UE (ECRIS-TCN). 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, lo cierto es que estos sistemas se evalúan de manera continua. Todo esto está determinando un incremento significativo en el alcance de las tareas de supervisión en relación con estas agencias y sistemas de información.

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 correspondiente a la "Memoria en cifras".

Con objeto de solucionar el aumento en la carga de trabajo que tiene que soportar el personal de la SGID, durante el año 2021 la SGID realizó un análisis de la situación existente y diseñó un plan para poder seguir prestando un servicio adecuado de este derecho fundamental. Con esta idea diseñó una estrategia basada en tres pilares:

- **Simplificación y automatización.** Durante el ejercicio 2021 se realizó la revisión de los procesos y actuaciones que se realizan en los diferentes trámites con objeto de simplificar, eliminar lo no necesario, y aumentar la automatización. Forman parte del análisis técnicas de robotización y de inteligencia artificial. Esto permitirá bajar la carga de trabajo de aquellas labores que sean predecibles y sencillas con objeto de que el personal pueda dedicarse a las labores más complejas.
- **Modificaciones normativas.** A raíz del análisis realizado, se comprobó que existía la necesidad de establecer algunas modificaciones y desarrollos normativos que dieran cobertura a las necesidades de la SGID en el marco actual. Por eso, ya durante el año 2021 se impulsó una modificación de la LOPDGDD.
- **Adecuación de la plantilla.** A lo largo de 2021 se identificó el número de trabajadores que debía tener la SGID para poder atender las diferentes actividades a realizar como consecuencia de las competencias que tiene, así como las mejoras que debían implementarse en sus condiciones laborales. Como consecuencia de ello, se estableció un plan a dos años vista y durante el 2022 la plantilla se aumentará en 10 personas, quedando el resto pendiente para 2023. Asimismo, se cambió la estructura de la Subdirección para separar la parte de Inspección de la de Instrucción.

Por otra parte, 2021 ha sido un año de desarrollo de las estructuras de teletrabajo en general y en la Agencia en particular, tanto por las exigencias sanitarias relacionadas con la pandemia de la COVID19, especialmente en la primera parte del año, como por la consolidación del programa de teletrabajo de la Agencia que se puso en marcha ya en 2018. La implantación de este programa ha llevado asociada la implantación secuencial de un conjunto de indicadores cuantificables que

permiten evaluar el rendimiento de cada persona y también el de la unidad.

Además de estos beneficios cualitativos, en la sección de "Memoria en cifras" antes referida se ha incluido también por primera vez un anexo que correlaciona el teletrabajo con aumentos de la productividad de la SGID.

Finalmente, cabe destacar la inversión en formación especializada. Esta ha sido otra de las medidas en que se ha apoyado la SGID y su personal para reforzar los conocimientos y, a su vez, la eficacia de sus actuaciones. En el plan de formación de la Agencia se incluye la posibilidad de sufragar con cargo al mismo la asistencia a actividades formativas externas en materias específicas relacionadas con el adecuado desempeño de los puestos de trabajo, lo que ha incluido en 2021 la financiación del Máster en el Reglamento General de Protección de Datos impartido por la UNED. Asimismo, se han desarrollado diversas actividades formativas propias, tanto para las nuevas incorporaciones, como para reforzar y completar los conocimientos del personal con experiencia. Los cursos de formación internos cubren desde los aspectos administrativos generales, hasta los elementos específicos que resultan necesarios para realizar las labores propias de inspectores e instructores, como han sido en este año:

- Formación relacionada con las actividades de investigación: como el curso de criptografía, blockchain y privacidad, el curso de análisis de aplicaciones móviles, o el curso de técnicas de investigación y análisis forense impartido por la UCO de la Guardia Civil.
- Formación relacionada con materias jurídicas de protección de datos: como el curso general de protección de datos, el curso de responsabilidad proactiva, las jornadas sobre las principales decisiones de órganos judiciales, o el curso de procedimiento sancionador.
- Formación en idiomas, tanto generales y de forma continuada, como desarrolladas por medio de talleres especializados

6.2. Reclamaciones y procedimientos más relevantes

Ámbito nacional

A lo largo de 2021 ha tenido lugar un significativo incremento, de más del 90% con respecto al año 2020, de las reclamaciones relacionadas con la promoción publicitaria, que supusieron casi un 15% del total de reclamaciones registradas. El 70% de las reclamaciones vinculadas con la promoción publicitaria se referían específicamente a la recepción de llamadas telefónicas no deseadas.

En este sentido cabe subrayar que en 2021 se resolvió el procedimiento sancionador PS/00059/2020 contra Vodafone, que se inició a consecuencia de las más de 190 reclamaciones recibidas contra este operador en las que se denuncia la práctica de acciones de mercadotecnia en nombre de esta entidad a través de llamadas telefónicas y comunicaciones electrónicas (SMS y correo electrónico). El procedimiento se resolvió con multas administrativas que ascienden a 8.150.000 € por infracción de los artículos 28 y 44 del RGDP, el artículo 48.1.b) de la Ley 9/2014 General de Telecomunicaciones (en adelante, LGTel) y el artículo 21 de la Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico (en adelante, LSSI).

Debe destacarse que una parte de las reclamaciones en el ámbito publicitario estaban vinculadas además con distintas irregularidades en los procesos de contratación, particularmente las que tienen su origen en la suplantación de la compañía que supuestamente ofrece el servicio, utilizando técnicas de vishing (a través de llamadas telefónicas) o smishing (mediante el envío de mensajes cortos). Fueron también numerosas, como otros años, las reclamaciones referidas a la suplantación de la identidad de la persona reclamante, a partir de datos identificativos obtenidos de fuentes ajenas. En estos casos las reclamaciones estaban asociadas a la contratación de servicios

de telecomunicaciones (particularmente, la solicitud de duplicados de tarjeta, SIM swapping) y de suministro energético, ámbito este último en el que se produjo un significativo aumento en el número de reclamaciones.

En el último trimestre de 2019, ante las noticias aparecidas en diversos medios de comunicación relativas a la utilización de prácticas fraudulentas basadas en la generación de duplicados de tarjetas SIM sin el consentimiento de sus titulares legítimos para acceder a información confidencial con fines delictivos ("SIM Swapping"), se iniciaron de oficio actuaciones de investigación tendentes a analizar estas prácticas y las medidas de seguridad existentes para su prevención. Igualmente, a finales de 2019, se empezaron a recibir en la Agencia reclamaciones de particulares que comunicaban haber sido víctimas de duplicaciones fraudulentas de sus tarjetas SIM y que, tras la realización de estas duplicaciones, se habían realizado en su nombre transferencias y otras operaciones bancarias fraudulentas, utilizando las tarjetas SIM duplicadas como medio de recuperación de las contraseñas de acceso a los servicios de banca electrónica. A lo largo de 2021 se han instruido diversos procedimientos sancionadores contra operadores de telefonía a consecuencia de la realización de estas prácticas: el PS/00001/2021 contra Vodafone por infracción de los artículos 5.1.f) y 5.2 del RGPD, que finaliza con una multa de 3.940.000€; el PS/00021/2021 contra Telefónica Móviles España por infracción del artículo 5.1.f) del RGPD, con una sanción económica de 900.000€; el PS/00022/2021 contra Orange Espagne, el PS/00027/2021 contra Xfera Móviles (MASMOVIL) y PS/00046/2021 contra Orange Virtual, todos ellos por la infracción del artículo 5.1.f) del RGPD, con multas de 700.000€, 200.000€ y 70.000€, respectivamente.

Cabe destacar igualmente los diversos procedimientos sancionadores que se han instruido contra la entidad EDP Comercializadora a consecuencia de diversas reclamaciones recibidas en las que, sustancialmente, se denuncia el tratamiento de datos personales sin consentimiento del interesado. Estos tratamientos se producen en el marco de la contratación de servicios de electricidad o gas, efectuadas supuestamente por un representante del cliente, sin que dicha entidad pueda acreditar la existencia de tal representación. Se puede citar a modo de ejemplo el PS/00037/2020, en el que se concluye que la entidad no ha adoptado medidas técnicas y organizativas para verificar si una persona que contrata sus servicios en representación de otra persona tiene autorización para llevar a cabo la contratación o para verificar si, quien actúa en nombre de otra persona física, está autorizado por esa persona a dar su consentimiento para otros tratamientos de datos personales en su nombre. Estos consentimientos fueron solicitados durante el procedimiento de contratación, con dos finalidades: el envío de comunicaciones comerciales propias y las de terceros y la elaboración de perfiles con información de bases de datos de terceros para la toma de decisiones automatizadas con el fin de enviar propuestas comerciales personalizadas y posibilitar la contratación de determinados servicios. Por otro lado, el documento destinado a proporcionar información a los interesados no ofrece suficiente información sobre el responsable del tratamiento, la base jurídica para el tratamiento (la que no se basa en el consentimiento), las finalidades del tratamiento relativas a la elaboración de perfiles sobre la base del interés legítimo, ni la posibilidad de oponerse a las actividades de tratamiento que el responsable del tratamiento basa en su interés legítimo. Además, en algunos procedimientos de contratación de los servicios de la empresa (por ejemplo, en la contratación por teléfono) la forma de acceso a toda la información requerida en virtud del artículo 13 no es sencilla ni de acceso fácil. Por todo ello, el procedimiento termina con multas por importe de 1.500.000€ por la infracción de los artículos 25 y 13 del RGPD. También se puede destacar el PS/00236/2020, con una fundamentación jurídica parecida a la del anterior, que termina igualmente con multas por importe de 1.500.000€ por la infracción de los artículos 25 y 13 del RGPD.

En el ámbito del perfilado de los datos personales de los clientes se puede subrayar el PS/00500/2020 contra CaixaBank Payments & Consumer, que se instruye a consecuencia de una reclamación en la que se pone de manifiesto el acceso indebido por

parte de Caixabank a un fichero de incumplimiento de obligaciones dinerarias en el contexto de una campaña comercial. Se sanciona a la entidad al considerarse que los procedimientos mediante los que recaba de sus clientes el consentimiento para elaborar perfiles con finalidades comerciales no se ajustan al RGPD. En particular, se considera que los clientes no reciben información específica sobre los diferentes tratamientos de elaboración de perfiles, lo que les impide conocer exactamente cuál es el tratamiento que se está consintiendo, y tampoco se da la posibilidad al interesado de prestar el consentimiento de forma individualizada en relación con todos los fines para los que se tratan los datos. Además de la sanción económica, que asciende a 3 millones de euros, se requiere a la entidad que adopte las medidas necesarias para adecuar sus procedimientos a la normativa de protección de datos personales.

Fueron especialmente numerosas las reclamaciones relacionadas, de una u otra forma, con la situación excepcional que, por segundo año consecutivo, atravesamos con motivo de la pandemia originada por la covid19. En este ámbito deben reseñarse, en particular, las relacionadas con el tratamiento de datos asociados al cumplimiento de las medidas restrictivas establecidas por las autoridades sanitarias, vinculadas con la exhibición de datos de salud sobre las circunstancias que, en ciertos casos, eximen del uso de mascarilla o con la utilización del certificado COVID digital de la UE.

El Reglamento (UE) 2021/953 y del Reglamento (UE) 2021/954 del Parlamento Europeo y del Consejo, ambos de 14 de junio de 2021, establecían la base jurídica para el tratamiento de los datos personales necesarios para expedir dicho certificado y para el tratamiento de la información necesaria para verificar y confirmar su autenticidad y validez. Gran parte de las reclamaciones ponían en duda la obligatoriedad, dictaminada en el segundo semestre del año por las respectivas Consejerías autonómicas competentes, de mostrar el certificado en la entrada de determinados establecimientos públicos y en determinadas circunstancias, lo que llevó a que, por parte de la Subdirección General de Inspección de Datos, se analizara, en cada caso, si la Orden sanitaria había sido convenientemente convalidada por el correspondiente Tribunal Superior de Justicia o, se encontraba dentro del marco definido por el Tribunal Supremo, al entender que el uso del citado instrumento era adecuado, proporcionado y necesario.

Hay que destacar también que durante 2021 se han concluido varias investigaciones que se habían iniciado de oficio a lo largo de 2020 relacionadas con tratamientos de datos personales en ámbitos directamente relacionados con la pandemia.

Un ejemplo es la investigación realizada en el E/03690/2020, en relación con el estudio y la herramienta de análisis de los datos de movilidad durante el estado de alarma con tecnología Big Data de los que es responsable el Ministerio de Transportes, Movilidad y Agenda Urbana (MITMA). El expediente finaliza con el archivo de las actuaciones al no observarse incumplimiento de la normativa de protección de datos personales.

En el E/06406/2020 se iniciaron actuaciones de oficio al conocerse que entre las medidas para hacer frente a la crisis sanitaria ocasionada por la COVID-19 aprobada por la Comunidad de Madrid se encontraba la obligación, para los salones de banquetes, discotecas y establecimientos de ocio nocturno de llevar un registro con datos de contacto de clientes para facilitar su localización en caso de confirmarse un caso positivo en alguno de estos establecimientos. Tras constatarse en las actuaciones la existencia de un Auto del Juzgado de lo Contencioso Administrativo nº 8 de Madrid, en el que se acuerda la ratificación de las citadas medidas, se procede al archivo de las actuaciones.

También el E/03882/2020 se inició de oficio debido a las noticias publicadas en relación con la instalación de cámaras fototérmicas a la entrada de los establecimientos de El Corte Inglés para la toma de temperatura de trabajadores y clientes. En relación con la toma de temperatura a los trabajadores, se trata de una obligación legal en virtud de la Ley de Prevención de Riesgos Laborales, que no se realiza de manera aislada, sino en conjunto con otras medidas para la lucha contra la COVID

19, previstas en un "Plan de contingencia para la reapertura de tiendas". En cuanto a la toma de temperatura a los clientes, no queda acreditado que se hayan tratado datos personales de personas identificables, por lo que no resulta de aplicación el RGPD. El expediente finaliza con el archivo de las actuaciones.

A raíz de las noticias publicadas sobre el proyecto de la Generalitat Valenciana de implantación de una app de rastreo por bluetooth de posibles infectados de COVID-19, se iniciaron actuaciones previas de investigación en el E/04294/2020. Esta actuación se archivó dado que, finalmente, la Generalitat no procedió a la implementación de una app propia y tampoco se realizaron tratamientos de datos personales en relación con dicha app.

El E/03783/2020 se inició como consecuencia de las noticias aparecidas en diversos medios de comunicación sobre la elaboración de un informe, por parte el Ministerio del Interior, dedicado a la identificación, estudio y seguimiento, en relación con la situación creada por el COVID-19 de campañas de desinformación, así como publicaciones desmintiendo bulos y fake news susceptibles de generación de estrés social y desafección a instituciones del Gobierno. Finalmente, se acordó el archivo de las actuaciones, al no quedar acreditada la realización de tratamientos de datos de carácter personal.

Dentro del ámbito sanitario, aunque ya no relacionado directamente con la pandemia, se han resuelto procedimientos como el PS/00250/2021, en el que se sanciona con apercibimiento al Servicio Extremeño de Salud por infracción de los artículos 32 y 5.1.f) del RGPD. Las actuaciones se iniciaron a consecuencia de un escrito en el que se denunciaron accesos indebidos a la historia clínica de un paciente, constatándose en las investigaciones realizadas por la Agencia la ausencia de medidas de seguridad técnicas y organizativas apropiadas por parte de esta entidad. El PS/00391/2021 se refiere a un particular que ejerció como médico en un hospital y que solicita la titularidad de los datos de las historias clínicas de sus pacientes, dado que, tras extinguirse la relación laboral, las historias clínicas quedaron en poder y disposición del hospital. El procedimiento concluye con el archivo de la infracción imputada al centro hospitalario, al observarse que es dicha entidad, y no el médico que interpuso la reclamación, quien cumple los requisitos para ser considerado responsable del tratamiento.

Deben destacarse otras reclamaciones que aludían a iniciativas de distintos responsables de tratamiento, particularmente en el entorno académico, que ponían en riesgo la confidencialidad de los datos sanitarios, concretamente la circunstancia de vacunación de las personas afectadas. En el mismo entorno académico la Agencia tuvo la ocasión asimismo de analizar, en supuestos concretos, la implantación de medidas técnicas de tratamiento de datos biométricos dirigidas a la autenticación de los alumnos en pruebas de calificación que, como alternativa a las pruebas presenciales, se desarrollaban de forma online, para el cumplimiento de las medidas restrictivas adoptadas para evitar la propagación de la pandemia.

En el ámbito educativo se puede destacar el procedimiento PS/00052/2020, en el que se examina la utilización de una aplicación informática como recurso metodológico en clase por varios profesores de un centro educativo de la Comunidad de Madrid, sin conocimiento por parte del Director del Centro, ni de la Consejería de Educación. Inicialmente se utilizaba mostrando nombres y apellidos, junto con diversas observaciones sobre las aptitudes de los alumnos. La Consejería tomó parte activa para enmendar la situación ordenando finalmente que cesara el uso de esta aplicación. El procedimiento concluye en una sanción de apercibimiento a la Consejería de Educación por infracción del artículo 5.1.a) del RGPD.

En el PS/00412/2020 se evalúa el caso de un reclamante que denuncia la grabación en video de las sesiones de las Juntas de Evaluación que se realizan telemáticamente en un instituto de educación secundaria adscrito a la Consejería de Educación y Juventud de la Comunidad de Madrid. El procedimiento finaliza con un aperci-

bimiento a esta Consejería por vulneración de los artículos 6 y 13 del RGPD y un requerimiento para la adecuación de los tratamientos a la normativa de protección de datos en el plazo de un mes.

El incremento en el número de reclamaciones fue también significativo en el ámbito online, creciendo más de un 40% con respecto a 2020, hasta situarse en casi un 20% del total de reclamaciones registradas. Los hechos se refieren, en una proporción importante, a la difusión no consentida de datos personales en sitios web, particularmente en redes sociales y servicios equivalentes de la sociedad de la información, y a la desatención de las solicitudes de supresión dirigidas a los prestadores de servicios, que en no pocas ocasiones presentan deficiencias informativas en sus políticas de privacidad. En este apartado son reseñables las reclamaciones recibidas a través del canal prioritario, habilitado en la sede electrónica de la Agencia para la atención de situaciones excepcionalmente delicadas, cuando los contenidos publicados tengan carácter sexual o muestren actos de agresión y se estén poniendo en alto riesgo los derechos y libertades de los afectados. Gran parte de las reclamaciones recibidas por esta vía tenían relación con presuntos delitos de sextorsión, vinculados a la grabación previa de videochats por parte de organizaciones criminales, y de suplantación de la identidad, particularmente de menores de edad, en perfiles que enlazan con otras plataformas en las que se ofrece como reclamo el acceso premium a contenidos sexuales que supuestamente afectan a las personas suplantadas.

Es destacable el PS/00410/2021, en el que se sanciona con 1.500€ a un particular por publicar en un sitio web fotografías y textos de contenido sexual sobre su esposa, sin contar con su consentimiento. Para justificar la legitimación del tratamiento de datos, la parte reclamada aportó un "Contrato de sumisión sexual BDSM", suscrito por ambas partes, en el que la reclamante renuncia a su intimidad y a la protección de su imagen. Se concluye en el procedimiento que dicho contrato carece de cualquier validez contractual.

También fueron frecuentes las reclamaciones referidas a irregularidades y posibles estafas en tiendas online, que en ocasiones no ofrecen una información suficientemente clara de la identidad del vendedor y que, como se señalaba antes, no cumplen todos los requisitos informativos de la normativa de protección de datos.

Resultan reseñables los incidentes de seguridad protagonizados por los responsables y encargados de tratamiento, particularmente los operadores de telecomunicaciones, alguno de los cuales acumuló cerca de 200 reclamaciones relacionadas con una brecha de seguridad de datos personales, que provocó que por los atacantes se pusieran al descubierto en Internet los datos de sus clientes y exclientes. Se iniciaron actuaciones de investigación contra una compañía del sector asegurador, que también vio comprometidos numerosos datos de sus clientes. Se pueden destacar igualmente las investigaciones realizadas a consecuencia de diversos incidentes de seguridad como el ataque de ransomware sufrido por una entidad privada que cifró y dejó indisponibles muchos de los servicios de la misma y acompañado de una exfiltración de datos (E/01714/2021), el ataque de phishing a los empleados de un Ayuntamiento, el envío por correo electrónico a los aspirantes a una oferta de empleo del listado completo de aspirantes con sus datos personales, el envío de un fichero Excel con datos personales de los convocados para realizarse una prueba serológica de COVID-19 (E/06863/2020), la brecha de datos personales en el tratamiento de datos del servicio de estacionamiento regulado de un Ayuntamiento o la brecha en el tratamiento de datos del servicio de Sugerencias y Reclamaciones de un Ayuntamiento, que permitía la publicación en Internet de datos de sugerencias y/o reclamaciones presentadas por los ciudadanos. En muchos de estos casos se inicia procedimiento sancionador para dirigir una sanción a los responsables en caso de observarse incumplimiento de la normativa de protección de datos.

A consecuencia de una reclamación sobre una potencial brecha de seguridad de datos personales de la app de pagos Bizum, en base a la cual se podría conocer si el titular de un número de

teléfono móvil está inscrito en el servicio, en cuyo caso sería posible extraer algunos datos identificativos como nombre, iniciales o apellidos, se inician actuaciones previas de investigación en el E/09977/2020. El procedimiento termina con el archivo de las actuaciones tras comprobarse que el responsable del tratamiento dispone de medidas de seguridad apropiadas, así como la legitimidad del tratamiento amparado en el art. 6.1.b) del RGPD

Tras la notificación por parte de Wizink, entidad responsable del tratamiento, de una brecha de seguridad de datos personales, se iniciaron actuaciones previas de investigación en el E/05175/2020. En este caso, se produjo el envío a un tercero de un correo electrónico con datos de clientes de la entidad por parte de una empleada que, en el momento de producirse los hechos, trabaja en una entidad filial de Wizink que actuaba como encargada del tratamiento. Se comprueba que las medidas implantadas por la entidad eran adecuadas y que la empleada las vulneró intencionadamente. El expediente finaliza con el archivo de las actuaciones, sin perjuicio de que las investigaciones en relación con la actuación particular de la empleada sigan su curso en vía judicial.

El volumen de reclamaciones relacionadas con la morosidad se mantuvo estable con respecto al ejercicio anterior, situándose en un 16% con respecto al total de reclamaciones registradas en 2021. Los hechos planteados que motivaron la intervención de la Agencia tenían relación, como en años anteriores, con el tratamiento de datos personales relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito por sistemas comunes de información crediticia, cuando no se cumplen las garantías que permiten apreciar la prevalencia del interés legítimo del responsable del tratamiento indicadas en el artículo 20 de la LOPDGDD. A este respecto, debe señalarse que la gran mayoría de las incidencias comunicadas en las reclamaciones fueron subsanadas por el responsable de tratamiento en la fase de traslado prevista en el artículo 65.4 de la LOPDGDD.

En 2021 se resolvió el procedimiento sancionador PS/00240/2019 contra Equifax Ibérica, tras haberse examinado cerca de 100 reclamaciones contra esta entidad sobre el tratamiento de datos personales asociados a supuestas deudas en conexión con el Fichero de Reclamaciones Judiciales y Organismos Públicos (en adelante, FIJ), del que esta entidad es titular. Se impone a la entidad una multa administrativa de 1 millón de euros por infracción de diversos artículos del RGPD -en particular, los artículos 5.1.b y 6.1, en relación con los artículos 5.1.a, 5.1. d, 5.1.c y 14. Asimismo, se imponen dos medidas: por un lado, el cese del tratamiento de datos que la entidad realiza a través del FIJ y, por otro lado, la supresión de todos los datos personales objeto de tratamiento a través del FIJ y que fueron obtenidos de la publicación de anuncios de notificaciones insertados en el Tablón Edictal Único del BOE, en diarios y boletines oficiales y en las sedes electrónicas de organismos y entidades de Derecho Público.

La videovigilancia también siguió motivando una parte importante de las reclamaciones y denuncias, representando en 2021 más de un 12% de la cifra total, con un 40% de incremento respecto del año 2020.

Cabe destacar asimismo que en torno al 30% del total de reclamaciones registradas en 2021 hacían referencia a la desatención de alguno de los derechos previstos en la normativa de protección de datos. Un 7% de esas reclamaciones se vinculan con el derecho al olvido en buscadores. También siguieron siendo numerosas las reclamaciones vinculadas con el derecho al olvido en redes sociales y servicios equivalentes y en diarios digitales o boletines oficiales. Son significativas asimismo las reclamaciones relacionadas con la denegación, por algunos operadores, del acceso a las grabaciones de los archivos de audio que contienen la voz de las personas solicitantes en procesos de contratación y las relacionadas con el requerimiento, no suficientemente justificado en ocasiones, de documentación adicional (parti-

cularmente, copia del documento nacional de identidad) para identificar a la persona solicitante, documentos que no habían sido previamente requeridos con la misma finalidad en el momento de la contratación del servicio.

Al margen del RGPD, las reclamaciones relacionadas con tratamientos del ámbito penal fueron analizadas por la Agencia en el estricto marco de sus competencias, teniendo en cuenta las competencias que a su vez tienen asignadas la Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial, la Unidad de Supervisión y Control de Protección de Datos de la Fiscalía General del Estado, la Autoritat Catalana de Protecció de Dades y la Agencia Vasca de Protección de Datos. A este respecto, las formuladas en particular contra las fuerzas y cuerpos de seguridad, que representaron un 2,5% del total, fueron analizadas, cuando se referían a hechos acontecidos a partir del 16 de junio de 2021, de acuerdo con los requisitos legales previstos en 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, que transpuso al ordenamiento jurídico español la Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Debe destacarse que, en los seis primeros meses de aplicación de la nueva norma, por la Agencia no se ha hecho uso de la facultad prevista en el artículo 25, que establece que, en los casos en que se produzca un aplazamiento, limitación u omisión de la información a que se refiere el artículo 21 o una restricción del ejercicio de los derechos contemplados en los artículos 22 y 23, en los términos previstos en el artículo 24, la persona interesada podrá ejercer sus derechos a través de la autoridad de protección de datos competente.

Durante 2021, se han resuelto 8 procedimientos sancionadores relacionados con la ausencia de delegado de protección de datos (DPD) en la organización . Dos de ellos se refieren a la infracción cometida por empresas privadas (PS/00231/2021 a Aconcagua Juegos y PS/00445/2020 a Esfera Capital Agencia de Valores). Los otros seis procedimientos sancionadores se han realizado como consecuencia de reclamaciones presentadas contra seis ayuntamientos que carecían de delegado de protección de datos (PS/00314/2021 al Ayuntamiento de Molina de Segura, PS/00215/2021 al Ayuntamiento de Santa Pola, PS/00079/2021 al Ayuntamiento de Monasterio, PS/00330/2020 al Ayuntamiento de San Bartolomé de Tirajana, PS/00329/2020 al Ayuntamiento de Burgos y PS/00290/2020 al Ayuntamiento de Zaratán).

Especial relevancia jurídica tiene el procedimiento PS/00204/2020, instruido contra EMÉRITA LEGAL, por la recopilación masiva de sentencias y otras resoluciones judiciales de diversas fuentes web, incluyendo datos personales de los profesionales de la justicia, para la realización de tratamientos de datos personales orientados al cálculo de indicadores de rendimiento judicial, sirviendo los mismos de forma directa para el posicionamiento de los abogados en distintos rankings. El procedimiento finaliza con un apercibimiento por infracción del artículo 14 del RGPD.

En 2021 se resolvió el PS/00477/2019, en el que se estudia la política de privacidad de Caixabank a consecuencia de una reclamación de un particular que denunció la obligación de aceptar las nuevas condiciones en materia de protección de datos personales de la entidad y, más en concreto, la cláusula relativa a la cesión de sus datos personales a todas las empresas del grupo, siendo necesario para cancelar dicha cesión dirigir un escrito a cada una de las empresas, lo que califica de desproporcionado considerando que la cesión se acepta en un solo acto. El procedimiento se resuelve con multas cuya suma asciende a 6 millones de euros, por infracción de los artículos 6, 13 y 14 del RGPD.

Otro procedimiento relevante finalizado en 2021 es el PS/00120/2021, en el que se estudia la implantación de un sistema de reconocimiento facial en algunos de los establecimientos de Mercadona. El procedimiento finaliza con una sanción de 2.520.000€ por la infracción de varios artículos del RGPD, incluyendo los artículos 6 y 9.

La relación de responsables sancionados con multas superiores al millón de euros en resoluciones firmes y ejecutivas se detalla en el apartado VII.1 de la Memoria en cifras.

Cabe destacar que, en diversas actuaciones previas de investigación realizadas en el marco competencial de la Agencia, se han apreciado indicios de un posible uso indebido del plan nacional de numeración por parte de algunos operadores de telecomunicaciones. En este sentido, la Agencia ha remitido un informe a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales en relación con una posible infracción de la Ley General de Telecomunicaciones.

Desde otra perspectiva, la de las cuantías económicas de las sanciones, se puede señalar que durante el año 2021 se han impuesto varias sanciones con multas superiores al millón de euros, de las cuales cinco son ya firmes y ejecutivas correspondiendo estas últimas a tratamientos de datos realizados por las siguientes empresas: Banco Bilbao Vizcaya Argentaria, S.A.(PS/00070/2019); Vodafone España, S.A.U. (PS/00059/2020 y PS/00021/2021); EDP Energía, S.A.U. (PS/00236/2020); EPD Comercializadora S.A. (PS/00037/2020); y Mercadona S.A. (PS/00120/2021). El detalle se puede ver en la parte correspondiente a las cifras de la Memoria, concretamente en el apartado relacionado con las Multas y dentro del subapartado Evolución de las multas impuestas.

También se podrían citar entre los expedientes relevantes algunos relacionados con las Administraciones Públicas en los que el hecho de que la sanción impuesta sea la de apercibimiento puede haber influido negativamente en la forma y la celeridad en la que se han realizado las medidas impuestas tendentes al cese de la conducta o la corrección de la infracción que se hubiese cometido.

Ámbito transfronterizo

Entre los asuntos de interés tramitados por el procedimiento de cooperación, previsto en el artículo 60 del RGPD, puede citarse el caso de Amazon, en el que la autoridad luxemburguesa actúa como Autoridad Principal, actuando la Agencia como Autoridad interesada. Este caso se refería a la falta de base legal para realizar tratamiento de datos con fines de publicidad comportamental -análisis de comportamiento y publicidad personalizada-. Entre otros supuestos, se constata que la entidad no tiene base legal para el tratamiento de los datos con fines de publicidad comportamental, dado que este tratamiento no puede quedar amparado por el interés legítimo y tampoco se obtiene un consentimiento informado y libre. La decisión final se adopta en julio de 2021, sancionando a Amazon con multa de 746.000.000 EUR por incumplimiento de los artículos 6.1, 12, 13, 14, 15, 16, 17 y 21 del RGPD.

También resulta de interés el estudio realizado por la Autoridad irlandesa sobre el cumplimiento de los requisitos de información y transparencia -artículos 12, 13 y 14 del RGPD- por parte de WhatsApp en relación con el tratamiento de datos personales, de usuarios y no usuarios, haciendo especial hincapié en la cesión de los mismos a su empresa matriz, Facebook. La Autoridad apreció varios incumplimientos de la normativa. El proyecto de decisión recibió numerosas objeciones de las Autoridades interesadas y fue remitido al Comité Europeo de Protección de Datos por la autoridad principal, en el marco de un procedimiento de resolución de disputas (art. 65 RGPD). Finalmente, el Comité emitió una decisión vinculante, y la Autoridad adaptó su decisión a la misma, multando a la entidad con 225 millones de euros y ordenándole que solucionase las deficiencias encontradas en el plazo de 3 meses.

Otro caso relevante es la investigación realizada por la Autoridad belga acerca de una funcionalidad de Twoo, una red social orientada a la búsqueda de nuevas amistades, que permite añadir los correos electrónicos de la libreta de contactos del teléfono móvil del usuario, para después mostrar una pantalla, con todas las direcciones marcadas

y sin posibilidad de desmarcarlas, dotada de un botón para enviar un e-mail de invitación a todos los destinatarios. La Autoridad belga considera que esta funcionalidad no cumple con el RGPD, y que el tratamiento carece de base jurídica. La decisión final impone al responsable del tratamiento una multa de 50.000 euros.

Finalmente, es interesante destacar la resolución del procedimiento sancionador instruido en relación con la notificación por parte de dos responsables del tratamiento de una brecha de seguridad de datos personales, que implicaba el tratamiento de datos de menores, a consecuencia de un ataque de ransomware sufrido por el encargado de tratamiento. Dado que el encargado del tratamiento se encuentra ubicado en Reino Unido, se consideró que la brecha de seguridad debía tratarse como un tratamiento transfronterizo mediante el procedimiento previsto en el artículo 60 del RGPD, liderado por la autoridad de Reino Unido y en el que la AEPD fuera considerada autoridad de control interesada. Al no constar aceptación del caso por parte de la citada autoridad de control de Reino Unido antes de la retirada definitiva del acervo comunitario de la Unión Europea (a partir del 01/01/2021) y ante la nueva situación del Reino Unido respecto a la aplicación de normativa del Espacio Económico Europeo, como es el RGPD, se optó por tratar el caso como local. El procedimiento concluye con una sanción económica al encargado del tratamiento por infracción del artículo 33.2 del RGPD y una orden para que en el plazo de 1 mes implante las medidas apropiadas para asegurar el cumplimiento de las obligaciones impuestas por dicho artículo.

Por otra parte, se ha participado en la Evaluación Schengen que se ha realizado a Malta, aportando un experto de la Agencia al equipo de la Comisión Europea.

7. Una estructura en permanente evolución

7.1. Avance en digitalización

Durante el pasado año 2021 la Agencia ha completado diversas iniciativas relevantes tanto en el área de las infraestructuras y la seguridad como de los servicios y aplicaciones, conforme a la hoja de ruta establecida para su digitalización, y con el fin de la mejora continua en la gestión de sus procesos y el desempeño de su cometido.

En primer lugar, el año comenzó con la puesta en marcha del sitio web del «Pacto digital para la protección de las personas», en el que se puede consultar la información sobre el Pacto y la relación de las entidades adheridas, o solicitar la adhesión a través de un formulario electrónico.
Se ha seguido trabajando en la actualización tecnológica y funcional de la sede electrónica, el principal medio de interacción con la Agencia a través de medios electrónicos, con la evolución de los formularios de brechas de protección de datos, quejas y sugerencias; la mejora en la gestión de la representación de entidades extranjeras y en la visualización de los procedimientos en curso disponibles en la sección de «Mis trámites». Además, se ha incorporado el sistema de firma «FIRe» para permitir al ciudadano la posibilidad de utilizar sus certificados en la nube.

En el ámbito de la administración electrónica, continúa la estrategia de adopción de los medios y servicios comunes, como trama en la nube, y se ha seguido trabajando en la integración de nuevos servicios de la plataforma de intermediación de datos, como la consulta del domicilio del INE y de bienes inmuebles de catastro; en la integración con el registro electrónico de apoderamientos y en la mejora de la remisión de expedientes electrónicos a la administración de justicia. Además, se ha trabajado en el desarrollo de la Política de gestión documental y la definición de unos catálogos de datos comunes a las diferentes aplicaciones para su explotación en la presentación de los contenidos en el portal web institucional.
En el ámbito de la tramitación de sus procedimientos electrónicos, se ha avanzado en la digitalización de la gestión de las brechas de protección de datos y en el visto bueno y sellado de las consultas que recibe la Agencia. En la tramitación de los procedimientos de la Subdirección General de Inspección de Datos se ha incorporado el concepto y gestión de «expediente» como aglutinador y ordenador de los actos de trámite, se ha realizado una actualización tecnológica del sistema de tramitación y se han implementado mecanismos de automatización, como los traslados de vídeo vigilancia y las admisiones a trámite fuera de plazo. Además, se ha acometido una importante mejora en la gestión de documentos, marcas y plantillas.

Por otra parte, para una mejor experiencia del ciudadano en su relación electrónica con la Agencia, y como otra de las actuaciones significativas acometidas en el año 2021, se ha seguido evolucionando el portal institucional de la Agencia, con la incorporación de nuevos elementos visuales, como el mapa de navegación web, y la evolución de los existentes, como los carruseles de la portada o la limpieza de metadatos de los ficheros publicados.

Se ha desarrollado en el portal institucional una nueva sección de preguntas frecuentes, trasladando los contenidos que se encontraban en la sede electrónica, facilitando así la edición de texto enriquecido, la incorporación de elementos multimedia y la vinculación de contenidos relacionados.
La nueva sección de preguntas frecuentes mejora las capacidades de navegación entre los elementos de las diferentes categorías e

incorpora un buscador de texto libre. Además, se integra en los resultados del buscador general del portal, permitiendo una búsqueda unificada en todos los contenidos publicados, de forma que el ciudadano pueda localizar desde un único punto todos los materiales relacionados con su búsqueda y encontrar la respuesta a sus preguntas con mayor facilidad.

Se ha revisado el proceso de publicación de resoluciones, desarrollando una interfaz de publicación más robusta a través de servicios web en sustitución del antiguo modelo de procesamiento en lotes, depurando una revisión automatizada de las publicaciones en un entorno previo a la publicación en producción y, con todo ello, incrementando la madurez del proceso.

Se han puesto en marcha diversas iniciativas de colaboración con el Ministerio de Justicia para la robotización y automatización de procesos, la explotación de datos, la utilización de técnicas de inteligencia artificial en la anonimización de documentos y la realización de actos de trámite en remoto.

Internamente, la Agencia ha continuado con las actuaciones de modernización de sus infraestructuras y la mejora de la seguridad, actualizando las versiones del gestor documental y de las bases de datos, promocionando la redundancia de los controladores de dominio y la evolución del punto de conexión a la «Red Sara NG», completando la integración de los lotes 1 y 3 del contrato unificado de comunicaciones (CORA).
Por último, se ha seguido trabajando en el mantenimiento y securización de los equipos en teletrabajo, con actuaciones como el filtrado de tráfico y la actualización de las soluciones de antivirus y de copias de seguridad de las cuentas personales.

7.2. El teletrabajo como herramienta esencial de compromiso con los empleados en el Plan de Responsabilidad Social de la AEPD

Si bien ya a inicios de 2020 el teletrabajo se encontraba implantando para el 80% de la plantilla, la situación de emergencia sanitaria vino a imponer el teletrabajo continuado para la totalidad de la plantilla.

Transcurridos 2 años desde el inicio de la pandemia, se puede afirmar que no sólo se ha contribuido a minimizar el impacto del COVID 19 entre los empleados de la Agencia al haber reducido los desplazamientos y establecer un sistema de turnos, sino que, además, se ha incrementado la productividad de la plantilla. Para el seguimiento de la productividad principalmente se hace uso de los diferentes cuadros de mando y de un sistema de Business Intelligence (BI) que permite la extracción de información. Los principales y más claros indicadores de productividad de la actividad global de la AEPD son la actividad de resolución y el tiempo de resolución de los expedientes. Durante 2021 las reclamaciones se vieron incrementadas en casi un 40% y todas ellas fueron resueltas sin incremento de plantilla y con un teletrabajo del 60% (un 100% de la plantilla realizando tres días por semana de teletrabajo, supone un 60% de teletrabajo).

Por otro lado, en consonancia con el compromiso de la AEPD con la conciliación de la vida laboral, personal y familiar de sus empleados, así como con el compromiso de esta Agencia con el medioambiente y el equilibrio territorial, se ha creado una nueva modalidad de teletrabajo, la modalidad ampliada, que persigue el objetivo de facilitar la conciliación a aquellos empleados cuyos núcleos familiares se encuentren más alejados de la sede. Esta modalidad de teletrabajo no sólo viene a consolidarse como herramienta esencial del compromiso de la AEPD en materia de conciliación tal y como se prevé en el Plan de Responsabilidad Social de la Agencia, sino que, además, ha permitido atraer a la AEPD el conocimiento.

Por último, señalar que el teletrabajo ha venido a modificar los patrones de las reuniones y actividades formativa de la Agencia. En la encuesta sobre formación realizada a finales de 2021, un 44% de las personas encuestadas ha valorado como preferente la formación a distancia frente a la presencial que obtuvo un 5% de adhesión. El 38% prefiere una combinación de ambas.

7.3. Actuaciones en materia de prevención de riesgos laborales

Como continuidad a las medidas adoptadas a lo largo de 2020 por la emergencia sanitaria derivada del COVID 19, durante 2021 se han tomado medidas juntamente con el comité de Seguridad y Salud y se han publicado los siguientes documentos:

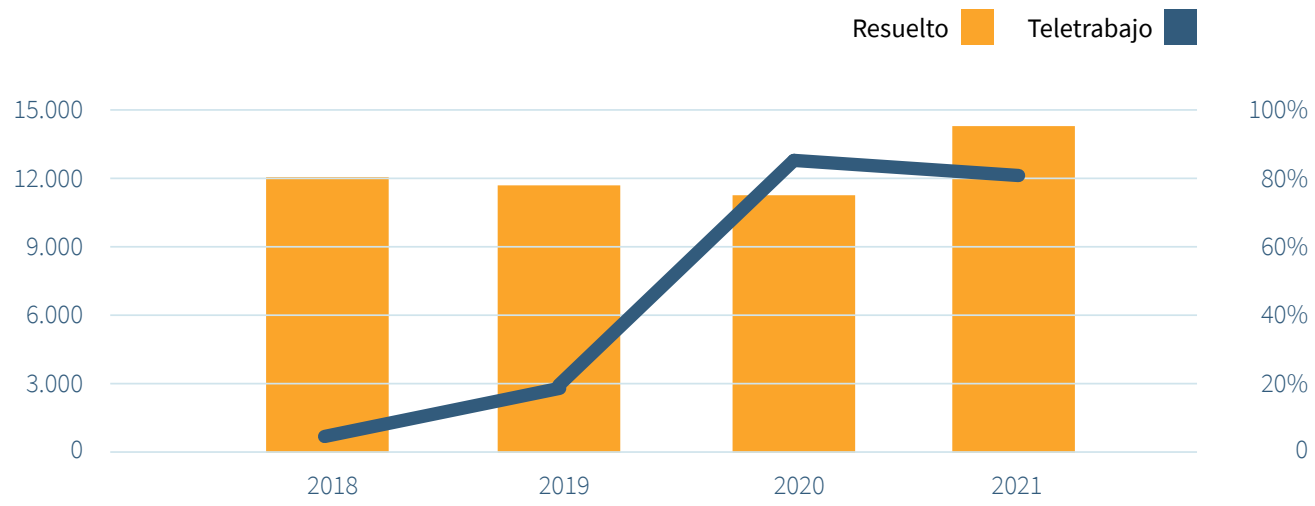
- Actualización de protocolo de reincorporación al trabajo presencial que se aprobó en abril de 2020
- Plan de contingencia de la AEPD

Con la vuelta a la presencialidad de la prestación laboral en el mes de abril, se han mantenido las medidas preventivas y los canales de comunicación habilitados al efecto: se ha dotado de gel hidroalcohólico, pantallas protectoras, mascarillas, pañuelos, papeleras con tapa y demás elementos recomendados por las autoridades sanitarias y laborales.

7.4. Provisión de puestos

La AEPD ha sufrido una importante transformación en sus funciones con motivo de la entrada en vigor del RGPD y de la LOPDGDD. Tras más de dos años desde la nueva normativa, el Parlamento Europeo el 25 de marzo de 2021 emitió un informe de evaluación de la Comisión acerca de la ejecución del RGPD señalando "la importancia de que las autoridades de control de la Unión dispongan de suficientes recursos financieros, técnicos y humanos para poder hacer frente rápida, pero exhaustivamente a un número cada vez mayor de casos complejos y que requieren una gran cantidad de recursos, y para coordinar y facilitar la cooperación entre las autoridades nacionales de protección de datos, hacer seguimiento adecuadamente de la aplicación del RGPD y proteger los derechos y libertades fundamentales".

Entradas resueltas y teletrabajo



Asimismo, el Parlamento Europeo manifiesta su gran preocupación el hecho de que las autoridades de control de 21 Estados del total de 31 Estados que aplican el RGPD (entre ellos, España) carecen de recursos humanos, técnicos y financieros, locales e infraestructura suficientes para desempeñar eficazmente sus tareas y ejercer sus competencias; manifiesta su preocupación, asimismo, por la falta de personal técnico especializado en la mayoría de las autoridades de control de toda la Unión, lo que dificulta las investigaciones y la ejecución; se observa con preocupación que las autoridades de control se encuentran bajo presión debido a la creciente disparidad entre su responsabilidad de protección de los datos personales y sus recursos para hacerlo; observa, además, que los servicios digitales serán cada vez más complejos debido al mayor uso de innovaciones como la inteligencia artificial (es decir, el empeoramiento del problema de la transparencia limitada en el tratamiento de datos, especialmente en el caso de la formación algorítmica).

En consecuencia, el Parlamento solicita a los Estados Miembros "que cumplan su obligación jurídica en virtud del artículo 52, apartado 4, de asignar suficientes fondos a sus autoridades de protección de datos, a fin de permitirles llevar a cabo su trabajo de la mejor manera posible y garantizar unas condiciones de competencia equitativas a escala europea en la aplicación del RGPD", al tiempo que insta a la Comisión que inicie los procedimientos de infracción contra los Estados miembros que hayan incumplido esta obligación.

Es por ello que, a lo largo del año se ha producido un importante esfuerzo para garantizar la cobertura de la práctica totalidad de los puestos:

- Concursos: tres concursos específicos y un concurso general, afectando a un total de 19 puestos de trabajo.
- Libres designaciones: seis convocatorias, afectando a un total de 12 puestos de trabajo.
- Publicaciones en Funciona de 19 puestos de trabajo.

Con ello, se alcanza un elevado grado de ocupación de los puestos de la entidad, con 165 puestos de funcionarios cubiertos, correspondiente la diferencia con el número total del ente (196) principalmente a puestos que solo pueden cubrirse por funcionarios de nuevo ingreso, puestos de nivel 14 de muy difícil cobertura y puestos reservados de funcionarios que ocupan otras plazas en comisión de servicio.

Persiste la necesidad de incrementar el número de empleados del ente, especialmente en la Subdirección General de Inspección de Datos a efectos de adaptar la estructura de la misma a las nuevas funciones y formas de trabajar (expedientes transfronterizos) que se han establecido tras la aprobación de la nueva normativa en materia de protección de datos.

7.5. Ejecución presupuestaria

Ejecución presupuestaria del presupuesto de gastos

El Presupuesto de la Agencia Española de Protección de Datos en el ejercicio 2021 ha ascendido a 15.762.500 euros, lo que supone un incremento del 10,78% respecto al presupuesto de 2020 si no se tiene en cuenta la transferencia de 21 millones de euros que se realizó al Tesoro Público en dicho ejercicio para contribuir a las necesidades económicas derivadas de la COVID-19.

A lo largo del ejercicio económico 2021 se ha aprobado una única modificación presupuestaria interna que no ha incrementado la cuantía inicial del presupuesto de gastos. Esta transferencia estuvo destinada a dotar de crédito las partidas presupuestarias destinadas a atender la productividad y las gratificaciones del personal, ya que su importe inicial resultaba inferior a los importes autorizados por la Secretaría de Estado de Presupuestos y Gastos, una vez certificados por la AEPD los valores de los indicadores definidos en el Modelo de Productividad Adicional por Cumplimiento de Objetivos. El crédito se transfirió desde una serie de partidas de los capítulos 1, 2, 4 y 6, cuya previsión de ejecución permitía considerar como presupuesto disponible parte de su importe

inicial por lo que podía ser utilizado para atender las necesidades antes descritas.

Aunque se ha producido un ligero descenso en el nivel de ejecución respecto al año anterior, éste continúa siendo elevado, por encima del 90%, alcanzándose un porcentaje de ejecución del 91,49%. Esta reducción se ha debido en gran parte a que los expedientes de contratación 60/2019 y 48/2021 no alcanzaron la ejecución prevista por incidencias diversas con los contratistas, quedando un remanente de 262.626,12 euros que estuvo disponible en las últimas semanas del ejercicio con lo que no pudo ejecutarse.

Ejecución presupuestaria del presupuesto de ingresos

El presupuesto aprobado para la Agencia en el ejercicio 2021 se cubre mayoritariamente, como en años anteriores, y al no recibirse transferencias del Estado, con unas previsiones de ingresos por recargos, sanciones e intereses de demora de 9.983.850 euros y con un remanente de tesorería por un importe de 5.737.850 euros. El resto se cubre igualmente con las previsiones de transferencias corrientes (transferencias de la UE) por un importe de 20.000 euros, y con las previsiones de préstamos por un importe de 22.800 euros.

Durante el año 2021, el importe de los derechos reconocidos brutos asciende 34.762.648,30 euros, correspondiendo el 99,99% (34.759.172 €) a derechos reconocidos por las sanciones impuestas por resoluciones de la directora de la Agencia Española de Protección de Datos, lo que supone un incremento en un 290% respecto a los datos de 2020. Los derechos reconocidos netos ascienden a 34.516.599,84 euros, una vez contabilizadas las insolvencias o anulaciones producidas durante este año.

La recaudación total en el ejercicio corriente 2021 asciende a 18.339.934,09 euros, de los que 18.337.168,62 euros corresponden a sanciones (un 99,99%). Esta recaudación ha supuesto un incremento de 122,27 % respecto a la recaudación total de 2020.

La recaudación neta en el ejercicio corriente 2021 ha sido de 18.232.420,63 euros, una vez contabilizadas las devoluciones de sanciones.

Teniendo en cuenta que, junto con la recaudación del ejercicio, también se produce recaudación de derechos reconocidos de ejercicios cerrados durante el ejercicio corriente, la recaudación total de sanciones en el ejercicio de 2021 asciende a 19.618.869,67 euros, y la recaudación neta total de sanciones ha sido de 19.511.356,21 euros una vez contabilizadas las devoluciones de ingresos como consecuencia de la estimación parcial o total de recursos.

La devolución de sanciones en el año 2021 asciende a 107.513,46 euros. En este campo hay que resaltar que las devoluciones de sanciones en comparación con 2020 han disminuido en más del 80%.

Por otra parte, el pago de intereses de demora como consecuencia de la estimación total o parcial de recursos potestativos de reposición o contencioso-administrativos ascendió a la cantidad de 2.651,15 euros lo que supone una disminución del 93,82% respecto al importe pagado en 2020.

Presupuesto 2020 - 2021 Presupuesto, obligaciones reconocidas y porcentaje de ejecución

2021

Cap	Descripción	Presupuesto	Obligaciones reconocidas	Porcentaje de ejecución
I	Gastos de personal	8.967.328,00 €	8.284.068,81 €	92,38%
II	Gastos corrientes en bienes y servicios	5.211.088,34 €	4.881.792,69 €	93,68%
III	Gastos financieros	350.950,00 €	124.655,41 €	35,52%
IV	Transferencias corrientes	350.983,66 €	344.983,66 €	98,29%
VI	Inversiones reales	861.350,00 €	828.773,06 €	96,22%
VIII	Activos financieros	20.800,00 €	0,00 €	0,00%
TOTAL		**15.762.500,00 €**	**14.464.273,63 €**	**91,76%**

2020

Cap	Descripción	Presupuesto	Obligaciones reconocidas	Porcentaje de ejecución
I	Gastos de personal	8.026.297,28 €	7.930.070,03 €	98,80%
II	Gastos corrientes en bienes y servicios	4.903.672,62 €	4.773.217,24 €	97,34%
III	Gastos financieros	262.172,47 €	222.095,43 €	84,71%
IV	Transferencias corrientes	21.428.877,63 €	21.422.868,30 €	99,97%
VI	Inversiones reales	584.860 €	583.294,96 €	99,73%
VIII	Activos financieros	22.800 €	1.673,36 €	7,34%
TOTAL		**35.228.680 €**	**34.933.219,32 €**	**99,16%**

DIFERENCIAS 2020 - 2021

Cap	Descripción	Presupuesto	Obligaciones reconocidas	Porcentaje de ejecución
I	Gastos de personal	941.030,72 €	353.998,78 €	-6,42%
II	Gastos corrientes en bienes y servicios	307.415,72 €	108.575,46 €	-3,66%
III	Gastos financieros	88.777,53 €	-97.440,02 €	-49,19%
IV	Transferencias corrientes	-21.077.893,97 €	-21.077.884,64 €	-1,68%
VI	Inversiones reales	276.490,00 €	245.478,10 €	-3,51%
VIII	Activos financieros	-2.000,00 €	-1.673,36 €	-7,34%
TOTAL		**19.466.180,00 €**	**20.468.945,68 €**	**-7,40%**

8. La necesaria cooperación institucional

8.1. Consejo Consultivo

El Consejo Consultivo, órgano colegiado de asesoramiento de la AEPD, se reúne cuando lo convoca la directora de la AEPD, que ostenta su presidencia, o cuando lo solicite la mayoría de sus miembros y, al menos, una vez cada seis meses.

En la práctica se reúne dos veces al año (normalmente en julio y en diciembre), aunque se mantiene contacto con sus miembros de forma bilateral en múltiples ocasiones.

En 2021, la secretaria del Consejo, por orden de la dirección, convocó 2 reuniones que se celebraron el 1 de julio y el 17 de diciembre de 2021, reuniones en las que se expuso y analizó la actividad del organismo.

En la reunión del 1 de julio destacó la publicación del nuevo Estatuto de la Agencia Española de Protección de Datos, en el que se da un nuevo nombre a la anterior Subdirección de Registro para adecuarla a sus nuevas funciones, pasando a denominarse Subdirección General de Promoción y Autorizaciones. Se recogen también en el Estatuto las dos nuevas Divisiones, de Innovación Tecnológica y de Relaciones Internacionales.

En la reunión del 17 de diciembre, además de exponer la actividad de las distintas subdirecciones, se designaron los trabajos premiados en la convocatoria de los premios de la AEPD de 2021. En efecto, los miembros del Consejo son el jurado que resuelve los premios de Protección de Datos que se convocan anualmente y la resolución de los mismos es el principal asunto del orden del día de la reunión de diciembre.

Ambas reuniones se celebraron telemáticamente aplicando las novedades normativas de 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.

8.2. Autoridades Autonómicas

La aplicación efectiva del Reglamento General de Protección de Datos y, en particular, las funciones que atribuye al CEPD, ha tenido una repercusión especialmente significativa en las actividades de cooperación con las autoridades autonómicas de protección de datos. Lo que ha determinado que en el año 2021, la mayor parte de dichas actividades se hayan focalizado en el denominado “Grupo internacional con autoridades autonómicas”. En 2021, la División de Relaciones Internacionales de la Agencia y representantes de las autoridades autonómicas han celebrado tres reuniones del “grupo internacional”.

En cuanto a las reuniones conjuntas de dichas autoridades destaca la celebración el 29 de noviembre de 2021 de un Seminario de Coordinación organizado por la Agencia Vasca de Protección de Datos en la ciudad de San Sebastián.

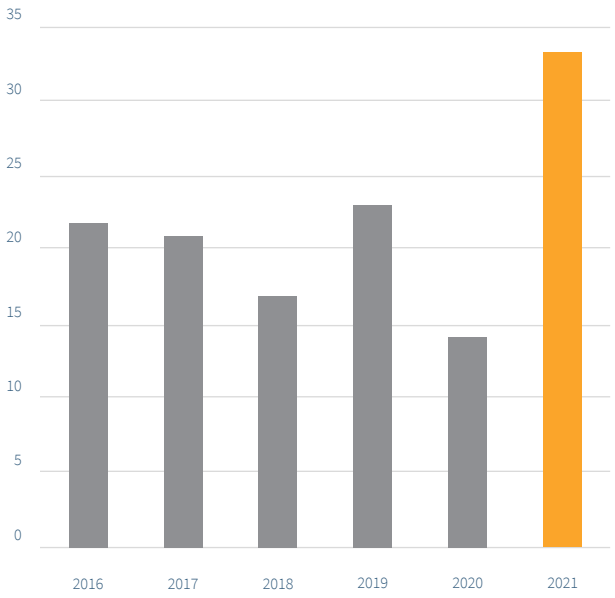
En el seminario se intercambiaron criterios sobre las iniciativas para impulsar la investigación sanitaria mediante la reutilización de la información en salud basada en el consentimiento amplio contemplado en el RGPD y la LOPDGDD, así como en los procesos de seudonimización; las garantías para la realización de transferencias internacionales de datos con posterioridad a la STJUE en el caso Schrems 2 y las implicaciones de la protección de datos en relación con identidad digital y su configuración en la carta de derechos digitales.

8.3. Relaciones con el Defensor del Pueblo

Asuntos o materias objeto de queja

Durante el presente año 2021 se han tramitado un total de 33 asuntos, frente a los 14 del pasado año.

Evolución quejas DP



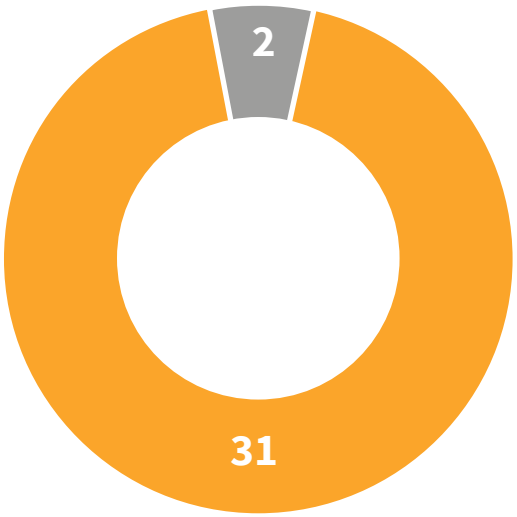
En cuanto a las materias o asuntos objeto de queja, el mayor número de ellas son solicitudes del propio Defensor del Pueblo requiriendo información sobre las medidas adoptadas por las administraciones públicas para el cumplimiento de las resoluciones de la Agencia.

Junto a ellas, destacan dos solicitudes de informe sobre el caso de La Manada y sobre los inconvenientes de la posibilidad de acceder al DNI de los empleados públicos en los certificados de firma electrónica.

Motivos de queja

Respecto a los motivos que han llevado a los ciudadanos a dirigirse a la AEPD mediante este cauce, el principal de ellos, en dos ocasiones, ha sido el relativo a la queja por la falta de respuesta en plazo de la resolución de las correspondientes reclamaciones formuladas ante la Agencia. De los restantes, junto a las ya mencionadas solicitudes de información sobre las medidas adoptadas por las administraciones públicas en cumplimiento de las resoluciones de la Agencia, así como las solicitudes de información sobre la tramitación de expedientes, destacan dos solicitudes de informe sobre el caso de La Manada y sobre los inconvenientes de la posibilidad de acceder al DNI de los empleados públicos en los certificados de firma electrónica.

Motivos de queja



Ausencia de respuesta / Retraso de la AEPD

Solicitud de información por el DP

9. Una autoridad activa en el panorama internacional

9.1. Unión Europea

9.1.1.Comité Europeo de Protección de Datos (CEPD)

La actividad del Comité Europeo de Protección de Datos ha sido intensa a lo largo del año 2021.

La Agencia Española ha participado de forma muy activa en estos trabajos. Por una parte, la Agencia está representada en todos los subgrupos de expertos del Comité Europeo. Por otra, actúa como coordinador de dos de sus subgrupos, el subgrupo de Cumplimiento, Salud y Gobierno Electrónico ("Compliance, Health and eGovernment) y, junto con la autoridad holandesa, el subgrupo de Supervisión del Cumplimiento ("Enforcement"). Finalmente, la Agencia ha participado como redactor principal o corredactor en varios de los documentos que el Comité ha publicado en 2021.

a) Directrices

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 2021 CEPD ha aprobado las siguientes Directrices:

i. Sobre ejemplos de notificaciones de brechas de seguridad

El subgrupo de tecnologías del CEPD ha elegido varios casos reales de notificaciones de brechas (el RGPD utiliza el término «violación») de seguridad y los ha analizado en estas Directrices. La AEPD participó activamente como ponente en el equipo de redacción de las Directrices, aportando varios ejemplos de notificaciones de brechas y colaborando en la elaboración del texto final. Las Directrices fueron definitivamente aprobadas por el CEPD en diciembre de 2021, después de un periodo de consulta pública.

El objetivo de estas directrices es ayudar a los responsables del tratamiento a decidir cómo gestionar las brechas de seguridad de datos, y qué factores se deben considerar durante la evaluación de riesgos.

Las brechas de seguridad pueden ser categorizadas en tres tipos:

- brecha de la confidencialidad divulgación o acceso no autorizado
- brecha de integridad: alteración no autorizada
- brecha de la disponibilidad: destrucción o pérdida de datos.

Tras recibir un ataque, el responsable debe analizar la situación e identificar los efectos adversos y su gravedad. Las directrices incluyen una serie de ejemplos prácticos para los que identifica distintas medidas que los responsables pueden aplicar con el fin de prevenir estos ataques, y entre los que se encuentran: la formación y concienciación, disponer de un equipo de respuesta a incidentes, definir un plan de respuesta, ejecutar pruebas periódicas de vulnerabilidad, proteger la información mediante cifrado, utilizar cortafuegos combinados con sistemas de detección de intrusos, controles de accesos, etc.

La guía también proporciona criterios para realizar las notificaciones tanto a la autoridad nacional de control como a los interesados.

ii. Sobre tratamientos de datos personales en el contexto de vehículos conectados y aplicaciones relacionadas con la movilidad

Estas directrices proporcionan una guía sobre el tratamiento de datos personales en los vehículos de movilidad personal y su interacción con otras aplicaciones con las que los vehículos intercambian datos.

Analiza distintos casos de uso, como el estudio de accidentes o el uso de los datos para evitar las sustracciones de los vehículos, así como los riesgos que dichos tratamientos representan para los derechos y libertades de los usuarios de estos servicios.

Entre estos riesgos, cabe señalar la falta de información que puedan tener los pasajeros de un vehículo si solo ha recibido información el conductor o propietarios del vehículo, aspecto que adicionalmente pude influir en la calidad del consentimiento del usuario cuyos datos son sometidos a dicho tratamiento, así como sobre tratamiento ulteriores que puedan existir. Tratamientos con fines incompatibles, como por ejemplo la telemetría con fines de mantenimiento del vehículo y su posible uso con fines de seguro. La problemática asociada a la seguridad de los datos y al principio de minimización así como al tratamiento de datos de geolocalización y datos biométricos.

Después de un largo proceso de más de dos años, El CEPD aprobó de forma definitiva las directrices en marzo de 2021 que ofrecen pautas para minimizar los riesgos anteriores.

iii. Sobre evaluación de criterios de certificación

Debido a la complejidad de los esquemas de certificación que se presentan para aprobación del CEPD, el subgrupo de Cumplimiento Normativo, Gobierno Electrónico y Salud (CEH), coordinado por la AEPD, ha elaborado un anexo a las Directrices 1/2018 sobre criterios de certificación que sirvan de guía a la hora de evaluar los criterios incluidos en los esquemas de certificación. Estas directrices aportan claridad y seguridad tanto a las autoridades de protección de datos como a los promotores sobre la forma en la que el CEPD evalúa los esquemas de certificación.

El anexo incluye criterios formales relativos al procedimiento a seguir para lograr el dictamen del CEPD abordando la diferente casuística que puede presentarse en función de los pasos intermedios y sus diferentes resultados, ya que combina las actuaciones a realizar por las autoridades nacionales que ha de ser seguidas por el dictamen del CEPD realizado al amparo del artículo 64.2 del RGPD y sobre los trabajos del subgrupo de cumplimento, salud y gobierno electrónico, coordinado por la Agencia Española de Protección de Datos.

iv. Sobre la aplicación del artículo 65.1.a

El Capítulo VII del RGPD recoge los mecanismos de cooperación y coherencia entre las autoridades de control que se aplican 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 en este informe), 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.

vi. Sobre focalización (targeting) de usuarios de redes sociales

En el primer semestre de 2021 se aprobaron definitivamente las Directrices sobre focalización o targeting de usuarios de redes sociales con fines publicitarios, políticos y de otro tipo. Estas directrices proporcionan orientación práctica sobre los tratamientos de segmentación o perfilados realizados a partir de los datos personales que figuran en las redes sociales.

Estos perfiles son utilizados por terceros para comunicar mensajes específicos a los usuarios de las redes sociales con la idea de que cuanto mejor sea el perfil o segmentación, más eficaz será la campaña de comunicación.

Esta focalización, entraña una serie de riesgos para los derechos y libertades del usuario de la red social:

- cuando para construir dicho perfil, se utilizan los datos obtenidos de la red social en combinación con datos obtenidos de otras fuentes externas;
- cuando el perfil se utiliza para discriminar o excluir al usuario de servicios o campañas publicitarias en base a criterios tales como la raza, el estado de salud o la orientación sexual, etc.
- cuando el perfil se utiliza para dirigir mensajes cuyo objetivo es manipular al destinatario al influir en sus decisiones de compra, o de pensamiento entornos a opiniones socio-políticas, etc.

Además de los riesgos, las directrices analizan diversos sistemas de segmentación en relación con la base jurídica de los tratamientos que se realizan ofreciendo pautas dirigidas a la transparencia, al ejercicio de los derechos, a la problemática asociada al tratamiento de datos sensibles en este tipo de tratamiento, así como a la realización de evaluaciones de impacto previas a la puesta en funcionamiento de este tipo de sistemas.

vi. Sobre la realización de Operaciones Conjuntas (art.62 RGPD)

Dentro de los mecanismos de cooperación entre autoridades de control recogido en el Capítulo VII del RGPD se encuentran las Operación Conjuntas recogidas en el artículo 62. Estas operaciones conjuntas pueden abarcar toda una variedad de actuaciones, como por ejemplo la aplicación de medidas de ejecución conjunta entre varias autoridades. Sin embargo, las que se regulan con mayor detalle en el RGPD son las investigaciones conjuntas en las que participan varias autoridades.

A pesar de ello, el nivel de detalle con el que se regulan estas investigaciones conjuntas en el artículo 62 del RGPD, no resulta suficiente para abordar todos los aspectos prácticos necesarios para desarrollar una de estas investigaciones, razón por la que ha sido elaborada esta guía en la que se han incluido, entre otros, procedimientos para el intercambio, acceso, retención, reutilización y confidencialidad de la información, transparencia y publicidad de la propia operación conjunta, idioma de trabajo y traducciones, reparto de costes y resolución de conflictos y retirada de una autoridad en medio de un operación conjunta.

Por ello, bajo el marco del anterior Grupo de Trabajo del artículo 29 (GT29) ya se elaboraron unas primeras directrices sobre Operaciones Conjuntas que fueron adoptadas por el CEPD tras su establecimiento.

Sin embargo, la realización de una primera Operación Conjunta entre la AEPD y su homóloga irlandesa puso de manifiesto las carencias de las primeras directrices, proponiéndose la AEPD como redactores

para su actualización, resultando de dicha actualización esta segunda versión de directrices de operaciones conjuntas que fueron las primeras directrices aprobadas por el CEPD en el ejercicio de 2021.

vii. Sobre el mecanismo de cooperación del artículo 60 del RGPD

La tramitación de los expedientes transfronterizos y la correspondiente interacción entre la autoridad principal y las interesadas es el objeto central del artículo 60 del RGPD. Si bien se desarrolló una primera guía bajo el antiguo GT29, posteriormente adoptada por el CEPD tras su constitución, dicha guía resultó claramente insuficiente tras su aplicación a los primeros casos transfronterizos.

Por este motivo, el CEPD decidió hacer una renovación total de dicha guía por fases. En una primera fase se abordó el tema de las objeciones pertinentes y motivadas, lo que dio lugar a un primer documento, aprobado en 2020 y que ya ha sido citado en este informe.
La segunda fase ha abordado los intercambios de información entre las autoridades implicadas desde el comienzo del caso hasta la presentación del primer borrador de decisión y comprende los artículos 60.1 y 60.3. Esta fase fue completada en marzo de 2021.

La tercera fase cubre toda la interacción entre las autoridades implicadas tendentes a negociar una decisión final a partir de primer borrador de decisión y comprende los artículos 60.4 al 60.6. Esta fase se ha completado recientemente.

La cuarta fase aborda la elaboración, adopción y notificación de la decisión final a las partes involucradas en el caso y comprende los artículos 60.7 a 60.10. Esta parte se encuentran actualmente en elaboración.

Finalmente se ha previsto una quinta fase en la que se abordará la realización de una guía práctica de consulta rápida.

Si bien a medida que se termina cada una de las fases es sometida a la aprobación del CEPD, está previsto que una vez estén aprobadas todas ellas se haga una revisión de conjunto y se someta a una aprobación final por parte del CEPD.

La AEPD forma parte del equipo de redacción de esta guía.

viii. Sobre relaciones entre el Art. 3 y el Capítulo V RGPD

Estas directrices son consecuencia de las adoptadas hace ahora dos años sobre ámbito territorial del RGPD.

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.

Para abordar esta duda se decidió entonces elaborar unas directrices específicas que son las que ahora se han adoptado (en versión para consulta pública).

La elaboración de estas directrices ha tenido también como consecuencia que el Comité ha alcanzado la primera definición de transferencia internacional de que se dispone, dado que esta definición no está presente en el RGPD, como no lo estaba en la anterior Directiva 95/46.

Para el Comité, existe una transferencia internacional cuando se dan los tres siguientes requisitos:

- El responsable o el encargado esté sujeto al Reglamento en función de un determinado tratamiento.
- El responsable o encargado (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, responsable conjunto o encargado (importador).
- El importador se encuentre en un tercer país o en una Organización Internacional, independientemente que al importador le resulte o no de aplicación el Reglamento respecto a un determinado tratamiento de acuerdo con el art.3 del Reglamento.

Como puede observarse, en esta definición de transferencia se incluye ya la respuesta a la controversia sobre la aplicación o no del concepto 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.

Esta conclusión está en línea con un acuerdo preliminar que el plenario del Comité alcanzó cuando se otorgó el mandato para elaborar las directrices que ahora se han aprobado.

Hay algunos otros elementos también de interés en las directrices, como pueden ser:

- No se considera transferencia el caso en 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 el caso en 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.

La Comisión Europea ha anunciado que preparará unas Cláusulas Contractuales Tipo para estas transferencias, adaptando el módulo correspondiente a "encargados/responsables" que se contiene en las actuales.

ix. Sobre Códigos de Conducta como instrumento de transferencias

El uso de los Códigos de Conducta (CdC) como instrumentos para proporcionar garantías adecuadas para la realización de una transferencia internacional está previsto en el artículo 46 RGPD y es una de las novedades que el Reglamento presenta.

La importancia de este nuevo instrumento de transferencias evidente, pues a través de su adhesión al mismo ofrece importantes ventajas tanto para los interesados como para los responsables y encargados del tratamiento. Los responsables y encargados del tratamiento pueden utilizar la adhesión a estos códigos como prueba de que cumplen con la exigente normativa comunitaria, reforzando así su imagen pública tanto a nivel nacional como a nivel internacional comprometiéndose con la protección de datos en sus operaciones.

Sin embargo, precisamente la novedad del instrumento ha hecho necesario que el CEPD elabore estas directrices a fin de ofrecer guía sobre algunos aspectos esenciales de la configuración de los CdC a los fines de transferencias internacionales.

El plenario del Comité adoptó una primera versión para consulta pública en su reunión del mes de julio.

Tras la consulta pública, se recibieron numerosas contribuciones, sobre las que se ha estado trabajando en el Subgrupo de Transferencias Internacionales. El principal punto que se aborda en estas contribuciones es decidir si los CdC, como instrumento de transferencia internacional:

- Requieren tener siempre validez general dentro de la UE (art.40.5 y 40.9 del Reglamento).
- O si se trata de un instrumento de transferencia que no requiere necesariamente la exigencia de esa validez general dentro de la Unión y puede estar limitado a uno solo o varios estados miembros.

Posteriormente en las diferentes reuniones de expertos se siguieron discutiendo y debatiendo diversos aspectos de este nuevo instrumento, y por lo que se refiere a esta cuestión relativa a los requisitos exigidos para su validez la mayoría de delegaciones se pronunciaron por la primera opción, de conformidad con lo dispuesto en el art. 40.1 del Reglamento, argumentando que los CdC como instrumento de transferencia requieren siempre, al igual que sucede con el régimen de las cláusulas tipo de protección de datos reguladas en el art.46.2 letras c y d del Reglamento, el cumplimiento de una doble condición: la aprobación por parte de la autoridad de control respectiva y la decisión de la Comisión Europea.

Finalmente, en el Plenario de febrero de 2022 se adoptaron esta Directrices en materia de Códigos de Conducta.

x. Sobre los conceptos de responsable y encargado

Estas Directrices abordan en detalle los conceptos de responsable, encargado y corresponsable del tratamiento y todo lo que conlleva cada uno de estos conceptos como, por ejemplo:

- Las distintas obligaciones que surgen en la relación responsable-encargado del tratamiento (p.ej., diligencia debida a la hora de seleccionar al encargado, la firma de un contrato por escrito, etc.);
- El contenido que debe tener el contrato que regule la relación entre ambas partes desde una perspectiva de protección de datos.

Tras una primera aprobación por el Comité fueron sometidas a consulta pública en a finales de 2020. Durante la consulta, se recibieron numerosas contribuciones, que determinaron varios cambios en la versión original. Estas propuestas han afectado a temas como:

- Distinción entre medios esenciales, es decir los fines y medios de tratamiento, y los medios no esenciales o aquellos relativos a aspectos prácticos que pueden ser elegidos por el encargado;
- Designación legal de corresponsables, es decir cuando dos o más entes determinan, de forma conjunta, los fines y medios en una operación de tratamiento;
- En grupos corporativos, considerar tercero respecto a un tratamiento a cualquier empresa del grupo al que pertenezca un responsable o un encargado, si dicha empresa no es ni responsable ni encargado respecto a dicho tratamiento.
- Servicios en la nube y desequilibrio de poder entre responsable y encargado prestador de servicios;
- Papel de los encargados en relación con las quiebras de seguridad.

Estos cambios, sin embargo, han sido principalmente de matización o aclaración, sin que se haya variados sustancialmente el planteamiento que en cada uno de estos temas mantenía la versión inicial sometida a consulta pública.

xi. Sobre limitaciones de acuerdo con el artículo 23 RGPD

Estas directrices también fueron aprobadas para consulta pública en la reunión plenaria del Comité de diciembre de 2020.

Como consecuencia de las contribuciones recibidas se han añadido algunos ejemplos de restricciones y se ha reestructurado el documento, en particular para diferenciar más claramente qué elementos de este son relevantes para los legisladores en los estados miembro y cuáles han de ser tenidos en cuenta por responsables y encargados.

La nueva versión fue aprobada en el plenario de octubre de 2021.

xii. Sobre asistentes de voz virtuales

En julio de 2021 se aprobaron definitivamente estas directrices después de que se incorporaran unas pequeñas modificaciones derivadas del trámite de consulta pública. Estas directrices analizan las características de estos tratamientos que se han incorporado a nuestra vida en múltiples dispositivos de uso cotidiano.

Entre los principales elementos de análisis abordados por las directrices se encuentran el marco jurídico de los tratamientos, la identificación de posibles responsables y encargados del tratamiento, la identificación de los usuarios a través de las características asociadas a su voz, la elaboración de perfiles del usuario para fines publicitarios o la selección de contenidos personalizados basados en los contenidos de las conversaciones, los tratamiento de datos de menores usuarios de estos sistemas, los problemas de seguridad y conservación de datos, el tratamiento de datos sensibles y de usos posteriores así como el ejercicio de los derechos de los interesados.

b) Declaración sobre el Paquete de Servicios Digitales y la Estrategia de Datos

Desde noviembre de 2020, la Comisión ha presentado varias propuestas legislativas en el marco de sus estrategias digitales y de datos, entre las que destacan la Ley de Servicios Digitales (DSA), la Ley de Mercados Digitales (DMA), la Ley de Gobernanza de Datos (DGA) y el Reglamento sobre un enfoque europeo para la inteligencia artificial (AIR).

El objetivo de las propuestas es facilitar el uso y el intercambio de datos (personales) entre entidades públicas y privadas dentro de la "economía de los datos", apoyar el uso de tecnologías específicas como el Big Data y la IA y regular las plataformas en línea y los guardianes de acceso (gatekeepers). Por lo tanto, el efecto combinado de la adopción y aplicación de las propuestas tendrá un impacto significativo en la protección de los derechos fundamentales a la intimidad y a la protección de los datos personales.

El CEPD y el Supervisor Europeo de Protección de Datos (SEPD) adoptaron dictámenes conjuntos sobre la DGA y la AIR a petición de la Comisión Europea, y el CEPD adoptó otra declaración separada sobre la DGA. El SEPD ha emitido además dictámenes sobre la DSA y la DMA, así como sobre la estrategia de datos de la UE. El SEPD no ha emitido ningún dictamen sobre la DSA, la DMA o las estrategias de datos subyacentes.

La declaración subraya las tres preocupaciones generales relativas a las propuestas que se han presentado hasta ahora (la DGA, la DSA y la DMA y AIR), apoyados en ejemplos concretos de las cuatro propuestas:

- Falta de protección de los derechos y libertades fundamentales de las personas;
- Fragmentación de los órganos de los órganos de supervisión; y
- Riesgos de incoherencias con el régimen de garantías del RGPD.

También se adelanta a la futura legislación, concretamente la Ley de Datos (DA) y las propuestas de creación de los llamados "espacios de datos" sectoriales, con especial atención al "Espacio Europeo de Datos de Salud". Destacando los retos particulares que plantea el aumento del intercambio de datos, el CEPD pide a los colegisladores que defina desde el principio las salvaguardias específicas de protección de datos, teniendo en cuenta, el tratamiento de categorías especiales de datos, como los datos sanitarios.

La redacción y discusión inicial de esta declaración se encargó al subgrupo de Cumplimiento Normativo, Gobierno Electrónico y Salud (CEH), coordinado por la AEPD.

c) Dictámenes

i. Dictamen sobre la decisión de adecuadión del Reino Unido

El 19 de febrero de 2021, la Comisión Europea aprobó su proyecto de decisión de ejecución sobre la protección adecuada de los datos personales por parte del Reino Unido de conformidad con el RGPD. A continuación, la Comisión Europea inició el procedimiento para su adopción formal.
En la misma fecha, la Comisión Europea solicitó el dictamen del Comité Europeo de Protección de Datos (en adelante, "EDPB") sobre la adecuación del nivel de protección en el Reino Unido. El EDPB se ha centrado en su dictamen en la evaluación de los aspectos generales del RGPD del proyecto de decisión y en el acceso de las autoridades públicas a los datos personales transferidos desde el EEE a los efectos de la ley cumplimiento y seguridad nacional, incluidos los recursos legales disponibles para las personas en el EEE.

El EDPB también evaluó si las salvaguardas proporcionadas bajo el marco legal del Reino Unido están en su lugar y son eficaces. El EDPB ha utilizado como referencia principal para este trabajo su Referencial de Adecuación del RGPD adoptado en febrero de 2018 y las Recomendaciones de la EPDB 02/2020 sobre las Garantías Esenciales Europeas en materia de interceptación de comunicaciones.

El 28 de mayo de 2021 el Parlamento de la UE aprobó una resolución declarando que, si las decisiones de implementación tomadas por la Comisión se adoptan sin cambios, las autoridades nacionales de protección de datos deberían suspender las transferencias de datos personales al Reino Unido cuando sea posible el acceso indiscriminado. La resolución solicita a la Comisión modificaciones al borrador del acuerdo e indica que las leyes de protección de datos del Reino Unido y la UE son muy similares, y es necesario ratificar un acuerdo de adecuación de datos antes de finales de junio para garantizar la transferencia continua de datos entre las dos partes.

La resolución del Parlamento Europeo hace suyas las sugerencias del CEPD en el sentido de que las prácticas de acceso masivo del Reino Unido, las transferencias posteriores y los acuerdos internacionales deben regularse de manera más clara. El régimen de protección de datos del Reino Unido contiene exenciones para la seguridad nacional y la inmigración, que se aplicarán a los ciudadanos de la UE que deseen permanecer o establecerse en el Reino Unido. La legislación actual del Reino Unido también permite acceder a datos masivos y retenerlos sin que una persona esté bajo sospecha de haber cometido un delito, que el tribunal de la UE ha juzgado recientemente que es incompatible con el Reglamento general de protección de datos. También existe la preocupación de que las transferencias de datos posteriores puedan ocurrir debido a los acuerdos de intercambio de datos del Reino Unido con los EE. UU.

ii. Dictamen 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. Los requisitos aprobados durante 2021 mediante dictamen en aplicación del artículo 64 RGPD corresponden a los presentados por las autoridades de Austria, Reino Unido, España, Bélgica, Francia, Alemania, Irlanda, Finlandia, Italia, Holanda, Dinamarca, Noruega, Hungría y Malta.

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 2021, las autoridades de Reino Unido, Luxemburgo, Irlanda, Alemania, República Checa, Holanda, Grecia, Italia, Rumanía, Portugal, Noruega, Bélgica y Letonia han recibido un dictamen favorable a sus requisitos de acreditación.

iii. Dictamen sobre el Proyecto de Decisión de Ejecución de la Comisión Europea sobre la protección adecuada de los datos personales en la República de Corea

La Comisión Europea inició el procedimiento formal de adecuación de Corea del Sur en junio de 2021. Siguiendo las previsiones del RGPD, en esa misma fecha la Comisión solicitó el dictamen sobre la propuesta de decisión al CEPD.

La AEPD formó parte del equipo de redacción del proyecto de dictamen que fue, finalmente, aprobado en el plenario del CEPD del mes de septiembre. Este es el cuarto dictamen sobre decisiones de adecuación emitido por el CEPD, después de los correspondientes a Japón y al Reino Unido (en este segundo caso uno en relación con el RGPD y otro con la Directiva de Ámbito Policial y Judicial Penal). Conviene destacar, por lo que revela de la complejidad de los trabajos en el Comité, que fue difícil encontrar autoridades que se ofrecieran a participar como redactores en la preparación del dictamen. Algo que está empezando a ser frecuente a la hora de desarrollar los documentos del CEPD.

En líneas generales, el dictamen del CEPD fue positivo respecto a la propuesta presentada por la Comisión. Se suscitaron algunos puntos en los que se solicitaban aclaraciones o confirmaciones a la Comisión Europea, como, por ejemplo, sobre la validez legal de algunos actos jurídicos en los que se basa la declaración de adecuación, el impacto de la seudonimización en la legislación coreana, la posibilidad de retirada incondicionada del consentimiento de acuerdo con esta legislación o la necesidad de seguir de cerca cualquier desarrollo que pudiera afectar a la independencia de la autoridad de supervisión coreana.

La Comisión tomó en consideración la mayoría de las observaciones hechas por el Comité en el texto que se presentó para la aprobación del comité previsto en el artículo 83 RGPD, que dio su conformidad con él, y la decisión final se publicó el 24 de septiembre de 2021.

iv. Dictamen conjunto CEPD-EDPS sobre la Ley de Gobernanza de Datos (Data Governance Act)

La Comisión Europea está impulsando un paquete normativo a raíz de su plan "Una estrategia europea para los datos". Estas iniciativas pretenden regular la denominada "economía del dato" y consolidar la soberanía digital europea. Muchas de estas nuevas normas tienen un impacto importante en el tratamiento de los datos personales.

Dentro de este paquete se encuentra la denominada "Ley de Gobernanza de los Datos" (Data Governance Act) que intenta facilitar el intercambio y la reutilización de los datos en la Unión a través de la confianza en los intermediarios y reforzando los mecanismos de compartición de datos. En el dictamen conjunto solicitado por la Comisión, el Comité y el Supervisor Europeo identificó diversas inconsistencias con el RGPD y propone posibles modificaciones para corregirlas. El dictamen se elaboró en el subgrupo CEH, coordinado por la AEPD.

Estas inconsistencias derivan, en gran medida, de que estas normas contemplan en la mayoría de los casos el uso de datos personales y no personales, y de que la regulación se hace con una fuerte inclinación hacia la perspectiva de mercado o de las tecnologías afectadas. La consecuencia es que existen incoherencias respecto a la normativa de protección de datos tanto en los conceptos empleados, como en las obligaciones que se establecen para los actores, en los modelos de gobernanza y, en último extremo, en el régimen sancionador que se establezca en cada caso.

v. Dictamen conjunto CEPD-EDPS sobre el certificado COVID Digital

El impacto de la pandemia COVID-19 ha seguido afectando la vida de los europeos y el trabajo del CEPD. La Comisión, a instancias del Consejo Europeo, elaboró en tiempo récord un reglamento para definir un certificado digital de vacunación, con validez en toda la Unión, que facilitara la vuelta a la normalidad y retomar el ejercicio de las libertades fundamentales establecidas en los tratados de la Unión.

Este Certificado COVID Digital (llamado originalmente Digital Green Certificate) ha despertado muchas dudas respecto a los principios de necesidad y proporcionalidad del tratamiento de datos que contempla, en particular teniendo en cuenta que, en los momentos en que se debatía, no existía aún una evidencia científica suficiente sobre la eficacia de las vacunas en la inmunización de las personas.
El dictamen, elaborado conjuntamente con el Supervisor Europeo en el subgrupo CEH, contó con la activa participación de la AEPD, al actuar como coordinadora del subgrupo como ponente. Recomendaba modificaciones en el texto legislativo para limitar la discrecionalidad de la Comisión al ampliar sus usos y solicita clarificaciones en cuanto a las definiciones de responsabilidades, así como a la transparencia y el almacenamiento de los datos.

Con todo, la principal preocupación de las autoridades de protección de datos se centró en las consecuencias que podría tener el uso interno de estos certificados por parte de uno o varios estados miembro para finalidades distintas de aquella para la que fueron concebidos, que era la de facilitar el proceso de levantamiento de restricciones a la libre circulación dentro de la UE que estaban iniciando los estados miembros. Desde esa perspectiva, el dictamen hace hincapié en la necesidad de que esos usos estén basados en normas legales, no den lugar a discriminación y estén sujetos a las suficientes salvaguardas desde el punto de vista de la protección de datos.

vi. Dictamen conjunto CEPD-EDPS sobre cláusulas contractuales estándar

El 12 de noviembre de 2020, la Comisión presentó un proyecto de decisión sobre cláusulas contractuales estándar entre responsables y encargados de tratamiento en aplicación, respectivamente, de los artículos

28 del RGPD y 29 del Reglamento de protección de datos de las instituciones europeas.

El mismo día, la Comisión Europea también publicó un proyecto de decisión sobre cláusulas contractuales estándar para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679.

El 12 de noviembre de 2020, la Comisión Europea solicitó un dictamen conjunto del Consejo Europeo de Protección de Datos (EDPB) y el Supervisor Europeo de Protección de Datos (SEPD) sobre la base del artículo 42, apartados 1 y 2, del Reglamento (UE). 2018/1725 (RPD de la UE) sobre estos dos conjuntos de proyectos de cláusulas contractuales estándar y los respectivos actos de ejecución.
Para conseguir una mayor claridad en su pronunciamiento, el EDPB y el SEPD decidieron emitir dos dictámenes separados sobre estos dos conjuntos de CCE. Ambos dictámenes fueron aprobados en enero de 2021, si bien la aprobación y publicación de las decisiones por parte de la Comisión se retrasó hasta el mes de junio.

En ambos casos, el Comité se mostró, en general, favorable al contenido de las propuestas de decisión, aunque se hicieron numerosas observaciones y recomendaciones que, en general, fueron tenidas en cuenta por parte de la Comisión.

En particular, uno de los aspectos más controvertidos en relación con el dictamen sobre CCE para transferencias internacionales fue el de cómo tener en cuenta la experiencia previa de un importador y de un exportador a la hora de determinar si la legislación aplicable en un país de destino de los datos contiene puede impedir al importador cumplir con sus obligaciones de acuerdo con las cláusulas, en particular cuando se trata de legislaciones que prevén el acceso de las autoridades públicas a los datos transferidos.

vii. Dictamen conjunto CEPD-EDPS sobre el Reglamento de Inteligencia Artificial

La Comisión presentó una propuesta de reglamento que establece normas armonizadas para el uso de la Inteligencia Artificial (IA), y solicitó un dictamen conjunto del CEPD y el SEPD.

En su dictamen, aprobado en junio del año 2021, se expresa el acuerdo con el enfoque de riesgo seguido por la Comisión (que establece diversos niveles, con diversas exigencias), pero considera que los criterios de "riesgo para los derechos fundamentales", presente en varios lugares de la propuesta, debiera alinearse con el marco de protección de datos europeo.
Dos aspectos centrales del dictamen se refieren al riesgo de los sistemas de IA utilizados para el reconocimiento biométrico remoto en tiempo real en espacios accesibles al público y con la gobernanza del sistema de supervisión.

Respecto a los primeros, el CEPD y el SEPD consideran que, dado su riesgo extremadamente alto, estos usos deben prohibirse. Debe notarse que en la noción de reconocimiento biométrico se incluye no solo el reconocimiento facial, sino también el reconocimiento de huellas, de ADN, de voz o incluso del modo de caminar.
Respecto a los segundos, se entiende que el modelo diseñado por la propuesta no da cabida en la medida adecuada a las autoridades de protección de datos, por lo que solicita que sean consideradas como autoridades de supervisión de los sistemas de IA.

d) Recomendaciones

i. Sobre la base jurídica para el almacenamiento de datos de tarjetas de crédito con el único propósito de facilitar transacciones online

Algunos comercios online conservan por defecto el número de las tarjetas de crédito en las compras ocasionales para facilitar las futuras compras de los consumidores. Ante las

dudas sobre la base legal necesaria para este tratamiento, el CEPD clarifica en su recomendación que la única base legal adecuada para almacenar este dato es el consentimiento del comprador.

ii. Sobre el referencial de adecuación en el marco de la directiva sobre protección de datos en el ámbito policial y penal

En febrero de 2021 se ha aprobado el referencial de adecuación de la Directiva UE/680/2016. Este referencial se desarrolla sobre la base de un proyecto del GT29 para la Directiva UE/46/95, que fue retomado por el Comité Europeo de Protección de Datos.

El objeto del referencial, como sucede con el adoptado en relación con el RGPD, es desarrollar los criterios ya establecidos por la propia Directiva 680/2016 a los efectos de valorar la existencia de un nivel de protección adecuado en países terceros en el marco de la cooperación policial y judicial. El trabajo del grupo de transferencias internacionales del CEPD permite determinar la definición del concepto de adecuación y su aplicación en el ámbito de la mencionada Directiva UE/680/2016. Permite también determinar cuáles son los requisitos en materia de protección de datos que deben cumplir terceros Estados y organizaciones internacionales en el marco de la Directiva para que se puedan producir transferencias internacionales de datos personales a terceros Estados y organizaciones internacionales dentro del ámbito de la cooperación policial y judicial.

iii. Sobre medidas complementarias de las herramientas de transferencia para asegurar el cumplimiento del nivel UE de protección de los datos personales

Estas recomendaciones fueron inicialmente aprobadas a finales de 2020. Posteriormente, fueron sometidas a un proceso de consulta pública que recibió en torno a las 200 contribuciones por parte del sector empresarial, gobiernos y organizaciones de la sociedad civil.

El número de aportaciones y su variedad y alcance han hecho que el proceso de adopción de la versión final de las recomendaciones se haya prolongado a lo largo del primer semestre. La AEPD ha formado parte del equipo de redacción de esta última versión.

Las recomendaciones mantienen en lo sustancial el mismo formato y contenido que la versión inicial. No obstante, se han incluido algunas importantes modificaciones, entre las que se pueden destacar las siguientes:

- Se enfatiza la importancia de examinar las prácticas de las autoridades de terceros países en la valoración que lleve a cabo el exportador.
- Se precisa que la legislación de un tercer país de destino que permita a sus autoridades acceder a los datos transferidos, incluso sin la intervención del importador, puede también afectar a la eficacia de la herramienta de transferencia.
- Se contempla que el exportador pueda considerar en su evaluación la experiencia práctica del importador, entre otros elementos, a los efectos de valorar la aplicación real de la legislación que pueda resultar problemática a efectos de asegurar el nivel de protección de los datos transferidos.

Es importante destacar que estas Recomendaciones están en gran medida en línea con las Cláusulas Contractuales de la Comisión, ya que en los procesos de elaboración de ambos documentos existió estrecho contacto entre el CEPD y la Comisión.

e) Aprobación de códigos de conducta con validez en la Unión Europea

El CEPD aprobó durante el año 2021 los primeros códigos de conducta con validez en toda la Unión. La adhesión a un código de conducta ofrece importantes ventajas tanto para los interesados como para los responsables y encargados del tratamiento. Estos códigos ofrecen directrices detalladas que adaptan los requisitos legales a sectores concretos y favorecen la transparencia de las actividades de tratamiento. Los responsables y encargados del tratamiento también

pueden utilizar la adhesión a estos códigos como prueba palpable de que cumplen la normativa de la UE y como forma de reforzar su imagen pública en tanto que organizaciones que priorizan y se comprometen con la protección de datos en sus operaciones.

La entidad Scope Europe presentó su 'EU Data Protection Code of Conduct for Cloud Service Providers – EUCLOUD' ante la autoridad belga, mientras que la Cloud Infrastructure Service Providers – CISPE hizo lo propio ante la autoridad francesa. Ambas autoridades analizaron y aprobaron los códigos y solicitaron el dictamen del CEPD. Después de analizar los códigos en el subgrupo CEH, el plenario del CEPD adoptó un dictamen favorable en mayo de 2021.

En el Plenario de febrero de 2022 se adoptaron las Directrices en materia de Códigos de Conducta en las que se exige como requisito necesario para la aprobación de estos su validez general en toda la UE.

f) Decisión vinculante artículo 65. Whatsapp

Esta decisión fue solicitada por la autoridad irlandesa para resolver las discrepancias surgidas a partir de la presentación por parte de esta autoridad de una propuesta de decisión sobre la política de información en materia de protección de datos de WhatsApp (WA).

A esa propuesta de decisión se presentaron varias objeciones relevantes y motivadas por parte de diferentes autoridades.
La propuesta de decisión vinculante fue discutida a lo largo de 8 reuniones celebradas en los meses de junio y julio por el Subgrupo de Enforcement, coordinado por las autoridades de España y Holanda.

Como comentario previo, debe señalarse que este caso, como ya sucediera con la primera decisión vinculante del Comité sobre Twitter, ha evidenciado que estas decisiones conllevan una muy importante carga de trabajo tanto para el Secretariado del Comité (que es quien debe ocuparse de preparar la propuesta de decisión según las Reglas de Procedimiento del Comité) como para el Subgrupo que se ocupa de la valoración y presentación al Plenario y, en general, para las autoridades que participan en él. Una sobrecarga de trabajo que se agrava por lo reducido de los plazos previstos por el RGPD.
Esta constatación está llevando al Comité a plantearse posibles enfoques estratégicos que permitan reducir al mínimo imprescindible los casos que llegan al Comité para resolver conflictos entre autoridades mediante estas decisiones vinculantes.

Algunas de las objeciones planteadas fueron desestimadas por el Comité en su decisión, al considerar que no reunían los requisitos para ser consideradas "relevantes y motivadas" en los términos del artículo 4.24 RGPD.

En el caso de las que sí fueron consideradas como relevantes y motivadas y que, por tanto, fueron objeto de análisis en cuanto a su contenido por el Comité, la mayor parte de ellas fueron aceptadas y, por tanto, se requirió a la autoridad irlandesa para que modificara su decisión en tal sentido.
Estas modificaciones incluyeron considerar que se habían producido infracciones adicionales a las identificadas por la autoridad irlandesa en relación con los artículos 13.1.d, 5.1.a, 13.2.e, 14, 83.1, 83.2 y 83.3 RGPD.

Como consecuencia, también se requirió a la autoridad irlandesa que elevara sustancialmente la sanción impuesta a la compañía, para tener en cuenta las nuevas infracciones y la diferente valoración hecha de otras. En la decisión que la autoridad irlandesa adoptó para dar cumplimiento a la del Comité, la multa se elevó de los 50 millones de euros inicialmente propuestos a 225. Por otro lado, y también como consecuencia de la decisión del Comité, el plazo que se dio a Whatsapp para modificar la información de su política de privacidad y corregir así las infracciones detectadas se redujo de los seis meses que proponía la autoridad irlandesa a la mitad.

g) Decisión vinculante artículo 65. Facebook

Esta decisión es consecuencia de una solicitud presentada por la autoridad de supervisión de Hamburgo en el marco de un procedimiento de aplicación de medidas urgentes de los previstos en el artículo 66 RGPD (esta autoridad es la competente, según la legislación alemana, para supervisar a compañías que, como ocurre con Facebook o Google, tienen su sede principal en Alemania en esta ciudad – estado).

Tras la notificación de WhatsApp Ireland a los usuarios alemanes de sus nuevos Términos de Servicio y Política de Privacidad, y la extensión del plazo para que los usuarios dieran su consentimiento hasta el 15 de mayo de 2021, la autoridad alemana consideró que Facebook (la compañía a la que pertenece Whatsapp Ireland) ya estaría tratando datos de usuarios de WhatsApp que residen en Alemania para sus propios fines en algunos casos o que podría empezar a tratarlos de forma inminente en otros. La autoridad alemana considera que esos tratamientos para finalidades propias de Facebook vulneran varias disposiciones del RGPD, por lo que en mayo de 2021 adoptó medidas cautelares en aplicación del art. 66.1 RGPD.

En virtud de estas medidas provisionales se prohibía a Facebook, durante 3 meses (duración máxima de este tipo de medidas según el art. 66 RGPD), tratar datos personales de usuarios de Whatsapp residentes en Alemania que sean transferidos desde Whatsapp a Facebook. Esta prohibición alcanzaría, entre otras, a finalidades de cooperación con empresas del grupo, seguridad e integridad de Facebook y mejora de la experiencia de producto en Facebook.

El 7 de junio de 2021 la autoridad de Hamburgo solicitó al CEPD la adopción de una decisión vinculante urgente de conformidad con el artículo 66 (2) del RGPD, a fin de convertir en definitivas las medidas provisionales adoptadas, así como extenderlas territorialmente a toda la Unión.
Esta fue la primera ocasión en que el Comité ha debido pronunciarse sobre una decisión en aplicación del artículo 66.2 RGPD. Ello hizo que existieran muchas dudas tanto sobre el procedimiento a seguir como sobre las posibles formas de concluirlo. La razón de estas dudas hay que buscarla en que el artículo 66 RGPD solo regula algunos aspectos generales de estas decisiones, pero no entra en otros y tampoco aborda cuestiones de detalle.

El CEPD aprobó en su momento una Guía para la aplicación del artículo 66. Sin embargo, confrontada con su utilización en un caso real, la Guía demostró algunas limitaciones. Todo ello hizo que, aparte de las reuniones específicamente dirigidas a analizar la solicitud presentada por Hamburgo, el Comité debiera reunirse en dos ocasiones al nivel de Subgrupo de Asesoramiento Estratégico para resolver estas cuestiones antes de aplicarlas a este caso concreto.

La propuesta de decisión vinculante fue discutida de forma conjunta en este subgrupo y en el Subgrupo de Enforcement.

La conclusión finalmente alcanzada por el Comité fue que no disponía de información que le permitiera concluir que se daban las condiciones que demostrarían la existencia de una infracción y la urgencia de que el Comité actuara a través de una decisión dando continuidad a las medidas contra Facebook adoptadas por Hamburgo,.
Sin embargo, el Comité consideró que existiría una alta probabilidad de que Facebook estuviera tratando datos recibidos de Whatsapp para fines propios o del conjunto de empresas de la familia Facebook, tales como seguridad e integridad, o mejora de los productos. Por ello, el Comité decidió adoptar una decisión vinculante dirigida a la autoridad irlandesa (que sería la autoridad competente para la supervisión de Facebook y las compañías de su grupo en la UE) solicitándole que llevara a cabo, como cuestión prioritaria, una investigación para determinar si los tratamientos identificados por Hamburgo se estaban realmente llevando a cabo y, en caso afirmativo, cuál sería la base jurídica para hacerlo.
A los efectos de este informe cabe destacar que la AEPD se abstuvo en la votación final en el CEPD al entender que, al no cumplirse los requisitos

de existencia de una infracción y urgencia en la adopción de medidas por parte del Comité que establecen los apartados 1 y 2 del artículo 66, no existiría base para adoptar una decisión vinculante conteniendo otras medidas que, además, se dirigirían a otro sujeto distinto del afectado por la solicitud de decisión presentada por la autoridad de Hamburgo.

La autoridad irlandesa anunció que no seguiría la decisión del Comité, dado que ya estaba analizando las cuestiones a las que esta se refiere en el marco de otros procedimientos de investigación ya iniciados contra Facebook.

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

9.2.1.Grupo de Coordinación de la Supervisión SIS II

La Agencia ha continuado desarrollando las actividades programadas en el marco de su Plan de Actuación quinquenal de la Evaluación Schengen (resultado de la evaluación Schengen de España realizada en 2017 y presentado al Consejo de Ministros de la UE en junio de 2019).

En el marco de este plan, la Agencia ha asistido a las reuniones convocadas por la Dirección General de Coordinación de Políticas Comunes y Asuntos Generales de la UE del Ministerio de Asuntos Exteriores con el fin de continuar con la coordinación de las actuaciones de cara a la preparación de la próxima evaluación Schengen de España que tendrá lugar en marzo de 2022.

Por otra parte, el pasado 25 de noviembre pasado tuvo lugar la segunda reunión anual del Grupo de Coordinación de la Supervisión del SIS II (GCS).

En el marco de esta reunión, la Comisión Europea presentó su campaña de información pública sobre el ejercicio de los derechos de los afectados por los tratamientos de datos personales del sistema IT-SIS II. La campaña de información tuvo lugar en noviembre, previo a la negociación de la propuesta de reforma del sistema iniciada por la Comisión Europea que se lleva ahora cabo por Parlamento Europeo y Consejo. El GCS dio su opinión favorable a los entregables presentados por la Comisión Europea que incluían, entre otros, los folletos de información para el ejercicio de los derechos de acceso, rectificación y restricción de los afectados por los tratamientos de datos personales del sistema SIS. Entre estos entregables se encuentran también videos informativos y posters que se harán visibles en los puntos de acceso en frontera a lo largo de todo el territorio nacional. Se acordó también la celebración de ruedas de prensa informativas sobre los derechos de los ciudadanos en el marco SIS por parte de las autoridades nacionales de los Estados miembros.

La AEPD paso a informar inmediatamente de su participación en la evaluación Schengen de Bélgica.

La Comisión Europea informó después del estado en que se encuentra la negociación del nuevo marco legal SIS y del mecanismo de evaluación Schengen. El SCG SIS acordó elaborar una carta conjunta con el SCG VIS con el fin de manifestar su opinión sobre la actual reforma SIS en el marco del proceso legislativo en marcha con la participación del Consejo de Ministros de la UE y del Parlamento de la UE.

9.2.2.Grupo de Coordinación de la Supervisión VIS

El pasado 24 de noviembre de 2021, la Agencia Española de Protección de Datos participó en la segunda reunión anual del Grupo de Coordinación de Supervisión del VIS.

La reunión contó con la presencia la Comisión Europea y la delegada de protección de datos de EU-LISA y en ella se informó del estado de situación del sistema VIS así como del estado de

implantación del nuevo visado digital de la UE y el nuevo marco común de inspecciones del sistema IT VIS, actualmente en desarrollo.

El Grupo también revisó la elaboración del nuevo Plan Común de Inspecciones del sistema IT VIS y acordó que las diferentes delegaciones remitieran sus informes nacionales sobre el sistema VIS relativos al periodo 2019-2020 y los cuestionarios sobre el borrado avanzado de los datos del sistema de visados antes del 31 de diciembre de 2021.

Finalmente, el Grupo también aprobó su aportación a la carta conjunta entre el Grupo del VIS y del SIS-II al Consejo de Ministros de la UE y al Parlamento Europeo sobre la nueva propuesta del Reglamento UE relativa al establecimiento y operativa de la evaluación Schengen y del mecanismo para la aplicación del acervo Schengen, que derogará el actual Reglamento UE/1053/2013.

Debe señalarse también que la Agencia ha participado en dos evaluaciones Schengen durante 2021. Estas evaluaciones están previstas en la normativa reguladora del sistema Schengen e incluyen, entre otras áreas, una específica de protección de datos en la utilización del sistema de información asociado, el SIS II. La Agencia ha participado en las correspondientes a Francia y Holanda.

9.2.3.Grupo de Coordinación de la Supervisión de Eurodac (sistema de información huellas dactilares)

El Grupo de Coordinación de la Supervisión de Eurodac mantuvo 24 de noviembre de 2021 su segunda reunión anual.

En dicha reunión se hizo un seguimiento de la revisión que se está llevando a cabo del Reglamento Eurodac, así como de los trabajos desarrollados en el marco de la colaboración entre el Comité Europeo de Protección de Datos y la Agencia Europea de Derechos Humanos (FRA), para elaborar recursos que puedan ser utilizados por las autoridades nacionales en materia de interior, inmigración y asilo con el fin de informar a las personas sobre sus derechos en el marco Eurodac.

La Agencia Europea de Derechos Humanos considera que su participación en el proyecto ha finalizado una vez que las delegaciones han trasladado sus folletos en las distintas lenguas nacionales y se ha aprobado la publicación de los folletos en la página web del Supervisor Europeo de Protección de Datos.

Finalmente, se ha debatido sobre un posible modelo estructurado y armonizado de informe para las auditorias nacionales y sobre el futuro programa de trabajo para la supervisión del sistema de información de Eurodac.

9.2.4.Comité de Cooperación de Europol

El 23 de noviembre de 2021 la Agencia Española de Protección de Datos participó en la segunda reunión anual del Comité de Cooperación de Europol, autoridad común de protección de datos del sistema de información de Europol.

En la reunión se debatió el futuro informe del Comité en relación con la reforma del actual Reglamento Europol, que se lleva a cabo por la Unión Europea. El borrador de la reforma ya ha sido objeto de una opinión por parte del Supervisor Europeo de Protección de Datos.
Las delegaciones acordaron realizar una declaración del Comité de Cooperación sobre las fórmulas de cooperación Europol con los actores privados en materia de obtención de prueba electrónica en el ámbito del Reglamento Europol.

También se informó en dicha reunión sobre el estado del traslado de la supervisión al Supervisor Europeo de Protección de Datos.
Por último, se aprobó el programa de trabajo del Comité de Cooperación para el periodo 2021-2023, teniendo en cuenta el futuro traspaso de las funciones al Comité de Supervisión de la Coordinación del Comité Europeo de Protección de Datos.

9.2.5.Grupo de Coordinación de la Supervisión VIS

El 24 de noviembre de 2021 tuvo lugar la segunda reunión de 2021 del Comité de Supervisión Coordinada de los sistemas de información de la Unión Europea en el ámbito de la cooperación policial y judicial.

En la citada reunión, se aprobó el texto del cuestionario estándar para las delegaciones en relación con el uso del Sistema de Mercado Interior (IMI) por parte de las autoridades de protección de datos nacionales. El texto será de uso general por las delegaciones, y permitirá el ejercicio de los derechos de acceso, rectificación, borrado y oposición por parte de los afectados.

El Comité fue informado sobre la última auditoria del sistema de información de Eurojust y las actuaciones de las autoridades nacionales sobre este sistema de información, así como del intercambio de datos personales que se están realizando en otros ámbitos como el Consejo de Europa con el fin de fijar pautas adecuadas para el intercambio de datos personales entre las unidades de investigación conjunta y en el marco de los expedientes Eurojust.

Por último, se informó al Comité de los nombre y datos de contacto de los fiscales delegados del Reino de España en la Fiscalía Europea, EPPO, que se encuentra en fase de implantación.

9.3. Participación de la AEPD en otros foros internacionales

9.3.1.Comité Consultivo y Mesa de la Convención 108+ del Consejo de Europa

La Agencia Española de Protección de Datos forma parte del Comité Consultivo de la Convención 108 de Protección de datos personales del Consejo de Europa. El Estado español ha ratificado en fecha 28 de enero de 2021 el nuevo instrumento para la protección de datos personales del Consejo de Europa denominado Convenio 108+.

Hasta finales de 2021, un total de 43 Estados han firmado la convención, de los cuales 14 han procedido también a su ratificación.

El 28 de enero de 2021, El Consejo de Europa celebró el 40 aniversario de la Convención 108 de Protección de Datos Personales. Ese mismo día, la Conferencia de Autoridades Independientes de Protección de Datos de la República Federal de Alemania y de los Estados Federados celebró juntamente con la Presidencia Alemana de la Unión Europea el Día de la Protección de Datos. La Agencia Española de Protección de Datos presidió uno de los Talleres celebrados en este marco bajo el título: “Data Protection Day 2021 in Latin-America,40th Anniversary os data protection Convention 108”.

En el marco de estos órganos, han venido continuando los trabajos de elaboración del referencial de adecuación de la nueva Convención 108+ de Protección de Datos. Este marco de referencia es el instrumento que permite al Consejo de Europa decidir si un Estado candidato a la adhesión cumple con los criterios necesarios para ser considerado como un Estado de derecho y si tiene un marco legislativo adecuado de protección de datos y una adecuada implantación de dicho marco. De la mano de los expertos de la Universidad de Namur, se presentó el último borrador del referencial a discusión por parte de las delegaciones.
Estos trabajos han continuado con la elaboración de un cuestionario de evaluación de los candidatos a la adhesión a la Convención y su posterior examen periódico en relación con las condiciones que las partes han de cumplir para obtener y mantener la membresía en el marco de la Convención 108+.

Se ha trabajado también en la redacción de recomendaciones para el tratamiento de datos personales en las campañas políticas, adoptando un documento al respecto.

También, se presentaron los trabajos relativos a la elaboración de la opinión del Comité Consultivo sobre el borrador del Segundo Protocolo de la Convención de Budapest para la lucha contra la criminalidad, que finalmente fue aprobado dentro del ejercicio 2021.

El Comité trató también el asunto de la identidad digital, que permitirá desarrollar servicios públicos y privados y facilitará a los Estados miembros de la Convención tener un conocimiento más adecuado de sus censos de población. Esta identidad digital presenta, sin embargo, grandes retos en términos de protección de datos que fueron estudiados en varias reuniones por parte del Plenario y la Mesa del Comité.

El asunto de la protección de datos en el marco de las campañas electorales fue objeto también de atención por parte del Comité consultivo de la Convención 108. Se prestó especial atención al uso de las plataformas sociales como vía de transmisión de información electoral y fenómenos como las fake news.

El Comité adoptó también los principios de protección de datos elaborados para su inclusión en el borrador de la Convención para la lucha contra la manipulación de las competiciones deportivas y acordó su traslado al Comité de la Convención sobre la Manipulación de Competiciones Deportivas (Convención Macolin).
Por último, el Comité procedió a discutir el próximo programa de trabajo para el periodo 2022-2025.

La Agencia Española de Protección de Datos coopera también con otras instancias del Consejo de Europa y recibe puntual información sobre los trabajos de Comités ad hoc del Consejo como el CAHAI (Comité Ad Hoc sobre la Inteligencia Artificial) y otros comités especializados (Comité para la lucha contra la manipulación de las Competiciones Deportivas, Convención de Macolin; CAHENF(Comité para los Derechos del Niño); CDMSI (Comité Director sobre Medios y Sociedad de la Información) y DH-Bio (Comité de Bioética).

9.3.2. Asamblea Global de Privacidad (GPA)

La Asamblea Global de Privacidad (GPA por sus siglas en inglés), que agrupa a la mayoría de las autoridades de protección de datos a nivel global, celebró en octubre de 2021 su 43 conferencia anual organizada por la autoridad Mexicana INAI y realizada de forma telemática como consecuencia de la pandemia.

En la conferencia se aprobaron las siguientes resoluciones:

a) Resolución sobre la Dirección Estratégica de la Asamblea para el periodo 2021-23.

Tras el vencimiento de plan estratégico anterior definido para el periodo 2019-21 se han aprobado las directrices estratégicas para el trienio siguiente que vendrán marcadas por tres líneas de actuación:

- **1.**La promoción de la privacidad global en una era de digitalización acelerada y ello mediante la realización de trabajos que lleven hacia un entorno normativo mundial con normas claras y coherentes de protección de datos.

- **2.**La potenciación de la voz e influencia de la GPA mediante el desarrollo de una política digital de amplio espectro y el refuerzo de las relaciones con otros organismos y redes internacionales que promuevan la protección de datos y la privacidad

- **3.**El desarrollo de las capacidades de la GPA y de sus miembros mediante la formación y puesta en común de experiencias, estrategias y buenas prácticas; la cooperación entra las autoridades y la respuesta coordinada a los problemas de protección de datos y privacidad.

Estas tres líneas de actuación se van a desarrollar sobre los mismos tres pilares que sirvieron de base para el desarrollo del plan estratégico anterior:

1. Desarrollo de marcos y normas globales

2. Cooperación para la aplicación de la legislación

3. Ámbitos de interés político.

b) Resolución sobre el intercambio de datos para el bien público

Esta resolución se encuadra en el marco de la crisis sanitaria de la COVID-19 y la problemática surgida en torno a los nuevos tratamientos de datos personales como consecuencia de dicha crisis.

La resolución aboga por constituir un grupo de trabajo al efecto que se centre en identificar enfoques prácticos sobre la forma en que los datos personales pueden compartirse y utilizarse para permitir la innovación y el crecimiento, protegiendo al mismo tiempo los derechos individuales, promoviendo la confianza de los ciudadanos y proporcionado las mejores prácticas en el intercambio de datos en aras del bien público.

Para la consecución de dichos objetivos, el grupo de trabajo deberá colaborar con las partes interesadas correspondientes: redes internacionales, organizaciones de la sociedad civil y defensores de la privacidad para desarrollar respuestas proactivas en los problemas relativos al intercambio de datos personales como los que se dan por ejemplo en los pasaportes sanitarios, el seguimiento de la salud de los viajeros entrantes y los nacionales que regresan, las medidas de rastreo de contactos, el tratamiento de los datos de los niños o estudiantes en las tecnologías de aprendizaje electrónico.

c) Resolución sobre los derechos digitales de los niños

La resolución, que se hace eco de trabajos realizados por otros organismos como la ONU, el Consejo de Europa, la OCDE y otros grupos y redes internacionales sobre protección de datos y privacidad, establece una serie de recomendaciones sobre:

- **1.**Las condiciones y requisitos asociados a los derechos e información del niño en el entorno digital: transparencia, calidad y adaptación al menor en la adquisición del consentimiento
- **2.**La protección de las libertades fundamentales de los niños en el tratamiento de sus datos personales teniendo en cuenta la edad del menor, no sometiendo al menor a vigilancia sistemática, manipulación o influencia en su comportamiento, no discriminar al menor y posibilitar la libre expresión de sus opiniones en el entorno digital
- **3.**La explotación comercial de los datos no realizando usos secundarios con fines comerciales o publicitarios, aplicar el principio de minimización de datos y no proceder al perfilado con fines comerciales en general
- **4.**Aplicar la privacidad por defecto mediante un diseño amigable de privacidad, utilizar técnicas de cifrado, no aplicar técnicas de geolocalización, realizar evaluaciones de impacto, establecer marcos regulatorios, promover los códigos de conducta y estándares y fomentar la participación de los menores en función de su edad en el desarrollo de los sistemas de tratamiento
- **5.**Respecto a los tutores y a la educación digital fomentar la sensibilización, el compromiso y el control parental, promover las evaluaciones de impacto a la protección de datos en políticas públicas y fomentar la cooperación entre autoridades.

d) Resolución sobre el acceso gubernamental a los datos, la privacidad y el estado de derecho: principios para el acceso gubernamental a los datos personales en poder del sector privado con fines de seguridad nacional y pública

Esta resolución establece las condiciones que garanticen que cualquier tipo de acceso legítimo de las autoridades públicas con fines relacio-

nados con la seguridad nacional o la seguridad pública también contribuya a la preservación de la privacidad y el Estado de Derecho.

La condición básica para dicho acceso es la existencia de una base legal que autorice dicho acceso. Dicha base legal deberá estar a disposición del público, estar formulada con un lenguaje claro y comprensible, así como especificar de forma precisa el alcance y condiciones de dicho acceso. También deberá aplicarse el principio general de necesidad y proporcionalidad, el principio de transparencia y deberán reconocerse y garantizarse los derechos de interesado.

Las leyes que autoricen el acceso deberán regular cualquier uso posterior o transferencia ulterior para otros fines, al objeto de garantizar una protección continua. También, deberán considerar estas leyes la posibilidad de prever tanto una supervisión previa independiente como una supervisión retroactiva también realizada por un organismo regulador independiente. Finalmente, deberán estas leyes prever la posibilidad de recurso a dicho accesos por parte de los ciudadanos afectados.

Es importante subrayar que esta resolución se hace eco de los criterios establecidos en documentos adoptados por el CEPD a raíz tanto de la primera Sentencia Schrems, que determinó la anulación del esquema de Puerto Seguro como de la segunda, que acarreó la anulación del Escudo de Privacidad. En ese sentido, cabe considerar un logro positivo que la Asamblea, que cuenta entre sus miembros a representantes de todas las regiones del mundo, haya adoptado los estándares fijados en el ámbito de la Unión.

e) Resolución sobre el futuro de la Conferencia y del Secretariado

Esta resolución establece la nueva estructura de gestión y financiación en la que se van a desarrollar el futuro de la GPA.

Básicamente se va a separar los roles relativos al Secretariado y a la Presidencia de la GPA. Ya en 2019 se acordó proceder a dicha separación mediante un proceso de varias fases que arrancaría con la constitución de una Secretaría independiente de la Presidencia dotada de fondos propios y dependiendo de una autoridad miembro que rotaría cada 3-4 años ya que se ha considerado que por el momento no resulta oportuno una Secretaría con personalidad jurídica independiente. La Presidencia sería ostentada por otra autoridad miembro, en principio diferente de la asociada a la Secretaría, si bien podrían coincidir en una misma autoridad si ello fuera necesario.

Para la dotación de los fondos necesarios para la Secretaría se ha establecido un modelo de tasas cuya aprobación definitiva se decidirá en una fecha posterior según una propuesta de calendario.

Finalmente se mandata al Comité Ejecutivo para que, de acuerdo con el calendario previsto, establezca un Comité de Selección de la Secretaría que desarrolle nuevas modalidades de recaudación de honorarios, sobre unas bases de recaudación ya establecidas, y recomiende a un candidato anfitrión de la Secretaría.

10. La cooperación con Iberoamérica

28 enero

Se celebró un evento virtual relacionado con el Día Internacional de la Protección de Datos en Latinoamérica 2021, organizado por el Consejo de Europa y la Red Iberoamericana, cuyo objeto fue celebrar el 40º Aniversario del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, con las partes interesadas en protección de datos de América Latina.

10 febrero

Se reunió, en formato virtual, el Grupo Permanente de Autoridades de Protección de Datos de la RIPD en el que participa la AEPD. El objeto de la reunión fue explorar, dentro del marco legal nacional y regional vigente, las posibilidades de cooperación entre las Autoridades Iberoamericanas de Protección de Datos.

4 marzo

Webinario denominado "Estrategias de las autoridades de protección de datos para luchar con la violencia digital en Iberoamérica con un enfoque de género". El objetivo principal del webinario fue dar a conocer las acciones que estaba realizando la RIPD en el marco del proyecto "Apoyo para el fortalecimiento de la estrategia de lucha contra la violencia de género contra niñas, adolescentes y mujeres en internet, promovido e impulsado por algunas de las Autoridades de Protección de Datos miembro de la Red, como México (INAI, INFOEM, INFOCDMX e ITEI), España, Colombia, Perú, Uruguay, Costa Rica y Portugal) en estrecha colaboración con institutos de la mujer, ministerios de igualdad, policías y fiscalías. El evento, contó con la participación de la directora de la Agencia Española de Protección de Datos y su intervención se centró en el funcionamiento del Canal Prioritario de la AEPD para solicitar la eliminación urgente de contenidos sexuales y violentos en internet.

En el evento la RIPD aprobó la "Declaración de la Red Iberoamericana de Protección de Datos (RIPD) contra la Violencia Digital en mujeres y niñas" donde se fijó la posición de la Red y sus autoridades en relación con esta problemática y su contribución para luchar de forma efectiva contra la misma en Iberoamérica.

En la declaración se recogió que la violencia digital o ciberviolencia, entendida con el alcance en que ha sido definida por algunos de los textos anteriormente citados, constituye, entre otras, una flagrante vulneración del derecho fundamental a la protección de datos personales, en la medida en que las imágenes, los videos, las fotos y la voz constituyen datos personales que están siendo objeto de un tratamiento ilegítimo y, en esa medida, debe ser erradicada; se reconoce que, si bien es cierto que todas las personas estamos expuestas a sufrir violencia en el entorno digital y mediático, sin embargo, las mujeres, las niñas y las adolescentes están afectadas de forma desproporcionada por la hipersexualización a la que históricamente han estado sujetas y, por ello, sufren en mayor medida las consecuencias extremadamente graves de este fenómeno.

A ello, se une también el perjuicio que ocasionan los estereotipos y roles de género arraigados en los países Iberoamericanos. Se considera que los Estados Iberoamericanos, desde una perspectiva global y regional, deben avanzar en la tarea de incorporar en sus respectivos marcos legislativos y en sus políticas públicas las distintas formas de violencia digital contra las mujeres, niñas y adolescentes, estableciendo mecanismos de tutela judicial y administrativa y servicios de información y apoyo de sus derechos legales y a las ayudas disponibles; siendo necesaria una estrategia de responsabilidad compartida entre

todas las instituciones competentes para hacer frente a este fenómeno de forma efectiva.

Las legislaciones nacionales y las organizaciones implicadas deben trabajar conjuntamente desde un enfoque integral -preventivo y reactivo-, a fin de contar con los correspondientes canales de denuncia, atención inmediata a las víctimas y castigo a las personas responsables, con el fin de mitigar los efectos de la violencia digital. Los Estados Iberoamericanos deberán impulsar instrumentos y herramientas que permitan a sus respectivas Autoridades de Protección de Datos combatir de forma efectiva y urgente estas conductas en internet, dotándolas, si fuese necesario, del marco legal adecuado para ello, incorporando en las legislaciones nacionales la tipificación de este delito de violencia digital, además de los correspondientes recursos materiales y personales.

En este sentido, se considera una buena práctica el llamado "Canal Prioritario" creado por la Agencia Española de Protección de Datos para solicitar la eliminación urgente (en menos de 72 horas) de contenidos sexuales o violentos en internet contra mujeres, niñas y adolescentes. Para ello, se hace un llamamiento a la industria digital con el fin de generar un diálogo permanente que permita identificar áreas de colaboración y trabajo, que generen esfuerzos conjuntos contra la violencia digital y líneas de acción para mitigar los riesgos y atender los fenómenos derivados de ella, en conjunto con las autoridades competentes, la sociedad civil y la RIPD.

9 abril

El Comité Jurídico Interamericano (CJI), órgano consultivo de la Organización de Estados Americanos (OEA) aprobó, por unanimidad, los "Principios actualizados sobre la privacidad y la protección de datos personales, con anotaciones". Estos Principios vienen a reemplazar el documento anterior, de 2015, y constituyen un estándar normativo para los países del continente americano, en especial para aquellos que aún no poseen legislación en la materia, o que están en proceso de actualización de esta, con el objetivo de impulsar la armonización jurídica en el continente.

La Red Iberoamericana de Protección de Datos (RIPD), que participó de forma activa en el proceso de consulta abierto por el CJI, observa que esta iniciativa representa un aporte de la OEA en el escenario internacional de la protección de datos. Como novedades más significativas puede destacarse el aumento del número de principios, que pasan de 11 a 13, con la inclusión de la Autoridad de Protección de Datos (principio 13) y las excepciones (principio 12). Se amplía asimismo el alcance de los principios existentes. Así ha ocurrido, por ejemplo, con el principio de responsabilidad (principio 10) o el catálogo de derechos que incorpora: acceso, rectificación, cancelación, oposición y portabilidad (principio 8).

14 abril

Se celebró un seminario virtual en el ámbito de la Protección de datos ante la disrupción tecnológica. "Protección de Datos en entornos de computación en Nube" organizado por la RIPD en colaboración con la AECID. La presentación fue realizada por el Presidente de la RIPD junto con la Directora del Centro de Formación de la Cooperación Española en Cartagena de Indias.

Por parte de la AEPD, participó en dicho webinario el Coordinador de la Unidad de Apoyo y Relaciones Institucionales, quien moderó una mesa donde se debatió en torno a la localización de los datos personales en entornos de nueve o cloud y quién los protege y en la que participó el director de Seguridad y Cumplimiento de AWS América Latina de El Salvador, un representante de Cloud Security Alliance y un Abogado Experto en Protección de Datos de España.

En este seminario también se presentaron las recomendaciones RIPD para Protección de Datos en entornos de Computación en Nube.

La computación en la nube o cloud computing es una alternativa mediante la cual las organizacio-

nes pueden obtener a través de Internet diversos recursos y servicios informáticos. El uso de dichos servicios implica la realización de tratamientos de datos personales, ya que se realizan operaciones, entre otras, de almacenamiento, circulación (nacional o transfronteriza) o uso de esa información. Esta guía pretende establecer los principales aspectos que deben tenerse en cuenta cuando se utilizan servicios de computación en la nube desde la perspectiva de la normativa de datos personales. Como tal, aporta directrices para quienes contratan servicios de computación en la nube y para los que prestan este tipo de servicios.

La guía es complementaria de las recomendaciones y documentos que han emitido algunas autoridades de protección de datos y otras organizaciones. Se centra en los aspectos jurídicos que involucra el tratamiento de datos a través de servicios de computación en la nube y no en los aspectos tecnológicos. Para la elaboración de este documento se adoptaron los Estándares de protección de datos personales para los Estados Iberoamericanos de la RIPD como el referente para establecer los principios, términos, definiciones, etc. No obstante, no se transcriben todos los aspectos de los mismos, sino que se hace alusión a algunos de ellos. Por lo tanto, el documento debe leerse de manera conjunta e integral con los citados estándares.

Este texto no es un concepto legal, ni un artículo académico, ni constituye asesoría jurídica. Tampoco pretende ser un listado exhaustivo de recomendaciones específicas porque ello es un asunto interno que corresponde decidir a cada organización a la luz de los objetivos y la magnitud de cada proyecto que implique el uso de servicios de computación en la nube.

En cuanto a su contenido, identifica los principales actores en el tratamiento de datos personales en los servicios de computación en la nube (CEN), así como recomendaciones, entre las que se encuentran las de respetar las normas locales sobre tratamiento de datos personales, formalizar un acuerdo con el proveedor de servicios de computación en la nube que contenga los aspectos mínimos sobre tratamiento de datos personales, respetar las reglas sobre transferencias internacionales de datos, efectuar estudios de impacto a la protección de datos personales, incorporar la privacidad, la ética y la seguridad desde el diseño y por defecto, materializar el principio de responsabilidad proactiva, adoptar medidas para garantizar los principios relativos a las transferencias internacionales de datos personales mediante los servicios de CEN, garantizar los derechos de los titulares de los datos e implementar mecanismos efectivos para su ejercicio e incrementar la confianza y la transparencia con los titulares de los datos personales.

15 abril

Se celebró un seminario virtual en el ámbito de la Protección de datos ante la disrupción tecnológica organizado por la RIPD en colaboración con la AECID. “Protección de Datos e Inteligencia Artificial”. La apertura estuvo a cargo del Presidente de la RIPD y por parte de la AEPD, participó el Director de la División de Innovación y Tecnología.

Se presentaron las Recomendaciones de RIPD sobre inteligencia artificial publicadas en junio de 2019 en la página web de la RIPD cuyo objetivo es aportar algunas sugerencias a quienes desarrollan productos de Inteligencia Artificial (IA), con el fin de orientarlos para que desde el diseño del producto, se tengan en cuenta las exigencias de las regulaciones sobre tratamiento de datos personales. Por lo tanto, las mismas solo son aplicables a ese tipo de información –datos personales- y no a cualquier información en general.

Para la elaboración de este documento se adoptaron los Estándares de protección de datos personales para los Estados Iberoamericanos de la RIPD como el referente para establecer los principios, términos, definiciones, etc., por lo tanto, este documento debe leerse de manera conjunta, integral y armónica con los citados estándares. Tienen un enfoque preventivo y parten del supuesto de que la mejor forma de proteger los derechos humanos comprometidos en el tratamiento de datos personales es evitar su vulneración.

Para conocer los detalles de la implementación de algunas de estas recomendaciones, la RIPD ha elaborado unas directrices complementarias y más detalladas contenidas en el documento denominado "Orientaciones específicas para el cumplimiento de los principios y derechos que rigen la protección de los datos personales en los proyectos de Inteligencia Artificial".

Se recogen aspectos tales como el impacto de la regulación del tratamiento de datos personales en la inteligencia artificial y recomendaciones. Entre estas últimas cabe destacar el cumplimiento de las normas locales sobre tratamiento de datos personales; efectuar estudios de impacto de privacidad; incorporar la privacidad, la ética y la seguridad desde el diseño y por defecto; materializar el principio de responsabilidad activa (accountability); diseñar esquemas apropiados de gobernanza sobre tratamiento de datos personales en las organizaciones que desarrollan productos de IA; adoptar medidas para garantizar los principios sobre tratamiento de datos personales en los proyectos de IA; respetar los derechos de los titulares de los datos e implementar mecanismos efectivos para el ejercicio de los mismos; asegurar la calidad de los datos personales así como utilizar herramientas de anonimización e incrementar la confianza y la transparencia con los titulares de los datos personales.

1 julio

Se celebró el VIII Congreso Internacional de Protección de Datos organizado por la Superintendencia de Industria y Comercio (SIC) de Colombia. Participaron por parte de la AEPD el Coordinador de la Unidad de Apoyo y Relaciones Institucionales en el panel dedicado al Sandbox sobre tratamiento de datos personales y el Director de la División de Relaciones Internacionales en un panel dedicado a las cláusulas contractuales como mecanismo para realizar transferencias internacionales de datos personales.

9 septiembre

Se celebró el webinario organizado por el Foro de la Sociedad Civil de la RIPD denominado "Análisis de impacto en protección de datos personales y derechos humanos", la AEPD tuvo participación desde la Dirección de Innovación y Tecnología.

5 octubre

La AEPD y la Autoridad Nacional de Datos de Brasil suscribieron un memorándum de entendimiento para el desarrollo de actuaciones conjuntas dirigidas a promover la difusión y aplicación práctica de la normativa en materia de protección de datos. Ambos se comprometieron, entre otros aspectos, a impulsar mecanismos de cooperación técnica para intercambiar conocimientos y experiencias adquiridas, a fomentar la realización de estudios e informes en materia de protección de datos y a colaborar en la elaboración y difusión de materiales orientados a facilitar el cumplimiento normativo por parte de responsables y encargados del tratamiento en los diferentes sectores de actividad pública y privada

14 octubre

Se celebró el webinario en el marco de la actuación de la RIPD con la AECID sobre "Buen Gobierno, Ética e Integridad Púbica, la función de compliance en el sector público, la figura del Delegado de Protección de Datos (DPD) y los sistemas de certificación de personas". Por parte de la AEPD participó la Subdirección General de Inspección de Datos en una mesa donde se analizó el rol de los delegados de protección de datos en la administración pública.

18 octubre

La AEPD participó en la 43ª Global Privacy Assembly (GPA), organizada por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), que

se celebró del 18 al 21 de octubre en Ciudad de México bajo el título 'Privacy and Data Protection: a human-centric approach'. El coordinador de la Unidad de Apoyo y Relaciones Institucionales de la Agencia intervino en la sesión paralela IX, titulada 'Identidad digital: derechos digitales e impactos en la privacidad en una sociedad hiperconectada'.

22 octubre

Se celebró el XIX Encuentro de la Red Iberoamericana de Protección de Datos Personales (RIPD) en Ciudad de México en formato on line y en sesión cerrada. Participaron en el citado encuentro los 12 Miembros de la RIPD. En el acto se dio la bienvenida a la República Federativa de Brasil como nuevo miembro de la RIPD, por parte de la Secretaría de la RIPD se informó sobre el estado de situación de los nuevos desarrollos legislativos y a continuación intervino el INAI para informar que México había asumido la Presidencia de GPA y que su agenda de trabajo sería con la participación de la RIPD. Posteriormente se presentaron diferentes documentos: por el Presidente de la RIPD: las recomendaciones para el tratamiento de datos personales mediante computación en la nube, por parte del Vocal Coordinador de la Unidad de Apoyo y Relaciones Institucionales de la AEPD las recomendaciones para el tratamiento de datos personales sobre la salud en tiempos de pandemia y por parte de Bruno Gencarelli, Head of Internacional data flows and protección unit de la European Commission y de, Pablo Palazzi, experto argentino en protección de datos y autor del documento, sobre cláusulas contractuales.

También intervinieron Ana Brian Nougreres, Relatora Especial sobre el Derecho a la Privacidad enviando un mensaje sobre la importancia de la privacidad y Dante Negro, Director del Departamento de Derecho Internacional de la Organización de los Estados Americanos (OEA) y Mariana Salazar Albornoz, Miembro del Comité Jurídico Interamericano (CJI) de la OEA y Relatora para la Protección de datos personales y para el derecho internacional aplicable al ciberespacio que hablaron sobre los principios actualizados sobre la privacidad y la protección de datos personales del Comité Jurídico Interamericano de la OEA.

Después de estas intervenciones se propusieron proyectos a desarrollar por la RIPD a lo largo del año 2022 y finalmente, antes de la clausura, se aprobó la declaración final del evento.

En la declaración, se acordó reconocer el hecho de que, a pesar de las dificultades y limitaciones impuestas por la pandemia de COVID 19, la Red Iberoamericana de Protección de Datos haya seguido desarrollando sus actividades con el fin de alcanzar sus objetivos de promoción del derecho a la protección de datos en la región, agradeciendo especialmente los esfuerzos desplegados por el INAI para que pudiera llevarse a buen fin el Encuentro.

Así mismo, fueron reconocidos también los continuos avances del derecho a la protección de datos en la región, tal y como demuestran la aprobación de nuevas leyes al respecto en países donde anteriormente no existían y la actualización y modernización de otras leyes ya vigentes, así como el establecimiento o fortalecimiento de las correspondientes autoridades de supervisión. Se reconoce también, la importancia del Flujo Transfronterizo de los datos personales en el contexto de la economía digital y en el desarrollo económico y social de los países de la región, resaltando la necesidad de generar mecanismos y procedimientos que faciliten la realización de Transferencias Internacionales de datos personales y que, a su vez, generen garantías para asegurar el respeto a los principios que rigen el derecho fundamental a la protección de datos personales.

En este sentido, se recuerda que los Estándares de Protección de Datos Personales de la RIPD tienen como uno de sus objetivos facilitar el flujo de los datos personales entre los Estados Iberoamericanos y más allá de sus fronteras, con la finalidad de coadyuvar al crecimiento económico y social de la región. De esta manera, la elaboración de guías y modelos encaminados a promover el libre flujo de datos y una protección adecuada de los mismo son una prioridad para la RIPD y su propósito de fortalecer la protección de este derecho en los Estados Iberoamericanos; señalan, en materia de

Tratamiento Internacional de Datos Personales, las leyes de protección de datos personales de los Estados Iberoamericanos tienen como finalidad garantizar la continuidad del nivel de protección provisto en sus leyes cuando se produce una transferencia de datos personales a un tercer país que se considere con un nivel de protección no adecuado.

En esos casos, entre otras opciones, las Cláusulas Contractuales Modelos -CCM- son una alternativa que permite adherirse a un modelo preaprobado por la Autoridad competente, cumpliendo así las obligaciones legales en materia de Tratamiento Internacional de protección de datos personales, asegurando la continuidad en el nivel de protección de esos datos.

En este sentido, se exhorta a los Estados Iberoamericanos, así como a los empresarios, a tomar en consideración las Cláusulas Contractuales Modelos desarrolladas por la RIPD -CCM- para las transferencias internacionales, principalmente a las transferencias a jurisdicciones no adecuadas desde la óptica de la protección de datos. Estas cláusulas, permiten el cumplimiento de los principios de protección de datos personales y, a su vez, una alternativa económicamente viable para los empresarios que no tendrán que negociar acuerdos individuales, sino adherirse a un conjunto de cláusulas previamente aprobadas por la Autoridad.

También manifiestan que mediante servicios de computación en la nube (cloud computing) se realiza tratamiento de datos personales como almacenamiento, circulación (nacional o transfronteriza) o uso de esa información, se llama la atención en que el uso de estos servicios no debe ir en detrimento de la privacidad ni de la protección de datos personales en relación con otras formas de tratamiento de esa información.

Lo anterior, considerando que las normas de protección de datos personales son tecnológicamente neutras, esto es, aplican para cualquier tratamiento realizado, independientemente del medio físico o electrónico aplicado, implica que el tratamiento de datos personales sobre la salud en tiempos de pandemia no suspende el derecho fundamental a la protección de datos personales, cuya normativa permanece plenamente vigente y es de obligatorio cumplimiento para los responsables y encargados de dicho tratamiento.

Asimismo, consideran que la normativas de protección de datos de los Estados Iberoamericanos contienen disposiciones que permiten conciliar el respeto al derecho a la protección de datos con la adopción de las medidas necesarias para hacer frente a la pandemia¸ destacan la importancia de la reciente actualización de los principios sobre la privacidad y la protección de datos personales del Comité Jurídico Interamericano de la OEA, alineados con los Estándares de la Red Iberoamericana de Protección de Datos y, en particular, resaltando la inclusión del principio 13 relacionado con las Autoridades de Protección de Datos, que subraya la importancia de contar con órganos de supervisión independientes, dotados de recursos suficientes para el ejercicio de las funciones de inspección, control y vigilancia sobre el tratamiento de datos personales, así como promover el cumplimiento de las normas de protección de datos personales.

30 noviembre

El Presidente del Consejo para la Transparencia de Chile, Bernardo Navarrete Yáñez, realizó una visita institucional a la Agencia Española de Protección de Datos. Durante la visita, se realizaron distintas sesiones informativas relacionadas con las principales áreas de actividad de la AEPD, el marco normativo de protección de datos -con especial énfasis en el principio de responsabilidad activa y la protección de datos desde el diseño y por defecto- y se presentaron diferentes iniciativas, recursos y materiales desarrollados por la Agencia, como las guías y herramientas para facilitar el cumplimiento de la normativa de protección de Datos.

9 diciembre

Se celebró el webinario "Pasaporte verde COVID-19: Riesgos en la privacidad y protección de datos" organizado por la Fundación Datos Protegidos en el marco de la planificación del Foro de la Sociedad Civil de la Red Iberoamericana de Protección de Datos. El evento contó con la participación del Director de la División de Relaciones Internacionales representando a la AEPD.

14 diciembre

Se celebró el webinario desarrollado por la RIPD en el marco de colaboración con la AECID "La privacidad desde el diseño" en el que participó, por parte de la AEPD, el Director de la División de Innovación y Tecnología en el panel "La privacidad desde el diseño: una visión desde su implementación, puesta en marcha y cumplimiento de la ley".

LA AGENCIA EN CIFRAS

1. Inspección de datos

1. 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 tutela o las de investigación oportunas, y cuando procede, instruye los procedimientos sancionadores para proponer a la Directora la adopción de la resolución que corresponda.

Las reclamaciones pueden recibirse directamente a 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 trabajos en los que la Autoridad de Control (AC) del EEE ha decidido iniciar una actuación por propia iniciativa y la AEPD se encuentra afectada. Por ello, la SGID también evalúa su participación en la iniciación de procedimientos de cooperación de casos transfronterizos en los que otras AC nos comunican una reclamación.

Bien como consecuencia de las reclamaciones, bien por propia iniciativa, la Directora de la Agencia puede determinar la apertura de actuaciones de investigación para alcanzar una mejor y más concreta determinación de las conductas o hechos que puedan infringir la normativa de protección de datos.

A todo ello hay que sumar la realización de auditorías de grandes sistemas de carácter europeo en los que la Agencia tiene un papel de supervisor, como pueden ser el Sistema de Información Schengen (SIS) o el Sistema de Información de Visados de corta duración (VIS), por citar algunos.

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 seguridad en materia de protección 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 se juzga pertinente, se propone a la Directora que sean trasladadas a la Subdirección General de Inspección de Datos, donde se valora el inicio de una posible investigación. Dada la importancia que tienen, se analizan de manera independiente bajo el epígrafe de notificaciones de brechas de seguridad. Se contabilizan en este apartado únicamente aquellas en las que la SGID determina que procede su evaluación y posible investigación.

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

Tipo de entrada	2020	2021	% relativo	Δ% anual
Reclamaciones presentadas en la AEPD	10.324	13.905	95%	35%
Casos transfronterizos procedentes de otras AC del EEE	784	581	4%	-26%
Propia iniciativa de la AEPD (excl. brechas)	26	9	0%	-65%
Notificaciones de brechas de seguridad trasladadas a la SGID	81	76	1%	-6%
TOTAL	**11.215**	**14.571**	**100%**	**30%**

Se puede observar un fuerte incremento respecto al año 2020 impulsado por el aumento del número de reclamaciones recibidas ante esta Agencia, que alcanzó una cifra sin precedentes en la historia de la AEPD.

En 2021 la tasa de reclamaciones resueltas frente a reclamaciones recibidas se ha mantenido ligeramente superior el 100%, lo que pone en valor el compromiso de la Agencia con la resolución de las reclamaciones en este contexto de fuerte aumento de la entrada. El número de reclamaciones resueltas ha sido también extraordinario en la historia de la Agencia, y un 35% superior al año anterior. En el Anexo B de esta sección se analiza con más detalle cómo se correlacionan las mejoras de productividad con la implantación del teletrabajo en la Agencia. En la siguiente tabla se pueden consultar las cifras relacionadas con la tasa de resolución de reclamaciones:

Tasa de resolución de reclamaciones	2020	2021	Δ% anual
Reclamaciones resueltas en el año*	10.443	14.098	35%
Reclamaciones pendientes de resolver al finalizar el año	3.709	3.516	-5%
Tasa de reclamaciones resueltas vs. recibidas en el año**	101%	101%	0%

2. Resoluciones

Uno de los indicadores que muestran la actividad que se realiza desde la Subdirección General de Inspección de Datos es el número de resoluciones que se emiten. Los diferentes conceptos en los que se clasifican las entradas, detallados en el apartado anterior, pueden dar lugar a diferentes 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, paralelamente, en una reclamación pueden aparecer múltiples reclamados, dando origen a múltiples procedimientos y, por lo tanto, a diferentes resoluciones.

Resoluciones en fase de Análisis previo de admisibilidad 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 normative, se inadmitirá y, en caso contrario, prosperará a la siguiente fase. El porcentaje de inadmisiones en esta fase se encuentra en torno al 60% de los casos, como muestra la siguiente tabla:

Tipo de resultado	2020	2021	% relativo	Δ% 2018/19
Resoluciones tras la fase de Análisis de la reclamación	**5.671**	**8.058**	**61%**	**42%**
Inadmisiones a trámite*	5.522	7.854	60%	42%
Competencia de otras AC nacionales (CGPJ, AC auton.)*	149	204	1%	37%
Resoluciones en otras fases	**4.396**	**5.053**	**39%**	**15%**
TOTAL	**10.067**	**13.111**	**100%**	**30%**

** Incluyen reclamaciones relacionadas con el ejercicio de derechos*

Resoluciones en otras fases

: Con la entrada en vigor del RGPD y, fundamentalmente, 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 consiguen 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 2021, tras haber procedido al traslado de la reclamación, se dictó resolución finalizando su tramitación en más del 73% de los casos, dando así una respuesta más rápida a los reclamantes que la que se conseguía con la normativa anterior. Por su parte, la Agencia consideró la existencia de responsabilidades que debían ser depuradas en procedimiento sancionador en el 12% de los casos.

En la siguiente tabla se muestra la distribución completa de resoluciones según la fase del procedimiento de Inspección en que se alcanza la finalización del caso.

Tipo de resultado	2020	2021	% relativo	Δ% 2018/19
Resoluciones tras Traslado*	**3.405**	**3.679**	**73%**	**8%**
Respuesta satisfactoria tras traslado al responsable o enc.	2.157	2.421	48%	12%
Archivo por ser plena competencia de otra AC del EEE	414	361	7%	-13%
Archivo provisional actuando como AC interesada en el EEE	451	304	6%	-33%
Archivo por otros motivos tras traslado	383	593	12%	55%
Resoluciones tras Actuaciones previas de Investigación	**347**	**438**	**9%**	**26%**
Archivo de actuaciones previas de investigación	347	438	9%	26%
Resoluciones tras procedimiento de Ejercicio de derechos	**251**	**351**	**7%**	**40%**
Resuelto en el procedimiento de ejercicio de derechos	251	351	7%	40%

** Incluyen reclamaciones relacionadas con el ejercicio de derechos*

Tipo de resultado	2020	2021	% relativo	Δ% 2018/19
Resoluciones tras procedimiento Sancionador	**393**	**585**	**12%**	**49%**
Resuelto en procedimiento sancionador - Multa	163	264	5%	53%
Resuelto en procedimiento sancionador - Apercibimiento	163	222	4%	36%
Resuelto en procedimiento sancionador - Archivo	58	99	2%	71%
TOTAL	**4.396**	**5.053**	**100%**	**15%**

** Incluyen reclamaciones relacionadas con el ejercicio de derechos*

Porcentaje del tipo de derecho en Procedimientos de derechos resueltos en 2021*	%
Acceso	54%
Supresión	47%
Rectificación	3%
Oposición	2%
Limitación del tratamiento	1%
Decisión automatizada	0%
Portabilidad	0%

** Un procedimiento puede resolver más de un único derecho.*

Tiempos medios de resolución

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

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. Debe tenerse en cuenta que el artículo 65.5 de la LOPDGDD establece un plazo de 3 meses para este concepto.

Tiempos medios de resolución en fase de Análisis (en días)	2020	2021	Δ% anual
Resoluciones tras el Análisis de la reclamación*	25	26	3%
TOTAL	**25**	**26**	**3%**

** Incluyen reclamaciones relacionadas con el ejercicio de derechos*

En la fase de traslado, el tiempo medio responde al tiempo desde que tiene entrada la reclamación hasta que se firma la resolución de inadmisión, lo que ocurre tras el traslado al responsable y el análisis de la respuesta recibida.

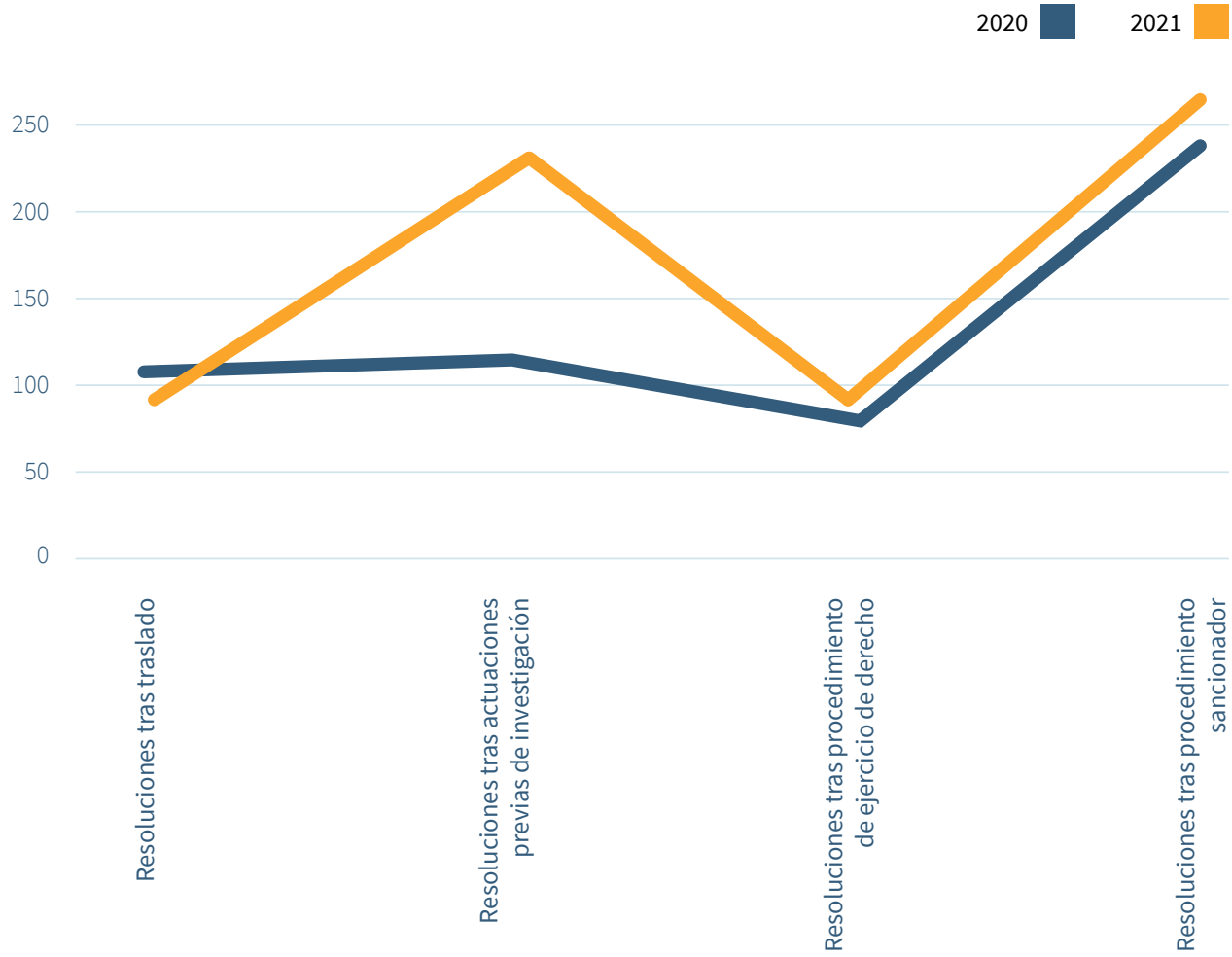
A su vez, los tiempos de resolución en actuaciones previas de investigación, en procedimientos de ejercicio de derechos y en procedimientos sancionadores, se contabilizan desde la fecha de admisión a trámite de la reclamación hasta que se firma la resolución.

El tiempo medio global de resolución ha disminuido en 10 días con respecto al año anterior, continuando la tendencia de años precedentes, y a pesar 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.
Las cifras que se muestran a continuación dan una perspectiva del total de las actuaciones realizadas en

Tiempos medios de resolución según la fase del procedimiento (en días)	2020	2021	Δ% anual
Resoluciones tras traslado*	110	87	-21%
Resoluciones tras actuaciones previas de investigación	228	233	2%
Resoluciones tras procedimiento de ejercicio de derechos	79	88	11%

Tiempos medios de resolución según la fase del procedimiento (en días)	2020	2021	Δ% anual
Resoluciones tras procedimiento sancionador	233	255	10%
TIEMPO MEDIO	**129**	**119**	**-7%**

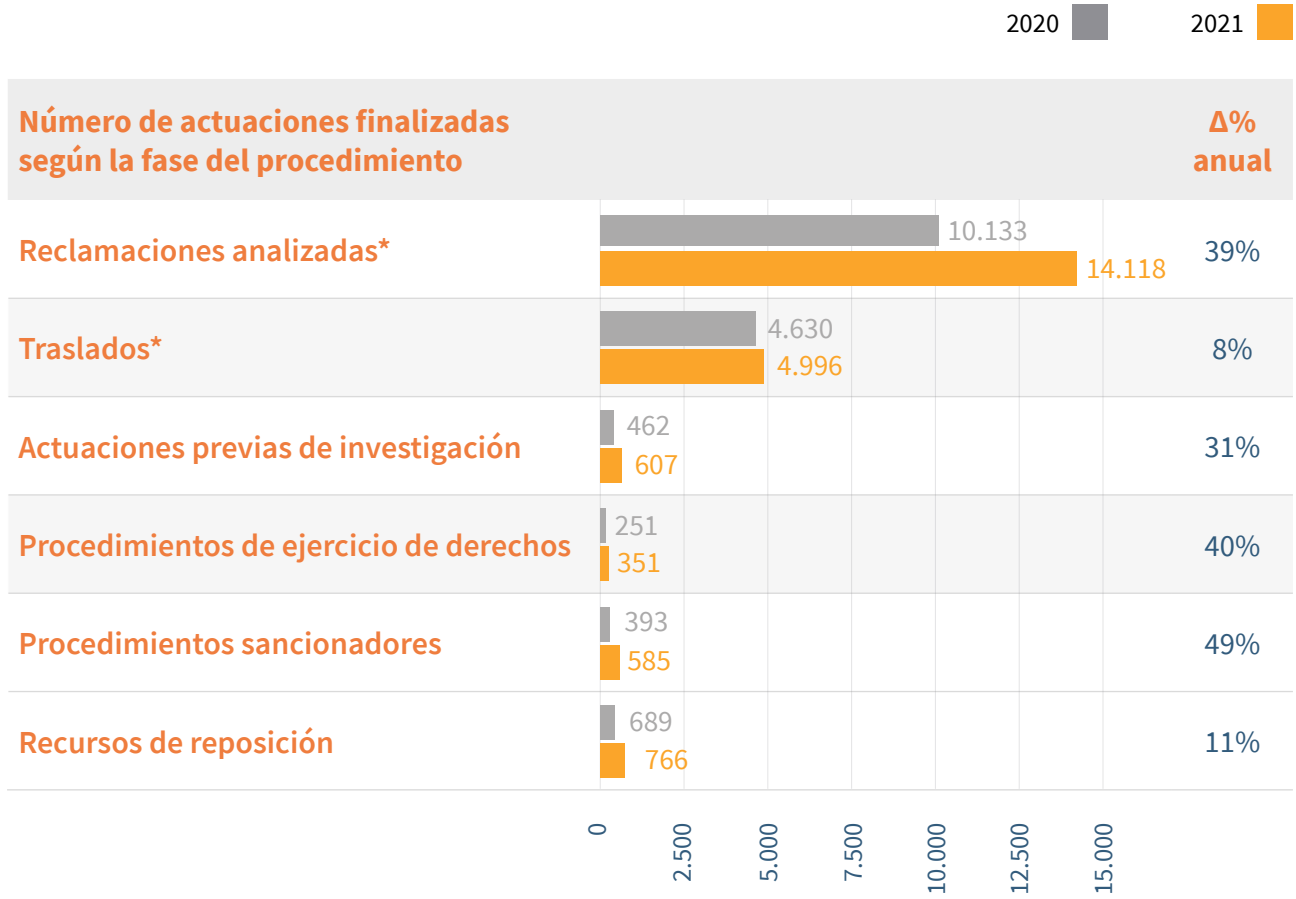
** Incluyen reclamaciones relacionadas con el ejercicio de derechos*



3. Actuaciones realizadas

la Subdirección General de Inspección de Datos que finalizan una fase del procedimiento administrativo, pero que no necesariamente lo concluyen y, por lo tanto, no dan lugar a resoluciones. Un ejemplo de ello sería una actuación previa de investigación que da lugar a un procedimiento sancionador; esta actuación no genera una resolución y, por lo tanto, no aparece detallada en el apartado anterior, pero, sin embargo, sí implica un trabajo que es el que se indica en este epígrafe. En el caso de procedimientos de ejercicio de derechos, sancionadores o recursos de reposición, que siempre ponen fin al procedimiento administrativo y producen, por tanto, una resolución, las cifras son coincidentes con las dadas en el apartado anterior.

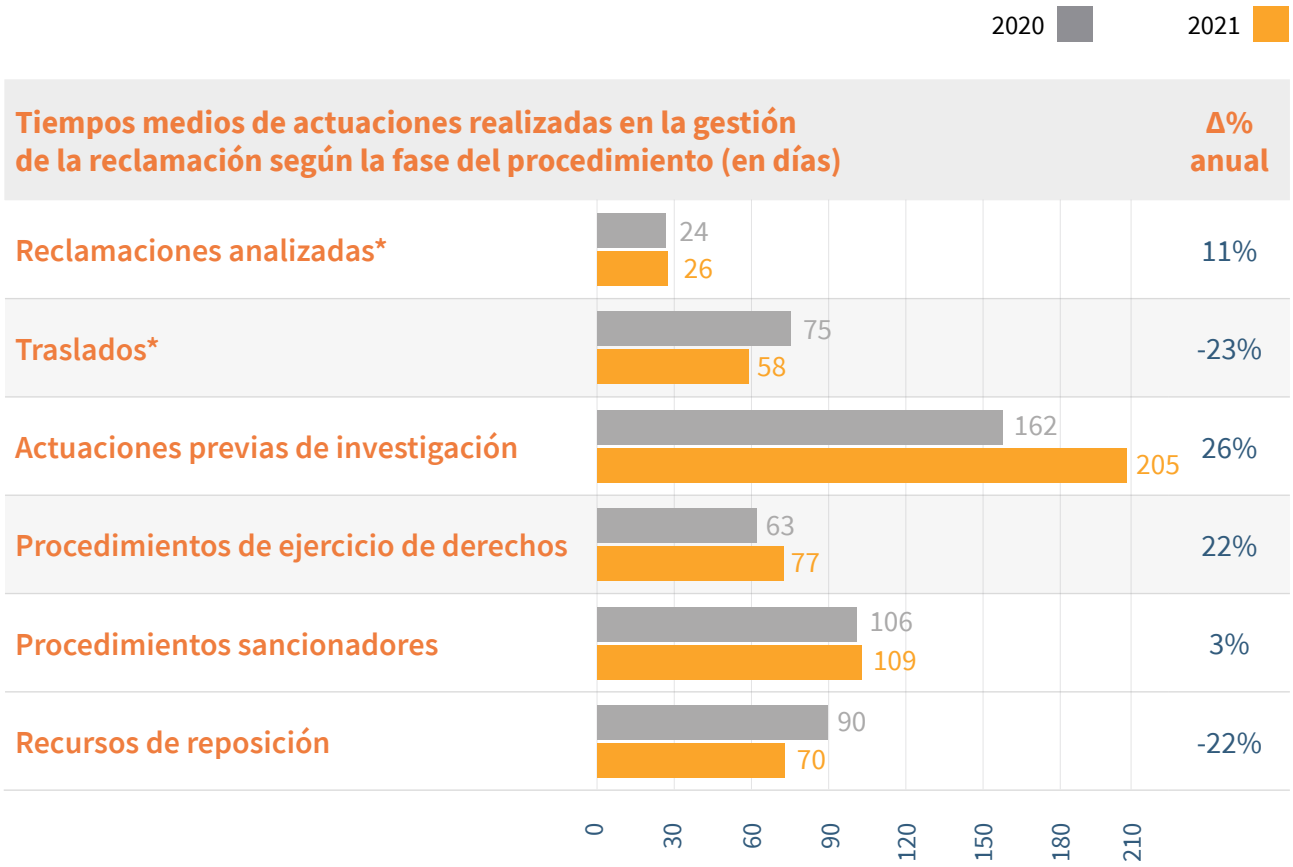
Se puede observar un aumento de actuaciones en todas las fases, consistente con el importante aumento de reclamaciones recibidas en 2021. Se debe puntualizar que el número de reclamaciones analizadas en la fase previa de admisibilidad puede oscilar frente al número de reclamaciones presentadas en el año, puesto que es un trámite que tiene una duración media de 26 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 de año.
Los tiempos que aparecen en este apartado miden los tiempos medios de actuaciones de cada una de las



** Incluyen reclamaciones relacionadas con el ejercicio de derechos*

Tiempos medios de tramitación

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.



TOTAL	**47**	**43**	**-8%**

** Incluyen reclamaciones relacionadas con el ejercicio de derechos*

4. Recursos

Los recursos interpuestos frente a resoluciones de los procedimientos realizados por la Subdirección General de Inspección de Datos se muestran a continuación, según hayan sido de reposición, extraordinarios de revisión, o contencioso-administrativos.

Tipo de recurso	2020	2021	Δ% anual
Recursos de reposición	674	795	18%
Recursos extraordinarios de revisión	7	7	0%
Recursos contencioso-administrativos	63	118	87%
TOTAL	**744**	**920**	**24%**

El aumento en recursos contencioso-administrativos recibidos no resulta sorprendente si se correlaciona con el aumento en el número de resoluciones emitidas por la Agencia, así como en la mayor complejidad de los procedimientos y gravedad de las sanciones impuestas, a lo que posteriormente se hará referencia.

Los recursos de reposición y revisión resueltos anualmente por la AEPD se muestran en la siguiente tabla:

Tipo de recurso	2020	2021	Δ% anual
Recursos de reposición	689	766	11%
Recursos extraordinarios de revisión	8	7	-13%
TOTAL	**697**	**773**	**11%**

5. Clasificaciones

Reclamaciones planteadas con mayor frecuencia

Se muestran las 10 áreas de actividad con mayor número de reclamaciones recibidas en 2021:

Reclamaciones planteadas con mayor frecuencia	2020	2021	% relativo	Δ% anual
TOP 10	**7.727**	**10.840**	**78%**	**40%**
Servicios de Internet	1.602	2.220	16%	39%
Videovigilancia	1.189	1.736	12%	46%
Publicidad (excepto spam)	681	1.528	11%	124%
Ficheros de morosidad	1.510	1.284	9%	-15%
Reclamación de deudas	656	859	6%	31%
Administración pública	503	740	5%	47%
Sanidad	388	680	5%	75%
Comercios, transporte y hostelería	405	663	5%	64%
Entidades financieras/acreedoras	437	643	5%	47%
Publicidad a través de e-mail o teléfono móvil	356	487	4%	37%
Otros	**2.597**	**3.065**	**22%**	**18%**
TOTAL	**10.324**	**13.905**	**100%**	**35%**

Áreas más frecuentes en procedimientos sancionadores

Se muestran las 10 áreas de actividad con mayor número de procedimientos sancionadores finalizados en 2021:

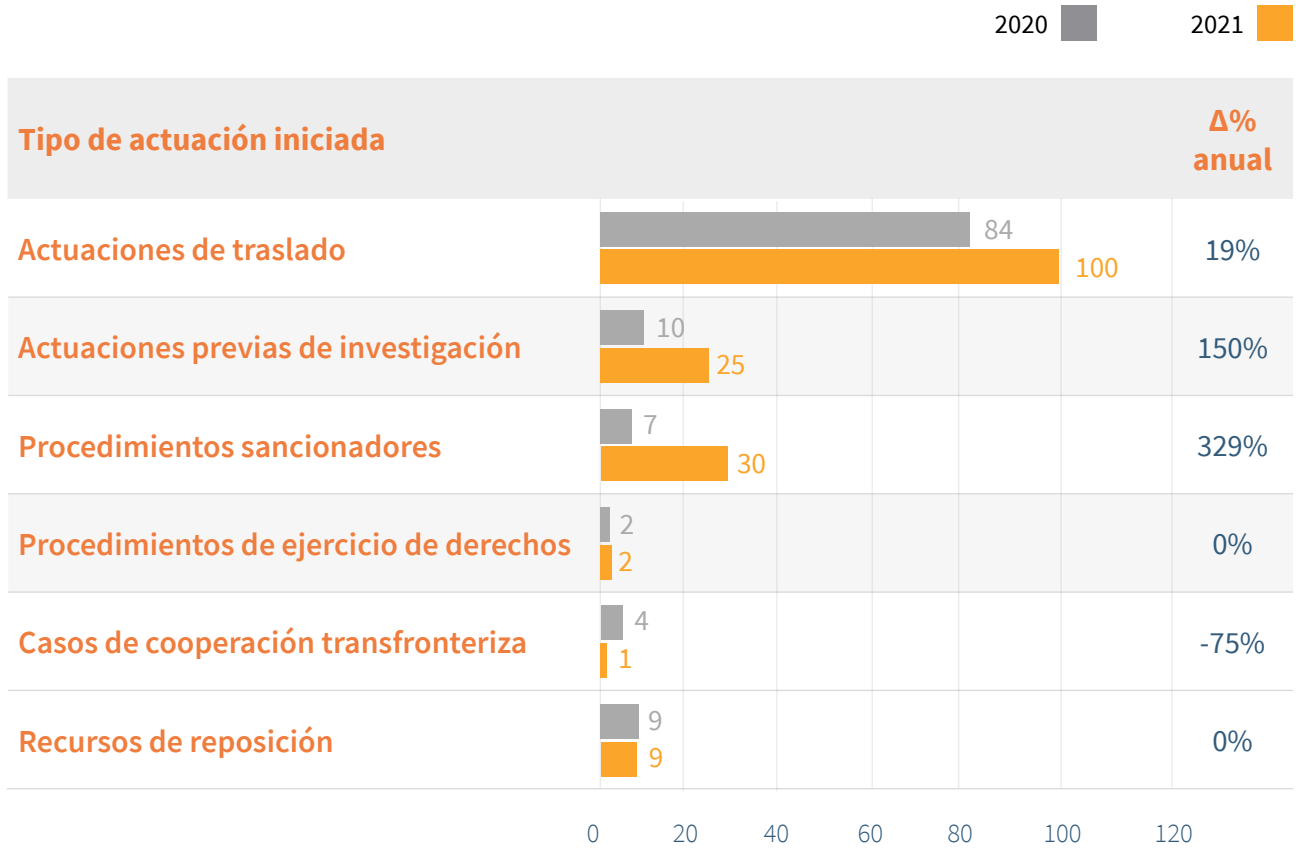
Grupo de actividad	2020	2021	% relativo	Δ% anual
TOP 10	**317**	**504**	**86%**	**59%**
Videovigilancia	94	147	25%	56%
Servicios de Internet	73	128	22%	75%
Publicidad a través de e-mail o teléfono móvil	17	51	9%	200%
Administración Pública	39	49	8%	26%
Asuntos laborales	13	26	4%	100%
Publicidad (excepto spam)	8	25	4%	213%
Comercios, transporte y hostelería	23	24	4%	4%
Contratación fraudulenta	14	19	3%	36%
Telecomunicaciones	27	18	3%	-33%
Quiebras de seguridad	9	17	3%	89%
Otros	**76**	**81**	**14%**	**7%**
TOTAL	**393**	**585**	**100%**	**49%**

Reclamaciones relacionadas con la pandemia de COVID-19

2020 y 2021 han sido años marcados por la crisis sanitaria ocasionada por la pandemia. En la siguiente tabla se muestra la cifra de reclamaciones:

Tipo de entrada	2020	2021	Δ% anual
Reclamaciones recibidas e iniciativa propia	241	233	3,4%

Las cifras que se muestran a continuación dan una perspectiva del total de actuaciones realizadas en la Subdirección General de Inspección de Datos relacionadas con la COVID-19, con un aumento importante en la instrucción de procedimientos sancionadores:



6. Ámbito transfronterizo (EEE)

La aplicación del RGPD desarrolla en su capítulo VII los mecanismos de cooperación entre autoridades de control del Espacio Económico Europeo, donde es de plena aplicación el Reglamento.

Casos transfronterizos con participación de la AEPD

En los casos con componentes transfronterizos que afectan a ciudadanos o a establecimientos de responsables en España, la AEPD 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.

Papel de la AEPD	2020	2021	Δ% anual
Nuevos casos liderados como autoridad principal	17	16	-6%
Nuevos casos en cooperación como autoridad interesada	451	304	-33%
TOTAL	**468**	**320**	**-32%**

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 recibidos por la AEPD, así como los proyectos de decisión analizados y participados por la AEPD.

Tipo de entrada	2020	2021	Δ% anual
Casos transfronterizos procedentes de otras AC	784	581	-26%
Solicitudes de asistencia de otras AC	207	274	32%

Tipo de entrada	2019	2020	Δ% anual
Consultas de otras AC en procedimientos transfronterizos	111	102	-8%
Proyectos de decisión de casos en los que la AEPD participa*	107	113	6%
Operaciones conjuntas donde la AEPD participa	1	0	-100%
TOTAL	**1.210**	**1.070**	**-12%**

** 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.*

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.

Tipo de notificación	2020	2021	Δ% anual
Casos transfronterizos compartidos de otras AC	40	30	-25%
Solicitudes de asistencia de otras AC	90	88	-2%
Consultas a otras AC en procedimientos transfronterizos	7	18	157%
Proyectos de decisión de casos liderados por la AEPD*	24	23	-4%
TOTAL	**161**	**159**	**-1%**

** Los proyectos de decisión emitidos por la AEPD suponen el trabajo subsiguiente de negociación y consenso entre todas las autoridades participantes y requieren una gran cantidad de recursos y de esfuerzo.*

7. Multas

Evolución de las multas impuestas

Las siguientes cifras hacen referencia a las sanciones impuestas en resolución definitiva, con independencia de su estado de ejecución y recaudación:

Evolución de las multas impuestas	2020	2021	Δ% anual
Número de multas	167	258	54%
Importe total	8.018.800	35.074.800	337%

El incremento en las cifras de multas impuestas guarda relación con el mayor número de procedimientos sancionadores resueltos y también denota un incremento en la envergadura y complejidad de los casos derivado a su vez de las magnitudes de los tratamientos de datos investigados. Buena muestra de ello da el hecho de que este año se hayan impuesto varias multas por un importe superior al millón de euros, de las cuales cinco son ya ejecutivas, y que el importe medio de las multas se haya triplicado con respecto al año anterior.

Las multas superiores al millón de euros en resoluciones que han devenido firmes y ejecutivas se detallan a continuación:

Responsable	Infracción	Multa
BANCO BILBAO VIZCAYA ARGENTARIA, S.A.	Artículo 13 del RGPD Artículo 14 del RGPD Artículo 14 del RGPD	5.000.000 €
VODAFONE ESPAÑA, S.A.U.	Artículo 48.1.b) de la LGT Artículo 21.1 de la LSSI Artículo 28 del RGPD Artículo 44 del RGPD	8.150.000 €
EDP ENERGIA, S.A.U.	Artículo 13 del RGPD Artículo 25 del RGPD	1.500.000 €
EDP COMERCIALIZADORA S.A.	Artículo 13 del RGPD Artículo 25 del RGPD	1.500.000 €

Responsable	Infracción	Multa
MERCADONA S.A.	Artículo 12 del RGPD Artículo 13 del RGPD Artículo 25 del RGPD Artículo 35 del RGPD Artículo 5.1.c) del RGPD Artículo 6 del RGPD Artículo 9 del RGPD	2.520.000 €

Áeras con mayor importe global de multas

La siguiente tabla desglosa las 6 áreas de actividad con mayor importe en sanciones en 2021:

Importe de multas en euros según el sector de actividad	2020	2021	% relativo	Δ% anual
Seis sectores con mayor actividad en 2021	**7.058.300**	**31.911.100**	**91%**	**352%**
Publicidad (excepto spam)	17.700	8.659.200	25%	48822%
Telecomunicaciones	1.009.000	6.500.000	19%	544%
Entidades financieras/acreedoras	5.045.000	6.243.000	18%	24%
Ficheros de Morosidad	387.000	4.209.000	12%	988%
Contratación fraudulenta	559.000	3.674.000	10%	557%
Asuntos laborales	40.600	2.625.900	7%	6368%
Otros	**960.500**	**3.163.700**	**9%**	**229%**
TOTAL	**8.018.800**	**35.074.800**	**100%**	**337%**

Anexo A: Datos del Canal Prioritario

En 2019 la AEPD creó un sistema específico para perseguir la difusión ilegítima de contenidos especialmente sensibles de menores y otros colectivos vulnerables, 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, facilitando un medio de contacto basado en un formulario abierto, sin necesidad de presentar certificado digital.

Entradas a través del Canal Prioritario			
Tipo de entrada	**2020**	**2021**	**Δ% anual**
Reclamaciones presentadas ante la AEPD por el Canal Prioritario	184	162	-12%
Comunicaciones del canal de menores (14-18 años)	174	215	24%
TOTAL	**358**	**377**	**5%**

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 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 contenidos especialmente sensibles.

La siguiente tabla muestra las entradas que, después de dicho análisis, fueron canalizadas por el canal urgente.

Tipo de entrada	**2020**	**2021**	**Δ% anual**
Reclamaciones recibidas por el Canal Prioritario	29	16	-45%
Reclamaciones recibidas por canales ordinarios	5	8	64%
Iniciativa Propia	0	0	0%

Tipo de entrada	2020	2021	Δ% anual
Comunicaciones del canal de menores (14-18 años)	15	5	-67%
TOTAL	**49**	**29**	**-41%**

Intervenciones realizadas con carácter de urgencia

Cuando se determina la naturaleza especialmente sensible de los datos personales divulgados y la afectación grave a la intimidad de las personas, 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 proveedores de servicios correspondientes la retirada de los contenidos sensibles con la mayor inmediatez posible. 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. Las intervenciones que no han resultado eficaces demuestran las dificultades en la retirada de contenidos cuando los responsables se localizan en terceros países.

Tipo de intervención	2020	2021	Δ% anual
Intervenciones con carácter de urgencia para la retirada de contenidos	29	31	7%
Intervenciones con carácter de urgencia para la retirada de contenidos que han resultado eficaces	25	25	0%

Anexo B: Mejora Productividad. Comparación con la implantación del Teletrabajo.

La productividad de la actividad global de la Subdirección General de Inspección de Datos se puede medir en base a indicadores como la actividad de resolución y el tiempo de resolución. La actividad de resolución se puede contabilizar, por un lado, de manera absoluta, mediante el número de entradas resueltas a lo largo de un ejercicio, y, por otro lado, mediante la tasa de resolución, que pone en relación las entradas resueltas y las que han sido recibidas en el mismo período. Una tasa de resolución del 100%, indica que se está dando respuesta a todo el volumen de trabajo que se recibe. El tiempo de resolución, por su parte, es una medida única que indica el tiempo medio desde que un nuevo caso tiene entrada en la Agencia hasta que se firma la resolución que pone fin al mismo.

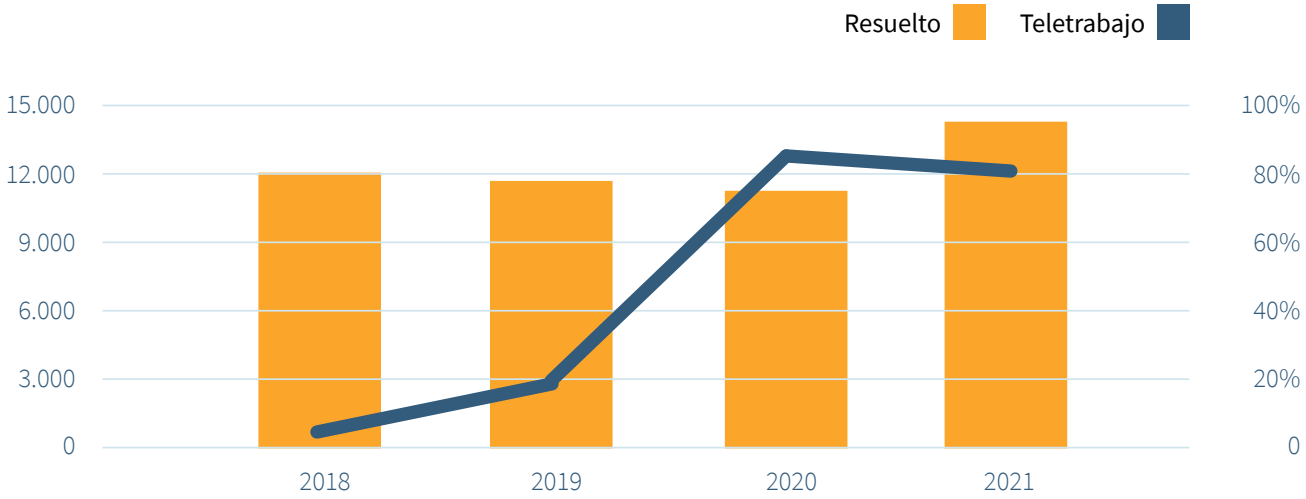
A continuación, se mostrará la evolución de los indicadores señalados desde 2018, año en que comienza la plena aplicación del RGPD, que supuso un cambio en la estructura y en el procedimiento de trabajo de la SGID, por lo que los datos de estos años son plenamente comparables.

Debe tenerse en cuenta que es durante el año 2018 cuando se lanza sistemáticamente el programa de teletrabajo, por lo que en los gráficos se incluirá también el grado de implantación del teletrabajo. A los efectos de este informe, la implantación del teletrabajo se estima como las jornadas de teletrabajo de todo el personal realizadas sobre el total de jornadas de trabajo, y por tanto para su cálculo se considera tanto el % de personal acogido al régimen de teletrabajo como el número de días por semana que realiza en el sistema de teletrabajo (así, por ejemplo, un 100% de la plantilla realizando tres días por semana de teletrabajo, supone un 60% de teletrabajo).

Actividad de resolución

La siguiente gráfica de actividad muestra el número de entradas resueltas, confrontado con la implantación del teletrabajo. Durante trece meses, entre marzo de 2020 y abril de 2021, prácticamente todo el personal estuvo trabajando en remoto la totalidad de su jornada. Ese imprescindible aumento de teletrabajo no solo ha permitido continuar con la actividad, sino que ha demostrado sostener una productividad sin precedentes en 2021, año en el que se han resuelto más de 14.000 reclamaciones, y alrededor de 750 casos procedentes de otros tipos de entradas (casos procedentes de otras AC del EEE, brechas de seguridad y casos del canal prioritario de menores). Esto supone un incremento de alrededor del 40% en comparación con los años anteriores a 2018.

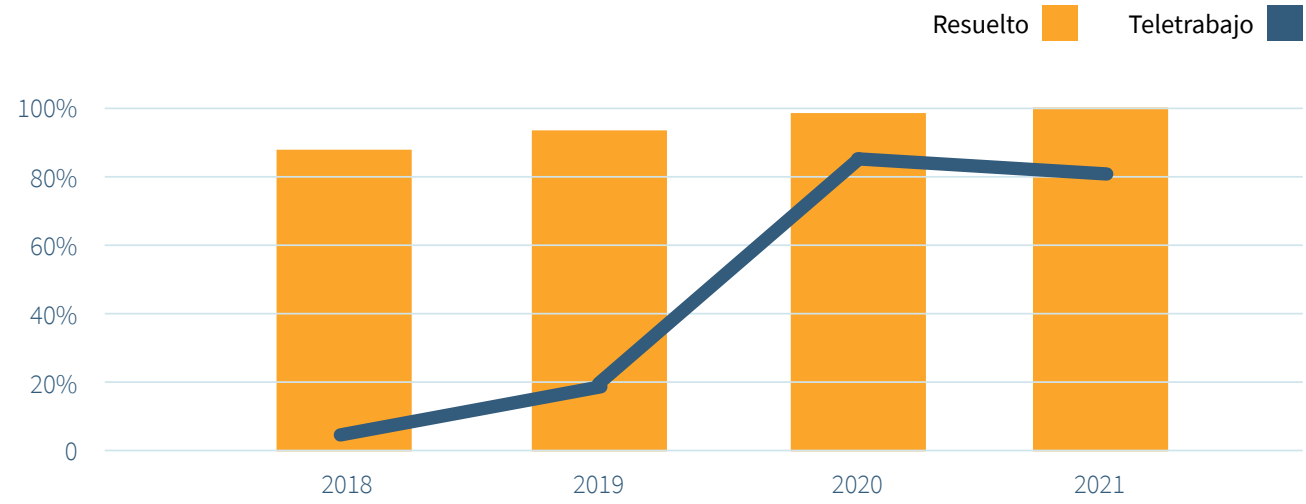
Entradas resueltas y teletrabajo	2018	2019	2020	2021
Resuelto	12.135	11.591	11.256	14.707
Teletrabajo	6%	22%	85%	80%



Al aumento en los casos resueltos se suma un incremento de la envergadura y complejidad que tienen, como demuestra el hecho de que el importe medio de las multas impuestas en 2021 triplique el importe medio de 2020 o multiplique por cinco el importe medio de los años previos al RGPD.

A continuación, se muestra un gráfico similar, pero usando para mostrar la actividad el indicador de la tasa de resolución (entradas resueltas en relación con las recibidas), obteniendo una lectura similar a la destacada anteriormente, las mejoras en tasa de resolución coinciden con años con una alta implantación de teletrabajo.

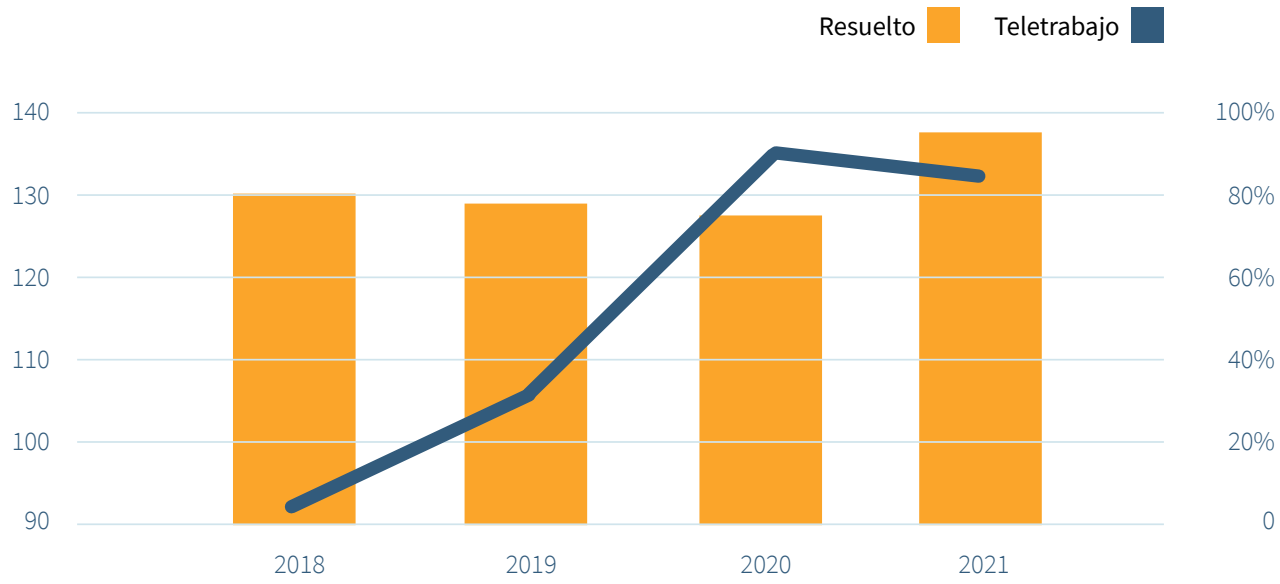
Tasa resuelto/recibido y teletrabajo	2018	2019	2020	2021
Resuelto/Recibido	89%	93%	99%	100%
Teletrabajo	6%	22%	85%	80%



Tiempo de resolución

Por lo que respecta al tiempo de resolución, se ha experimentado una reducción sostenida desde 2018, reduciendo por tanto el plazo en el que el ciudadano obtiene una respuesta a su caso. Esta tendencia es paralela al aumento de implantación del teletrabajo, reduciéndose año tras año a valores mínimos desde que se analiza este indicador. Así, como se observa a continuación, se ha podido reducir el plazo medio de respuesta de 139 a 119 días en solo tres años.

Tiempo medio resolución y teletrabajo	2018	2019	2020	2021
Tiempo medio resolución (días)	139	132	129	119
Teletrabajo	6%	22%	85%	80%



2. Gabinete Jurídico

Consultas

	Administraciones Públicas
AGE	56
CCAA	6
Entidades locales	2
Otros	5
TOTAL 1	**69**
	Consultas Privadas
Asociaciones y Fundaciones	1
Empresas	14
Particulares	0
Sindicatos	0
Otros	0
TOTAL 2	**15**
TOTAL	**84**

Evolución de consultas por sectores (2020-2021)		
	2020	2021
Administraciones Públicas	72	**62**
AAPP Sanidad	0	**6**
Particulares	3	**0**
Telecomunicaciones	15	**5**
Asesoría y consultoría	1	**0**
Sindicatos	0	**0**
Servicios informáticos	0	**0**
Asociaciones empresariales	0	**1**
Asociaciones y fundaciones	1	**1**
Solvencia patrimonial	0	**0**
Servicios	1	**2**
Sanidad y farmacia	3	**0**
Agua y energías	0	**0**
Seguridad	0	**0**
Transporte	0	**0**
Servicios financieros	0	**3**
Investigación	0	**0**
Servicios de mensajería	0	**1**
Seguros	0	**0**
Partidos políticos	1	**0**
Comunidades de propietarios	0	**2**
Industria y construcción	0	**1**
Educación	2	**0**

Nota: Existen consultas que versan sobre más de un sector y son clasificadas en el que mas relevancia tengan. Asimismo otras categorias 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 (2020-2021		
	2020	2021
Conceptos Generales*	4	**52**
Ámbito de Aplicación	8	**6**
Licitud	0	**8**
Derecho de Información y Transparencia	18	**4**
Finalidad	5	**6**
Minimización y Proporcionalidad	17	**13**
Exactitud/Calidad de datos	9	**7**
Plazo de Conservación	4	**2**
Integridad y Cofidencialidad	2	**2**
Consentimiento	36	**11**
Interés Legítimo	1	**0**
Responsable	6	**5**
Encargado	33	**7**
Corresponsable	11	**0**
Derechos	7	**4**
Derecho a información y Transparencia	15	**5**
Tratamientos Videocámaras	1	**1**
Categorías Especiales de datos	15	**13**
Seguridad en el Tratamiento	4	**4**
Responsabilidad Activa	0	**7**
Delegado Protección Datos	8	**5**
Gestión Riesgo y Evaluación de Impacto	1	**3**
Transferencias Internacionales	1	**1**
Transparencia y acceso a registros públicos	13	**5**

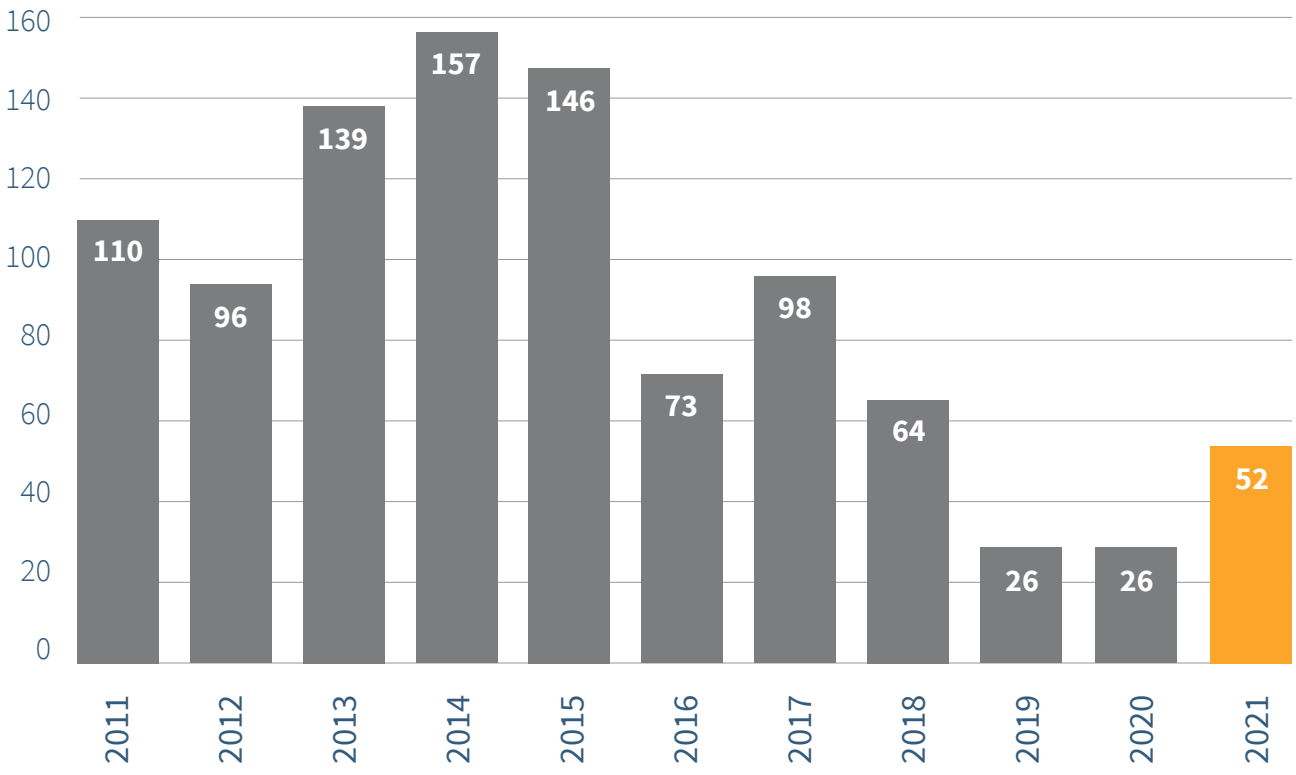
Evolución de consultas por materias (2020-2021)		
	2020	2021
Telecomunicaciones	22	**4**
Menores	0	**0**
Administración electrónica	3	**1**
Estadística	0	**1**

Nota: Existen consultas que versan sobre más de una materia (se realizan búsquedas en las columnas materia 1, materia2 y materia 3 y que por su relevancia constan en más de un apartado. Se han actualizado las categorías para adaptarlas al RGPD y LOPDGDD por lo que algunas aparecen con 0 (categoría) y otras han desaparecido y puede no haber coincidencia con los datos que se publicaron en la memoria de 2020 respecto de ese ejercicio.

*** Conceptos Generales**: *se incluyen aquí las consultas sobre proyectos de disposiciones generales*

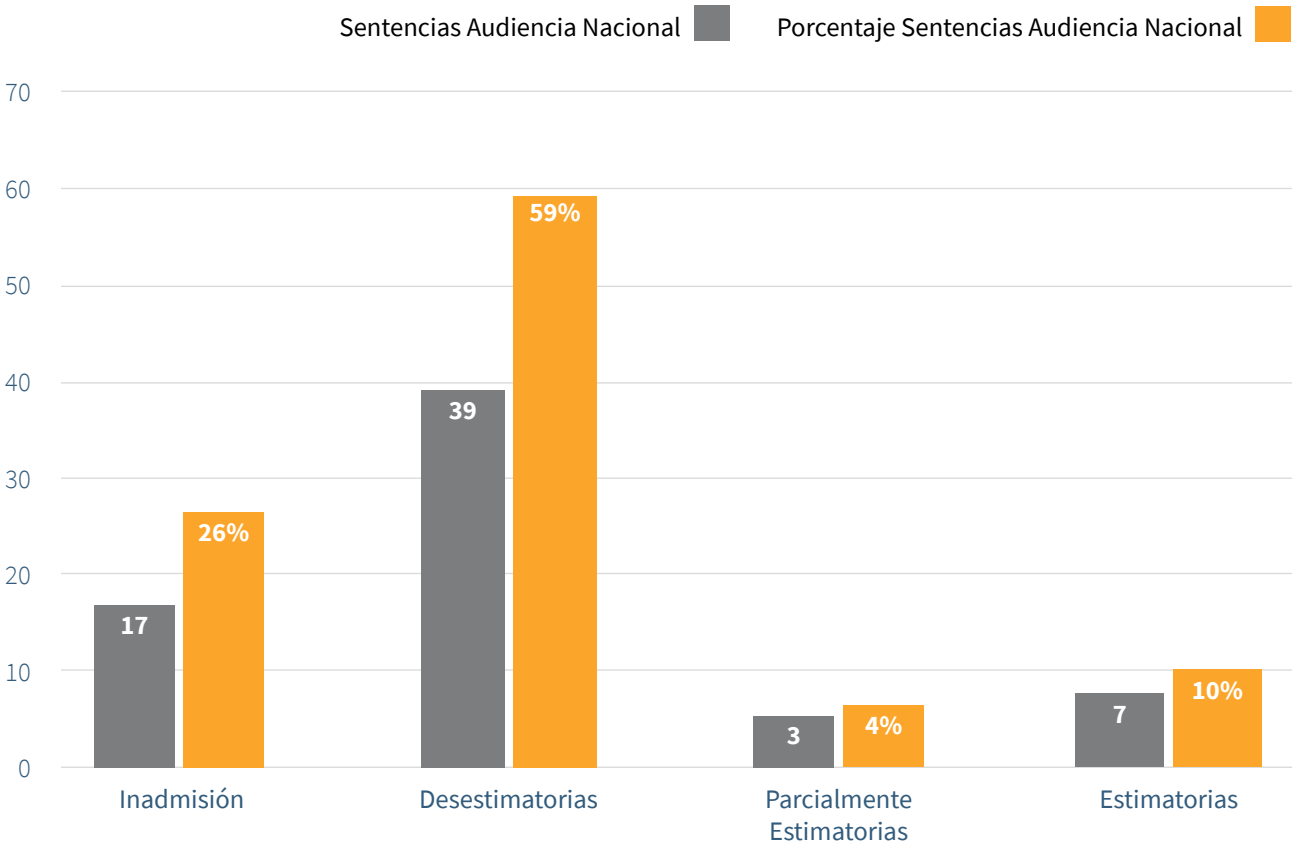
Evolución de informes preceptivos a disposiciones generales (2011-2021)

Disposiciones Generales



Evolución informes preceptivos (2011-2021)				
Año	Disposiciones generales	RD 424/2005	Prec. Otros	Total
2011	110	30	-	140
2012	96	27	51	174
2013	139	21	2	162
2014	157	23	2	182
2015	146	15	12	173
2016	73	23	1	97
2017	98	28	0	126
2018	64	24	2	90
2019	64	12	0	76
2020	26	15	0	41
2021	**52**	**5**	**0**	**57**

Sentencias Audiencia Nacional 2021

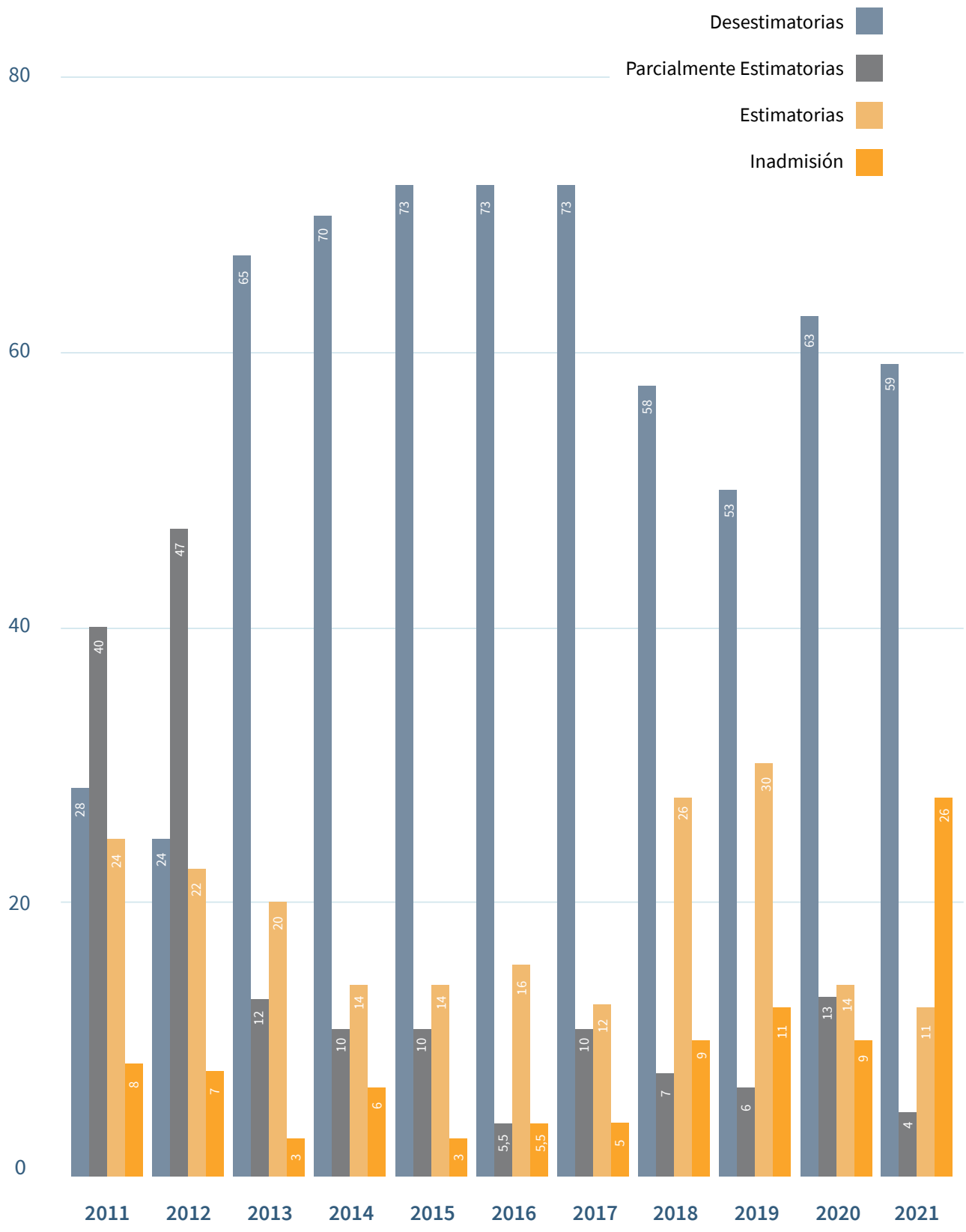


TOTAL Sentencias Audiencia Nacional 2020	**66**

Sentencias Tribunal Supremo (2021)

Evolución por sentido del fallo en porcentajes (2011-2021)				
Ejercicio (año)	Desestimatorias	Parcialmente Estimatorias	Estimatorias	Inadmisión
2011	28	40	24	8
2012	24	47	22	7
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**

Evolución por sentido del fallo en porcentajes (2011-2021)



Comparativa por sector recurrente (2020-2021)		
	2020	2021
Particulares	47	**41**
Banca y seguros	3	**7**
Telecomunicaciones	4	**5**
Solvencia patrimonial y crédito	7	**3**
Distribución y venta	2	**3**
Agua y energía	1	**3**
Administraciones Públicas	1	**2**
Asociaciones y sindicatos	0	**2**
Sociedad de la información	6	**2**
Publicidad y prospección	0	**1**
Salud	1	**0**
Otros	5	**2**
TOTAL	**77**	**71**

Nota: Se incluyen todo tipo de resoluciones de la AN y el TS, sentencias, autos, providencias, etc.

3. Atención al ciudadano y sujetos obligados

Consultas totales planteadas ante el área de Atención al Ciudadano[1]				
	2019	2020	2021	% 2020-2021
Presenciales	2.443	310[2]	64[3]	-79,35
Telefónicas	60.288	41.096	41.022	-0,18
Sede electrónica y email	10.082	8.280	3.779[4]	-54,36
TOTAL	**72.813**	**49.686**	**44.865**	**-9,70**

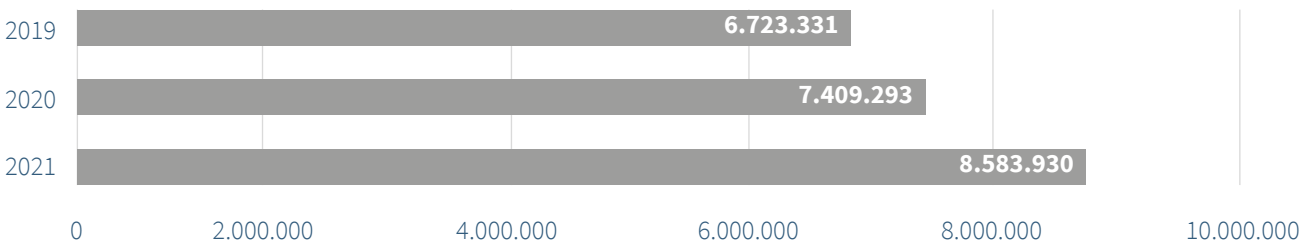
[1]Desde esta área se han atendido 57 requerimientos y solicitudes de información procedentes de Juzgados y Tribunales.

[2]Del 1 de enero al 13 de marzo 2020 - La atención presencial dejó de prestarse el 16 de marzo de 2020.

[3]Se reanuda la atención presencial el día 19 de abril de 2021, con cita previa.

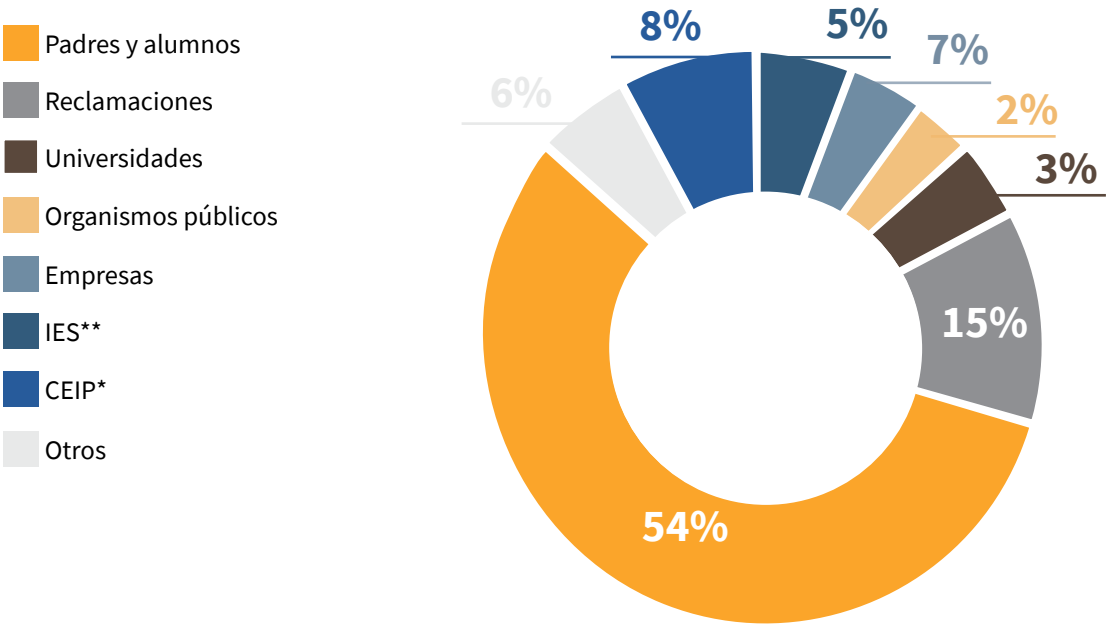
[4]Incluye las Quejas y Sugerencias (73) atendidas conforme al Real Decreto 51/2005, de 29 de julio, por el que se establece el marco general para la mejora de la calidad en la Administración General del Estado.

Comparativa de visitas a la web (*www.aepd.es*)				
	2019	2020	2021	% 2020-2021
Visitas	6.723.331	7.409.293	8.583.930	15,85



Consultas especializadas sobre el tratamiento de datos de menores				
	2019	2020	2021	% 2020-2021
Teléfono	535	552	564	2,17
WhatsApp	421	424	624	47,17
Correo-e	380	241	366	52,50
Sede electrónica	166	176	235	34,29
TOTAL	**1.502**	**1.393**	**1.789**	**28,61**

Consultas por categorías[5]



[5]Este epígrafe sólo recoge las consultas recibidas por Canal Joven y Sede electrónica

** CEIP: Planteadas por Centros de Educación Infantil y Primaria.*

*** IES: Planteadas por Institutos de Educación Secundaria.*

Accesos a la web www.tudecideseninternet.es				
	2019	2020	2021	% 2020-2021
Visitantes distintos[1]	71.651	60.478	47.130	-22,07
Números de visitas[2]	117.234	92.196	82.589	-10,42

[1] *Visitante que ha solicitado al menos una página. Si este visitante ingresa numerosas veces sólo contará como una.*

[2] *Número de visitas realizadas por todos los visitantes. Si cada visitante tiene una sesión, cada visita que realice aumentará este contador.*

Accesos a la sección de vídeos "Protege tus datos en internet"[3]				
	2019	2020	2021	% 2020-2021
Accesos al canal	87.249	21.373	22.588	5,68
Visualizaciones de vídeos	175.418	93.218	120.685	29,47

[3] *Publicados en https://www.aepd.es/es/guias-y-herramientas/videos*

Accesos al portal de transparencia			
2019	2020	2021	% 2020-2021
436.053	138.264	166.290	20,27

Canal del DPD[4]		
	2020 (desde 1/11)	2021
Consultas	200	669

[4] *El Canal del DPD sustituye al Canal Informa a partir del 1 noviembre 2020.*

Informe de Accesos a FAQ en Sede Electrónica (hasta 10/11)[5]	
Temas de consulta	Nº de visitas
En qué te podemos ayudar y en qué no	800.829
Cuestiones sobre la Sede Electrónica	100.800
Solvencia patrimonial (ficheros de morosos)	75.354
Delegado de Protección de Datos	62.858
Tratamiento de datos en el ámbito laboral	54.946
Menores y educación	52.352
Sobre el coronavirus	48.596
Comunidades de Propietarios	48.448
Videovigilancia	46.950
Difusión ilegítima de contenidos sensibles	42.240
Reglamento General de Protección de Datos. Cuestiones generales	41.586
Derechos de los afectados	35.878
Transparencia y protección de datos	30.844
Reclamaciones y otros organismos competentes	23.598
Adecuación al RGPD.	23.179
Certificación de Delegados de Protección de Datos	21.518
Transferencias Internacionales, BCR y Códigos de conducta	12.840
Procesos electorales	11.022

[5] *Hasta el 10 de noviembre el acceso a las FAQ únicamente se producía a través de la Sede Electrónica de la AEPD*

Informe de Accesos a FAQ desde el Portal Institucional (hasta 10/11)[6]	
Temas de consulta	Nº de visitas
Reglamento General de Protección de Datos. (RGPD)	5.174
Responsable, Encargado y Delegado de Protección de Datos	3.148
Tus Derechos (Información, Acceso, Rectificación y Cancelación)	2.519
Videovigilancia	2.311
Tratamiento de datos en el Ámbito Laboral	2.123
Comunidades de Propietarios	1.895
Transferencias internacionales, BCR y Códigos de conducta	1.722
Salud y coronavirus	1.708
Menores y educación	1.654
Redes sociales, difusión ilegítima de contenidos sensibles	1.561
Solvencia patrimonial (ficheros de morosos)	1.481
Cuestiones sobre la sede electrónica	1.337
Reclamaciones ante AEPD y ante otros organismos competentes	1.143
Transparencia y protección de datos	1.098
Publicidad no deseada	564
Procesos electorales	371

[6] *Desde el 10 de noviembre también se puede acceder a las FAQ desde el portal de la AEPD*

Temas más consultados en la atención telefónica					
Orden	Temas de consulta	2020	%	2021	%
1	Reclamaciones	6.203	25,3	10.441	24,63
2	Reglamento general de protección de datos (RGPD)	5.846	23,8	6.899	16,27
3	Derechos	3.415	13,9	5.603	13,21
4	Videovigilancia	1.727	7,4	3.061	7,22
5	Ficheros de solvencia patrimonial	1.818	7.4	2.681	6,32
6	Cuestiones técnicas de la sede electrónica	249	1,7	1.831	4,32
7	Herramienta FACILITA	1.380	7,04	1.438	3,39
8	Delegados de Protección de Datos	544	5,6	1.342	3,16
9	Comunidades de propietarios	424	2,2	1.038	2,44
10	Tratamiento de datos en el ámbito laboral	45	0,15	543	1,28
11	Transparencia y Protección de Datos	186	1,07	150	0,35
12	Otras cuestiones	2.713	11,07	4.578	10,80

Otros contenidos	
Guías	**Descargas**
Guía sobre el uso de videocámaras para seguridad y otras finalidades	**104.921**
Guía sobre el uso de las cookies	**90.180**
La protección de datos en las relaciones laborales	**44.378**
Guía para la gestión y notificación de brechas de seguridad	**43.804**
Protección de datos y Administración Local	**43.532**
Guía para pacientes y usuarios de la Sanidad	**42.706**
Guía para el ciudadano	**42.668**
Guía de protección de datos y prevención de delitos	**41.560**
Guía de Privacidad y Seguridad en Internet	**36.176**
Guía para el responsable de tratamiento de datos personales	**35.722**
Guía para el cumplimiento del deber de informar	**35.390**
Directrices para la elaboración de contratos entre responsables y encargados del tratamiento	**29.095**
Gestión del riesgo y evaluación de impacto en tratamientos de datos personales	**27.414**
Guía para Centros Educativos	**23.177**
Guía de Protección de Datos por Defecto	**20.812**
Compra segura en INTERNET - Guía Práctica	**19.811**
Requisitos para Auditorías de Tratamientos que incluyan IA	**19.795**
Listado de elementos para el cumplimiento normativo	**18.868**
10 malentendidos relacionados con la anonimización	**16.413**
Orientaciones y Garantías en los procedimientos de anonimización	**16.377**
Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial	**14.554**
Guía de Privacidad desde el diseño	**14.234**
Guía de Tecnologías y Protección de Datos en las AA.PP.	**14.103**

Otros contenidos	
Guías	**Descargas**
Guía de administradores de fincas	**11.593**
Drones y Protección de Datos	**11.568**
Código de buenas prácticas en protección de datos para proyectos Big Data	**8.671**
Protección de Datos por Defecto: Listado de medidas (Excel)	**8.096**
Guía de Privacidad desde el diseño (versión en inglés)	**7.447**
Informe utilización por profesores y alumnos de aplicaciones que almacenan datos en nube	**6.850**
Infografías	**Descargas**
Decálogo para el personal sanitario y administrativo	**11.686**
Riesgos del internet de las cosas en el hogar	**8.669**
Información sobre consentimiento para tratar datos personales de menores de edad	**8.300**
Adaptación al RGPD del Sector Privado	**7.805**
Cuáles son tus derechos de protección de datos	**7.036**
Los derechos que tienes para proteger tus datos personales	**5.339**
Quién es quién en el tratamiento de datos personales en tu centro educativo	**3.595**
Infografía Protección del menor en Internet	**3.052**
Canal prioritario para comunicar la difusión de contenido sensible y solicitar su retirada	**2.833**
Infografía: Medidas para minimizar el seguimiento en internet	**2.373**
Adaptación al RGPD de las Administraciones Públicas	**2.298**
Infografía: El control es tuyo, que no te controlen	**1.971**
Recomendaciones en la contratación a distancia de servicios de telecomunicaciones y energía	**1.698**
10 consejos básicos para comprar en internet de forma segura	**1.680**
Cómo evitar la publicidad no deseada	**1.005**

Otros contenidos	
Infografías	**Descargas**
Facilita Emprende	**765**
Denuncia la difusión de contenidos violentos o sexuales en Internet	**649**
Otras publicaciones	**Descargas**
El uso de las tecnologías en la lucha contra el COVID19	**46.845**
Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo	**24.968**
FAQ sobre el COVID-19	**22.539**
Preguntas frecuentes sobre la anulación del Escudo de Privacidad	**9.601**
Informe sobre políticas de privacidad en internet. Adaptación al RGPD	**9.046**
Introducción a las tecnologías 5G y sus riesgos para la privacidad	**8.778**
Adecuación a la normativa a 'coste cero' y otras prácticas fraudulentas	**7.967**
14 equívocos con relación a la identificación y autenticación biométrica	**7.961**
Introducción al hash como técnica de seudonimización de datos personales	**6.395**
Protección del menor en Internet	**6.334**
Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para el Sector Privado	**5.867**
Fingerprinting o Huella digital del dispositivo	**5.588**
Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para Administraciones Públicas	**5.347**
LOPD: Novedades para el Sector Público	**4.846**
Decálogo para la adaptación al RGPD de las políticas de privacidad en internet	**4.448**
Consecuencias administrativas, disciplinarias, civiles y penales de la difusión de contenidos sensibles	**3.863**
LOPD: Novedades para los ciudadanos	**3.614**
Plan de inspección de oficio de la atención sociosanitaria	**3.247**
LOPD: Novedades para el Sector Privado	**2.930**

Otros contenidos	
Otras publicaciones	**Descargas**
Plan de inspección de oficio sobre contratación a distancia en operadores de telecomunicaciones y comercializadores de energía	**2.678**
Orientaciones para la aplicación de la disposición adicional octava y la disposición final duodécima de la LOPDGDD	**2.596**
Fingerprinting o Huella digital del dispositivo (Versión en Inglés)	**2.236**
25 años de la Agencia Española de Protección de Datos	**2.054**
Plan de inspección sectorial de oficio Hospitales Públicos	**1.821**
Memorias	**Descargas**
Memoria 2020	**5.023**

Pacto digital para la protección de personas

Pacto digital para la protección de personas	
	2021
Entidades adheridas	349

Códigos de Conducta[7]					
	Aprobados	**Inadmitidos**	**En tramitación**	**Iniciativas**	**Códigos Tipo cancelados**
2020	1	2	12	6	5[8]
2021	0	0	14*	4	0

* *Tres códigos son de carácter transnacional, en uno de ellos actuamos como correvisores.*

[7] *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.*

[8] *Disposición transitoria segunda LOPDGDD*

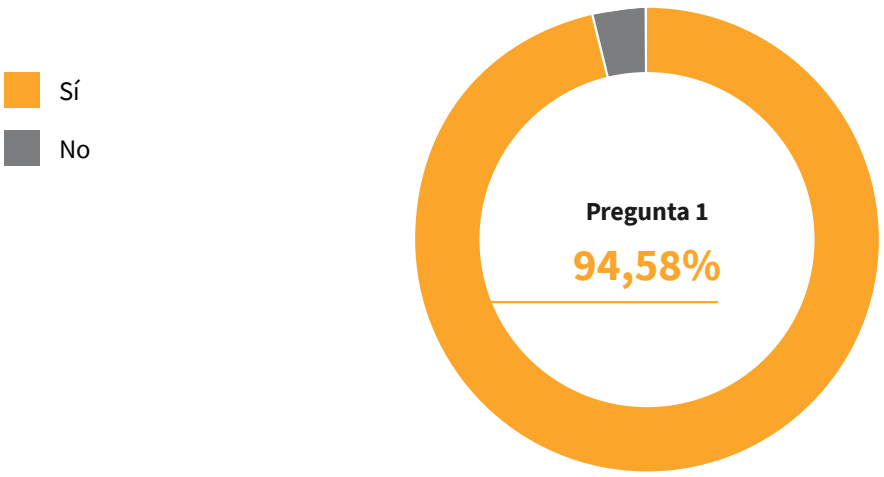
Encuestas de Calidad 2021			
Resumen general		**SI**	**NO**
1	¿Está satisfecho/a con el contenido de la información recibida?	2.809	161
2	¿Considera que la persona que le atendió tiene los conocimientos técnicos suficientes?	2.799	171
3	¿Está satisfecho/a con la corrección en el trato por parte del operador?	2.879	91
Total de encuestas realizadas		**2.970**	

Análisis de respuestas		**SI**	**NO**
1	¿Está satisfecho/a con el contenido de la información recibida?	94,58%	5,42%
2	¿Considera que la persona que le atendió tiene los conocimientos técnicos suficientes?	94,24%	5,76%
3	¿Está satisfecho/a con la corrección en el trato por parte del operador?	96,94%	3,06%
Total de encuestas realizadas		**100%**	

Encuestas de Calidad

Número Total 2.970

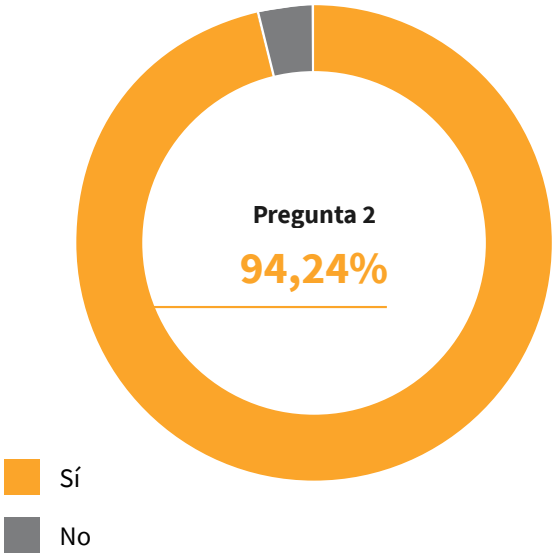
¿Estás satisfecho/a con el contenido de la información recibida?



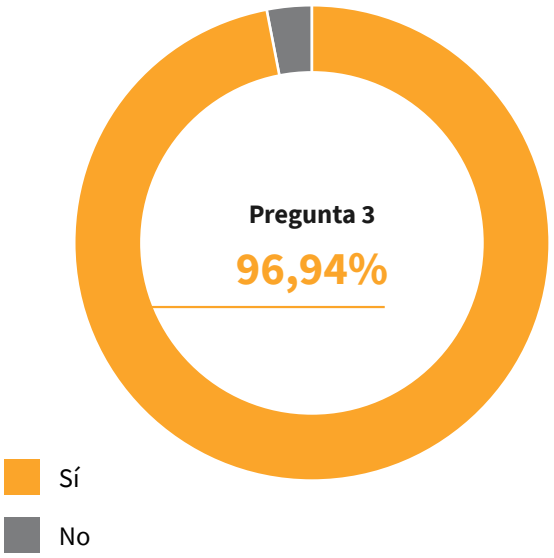
Encuestas de Calidad

Número Total 2.970

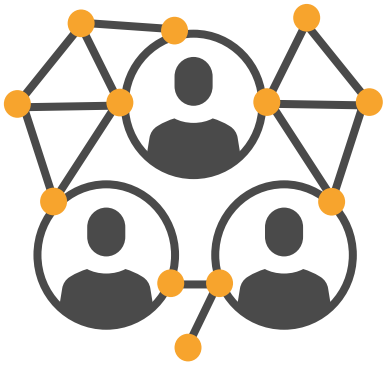
¿Considera que la persona que le atendió tiene los conocimientos técnicos suficientes?



¿Está satisfecho/a con la corrección en el trato por parte del operador?



Herramienta Facilita RGPD[8]			
	2019	2020	2021
Accesos a Facilita RGPD	197.279	124.460	63.417
Cuestionarios finalizados	49.086	26.504	24.185



[8] *Facilita RGPD, herramienta para facilitar la adecuación al RGPD de empresas y profesionales, implantada en septiembre de 2017.*

Herramienta Facilita EMPRENDE[9]		
	2020	2021
Accesos a Facilita EMPRENDE	7.682	4.747
Cuestionarios finalizados	562	794

[9] Facilita EMPRENDE, herramienta para ayudar a los emprendedores y startups tecnológicas a cumplir con la normativa de protección de datos, implantada en junio de 2020.

Herramienta Gestiona[10]		
Sección	Abierto	Finalizado
Evaluaciones de impacto en la privacidad (EIPD)	5.262	2.664
Análisis de riesgos	4.817	2.331

[10] Gestiona EIPD: Asistente para el análisis de riesgos y evaluaciones de impacto en protección de datos.

Herramienta COMUNICA-Brecha RGPD[11]	
	2021
Accesos a COMUNICA-Brecha RGPD	5.611
Cuestionarios finalizados	921

[11] 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.

Solicitudes de acceso a la información pública						
Año	Solicitudes	Autorizadas	Inadmitidas[12]	Autorizadas parcialmente	Denegadas	Desistidas
2019	94	45	10	-	3	7
2020	145	29	95	11	2	8
2021	150	48	67	14	2	19

[12] *Inadmitidas incluye devoluciones a la UIT Central. En 2021 fueron 22.*

Esquema de Certificación de DPD (AEPD-DPD)			
	2019	2020	2021
Auditorías	21	9	12
Revisión de preguntas de examen	4.300	1.927	8.538
Elaboración de exámemes	46	61	95
Seguimiento de entidades de formación	36	68	13
Seguimiento de entidades de certificación	11	7	164
Reconocimiento de formación universitaria	0	0	1
DPD Certificados	269	200	175

Transferencias Internacionales			
	2019	2020	2021
Autorizaciones de transferencias internacionales y de Normas Corporativas Vinculantes (BCR) emitidas por la AEPD	1 (Art. 46.3.b RGPD)	2	5
Actuaciones en la adopción de Normas Corporativas Vinculantes (BCR)	6 (3-C[13] y 3-AL[14])	12 (4- C y 8- AL)	11 (8-C y 3- AL)

[13] *C: La AEPD actúa como correvisora*

[14] *AL: La AEPD actúa como autoridad líder*

Registro de Delegados de Protección de Datos comunicados[15]		
Titularidad		**Total notificados**
Entidades Privadas		74.033
Entidades Públicas		8.396
	Administración General del Estado	171
	Comunidades Autónomas	416
	Entidades Locales	3.997
	Otras personas Jurídico-Públicas - Consejo General del Poder Judicial - Notarios - Colegios Profesionales - Universidades - Cámaras de Comercio - Comunidades Regantes	3.812
TOTAL		**82.249**

[15] *Durante 2021 se han atendido 1.387 consultas e incidencias relativas a la comunicación de los DPD.*

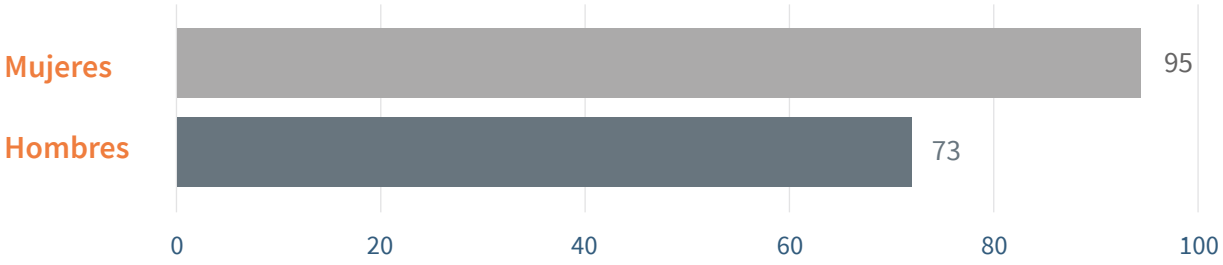
4. Secretaría General

Evolución del presupuesto			
	Crédito Ejercicio		
	2019	2020	2021
Capítulo I	7.986.570	7.986.570	8.751.570
Capítulo II	4.956.060	4.956.060	5.235.310
Capítulo III	40.950	40.950	350.950
Capítulo IV	284.440	284.440	475.520
Capítulo VI	937.860	937.860	928.350
Capítulo VIII	22.800	22.800	20.800
TOTAL	**14.228.680**	**14.228.680**	**15.762.500**

Secretaría general

Gestión de recursos humanos a 31 de Diciembre 2021		
	Dotación	Cubiertos*
Funcionarios	196	160
Laborales	6	5
Laborales fuera de Convenio	2	2
Alto cargo	1	1
TOTAL	**205**	**168**

** Los puestos no cubiertos corresponden a puestos que solo pueden cubrirse por funcionarios de nuevo ingreso, puestos de nivel 14 de muy difícil cobertura y puestos reservados de funcionarios que ocupan otras plazas en comisión de servicio.*



Funcionarios												
Nivel	30	29	28	26	24	22	20	18	17	16	15	14
Efectivos	6	3	32	61	0	19	3	26	1	5	3	1

Grupo	A1	A2	C1	C2
Efectivos	42	61	31	26

5. Presencia internacional de la AEPD

Desde el 1 de marzo de 2020, debido a las circunstancias motivadas por la pandemia COVID-19, las reuniones plenarias del Comité Europeo de Protección de Datos, así como las de sus diferentes subgrupos de trabajo, pasaron a celebrarse por medio de videoconferencia, situación que se ha mantenido durante el ejercicio 2021.

Este sistema ha permitido incrementar la frecuencia con la que se reúnen las Autoridades de Supervisión del Espacio Económico Europeo, junto el Supervisor Europeo de Protección de Datos y la Comisión Europea.

Reunión	Fecha	Lugar
Sesiones Plenarias del Comité Europeo de Protección de Datos	18 de noviembre	Bruselas (Bélgica)
	14 de enero 2 de febrero 9 y 30 de marzo 13 de abril 19 de mayo 18 de junio 7, 12 y 28 de julio 14 y 24 de septiembre 13 de octubre 14 de diciembre	Videoconferencia

Reuniones de subgrupos del Comité Europeo de Protección de datos		
Reunión	**Fecha**	**Lugar**
Reunión de Coordinadores de Subgrupos	28 de octubre	Videoconferencia
Subgrupo de asesoramiento (Strategic advisory)	15 de enero 11 y 15 de febrero 3 de marzo 10 y 31 de mayo 8 de junio 1 y 20 de julio 30 de noviembre	Videoconferencia
Grupo de trabajo Cookie Banners	8 y 29 de noviembre	Videoconferencia

Reuniones de subgrupos del Comité Europeo de Protección de datos		
Reunión	**Fecha**	**Lugar**
Grupo de trabajo sobre las 101 denuncias presentadas tras la sentencia Schrems II del TJUE	4 y 19 de febrero 31 de marzo 28 de abril 28 de mayo 17 de junio 5 y 30 de julio 23 de septiembre 14 de octubre 5 de noviembre 9 de diciembre	Videoconferencia
Medios Sociales Digitales (Social Media)	26 de febrero 12 de abril 17 de mayo 9 de julio 17 de septiembre 13 de diciembre	Videoconferencia
Usuarios de sistemas de información del CEPD (IT Users)	26 de enero 4 de mayo 22 de junio 22 de septiembre 9 de diciembre	Videoconferencia
Cooperación	18 de enero 8 y 22 de febrero 23 de marzo 29 de abril 6 y 27 de mayo 17 de junio 15 de julio 23 de septiembre 29 de octubre 25 de noviembre 15 de diciembre	Videoconferencia
Asuntos financieros	11 de enero 15 de febrero 18 de marzo 26 de abril 18 de mayo 22 de junio 20 de julio	Videoconferencia

Reuniones de subgrupos del Comité Europeo de Protección de datos		
Reunión	**Fecha**	**Lugar**
Multas	19 de enero 2 y 3 de marzo 15 de abril 25 de mayo 29 de septiembre 2 de diciembre	Videoconferencia
Transferencias internacionales	6, 12, 25 y 29 de enero 10 y 24 de febrero 26 y 29 de marzo 7, 8, 16, 27 y 28 de abril 26 de mayo 1, 2, 9, 29 y 30 de junio 9, 13, 27 de julio 7, 8, 20 y 28 de septiembre 5 y 6 de octubre 9, 10 y 19 de noviembre 7, 8 y 13 de diciembre	Videoconferencia
Fronteras, viajeros y aplicación legislativa (BTLE)	21 de enero 18 de febrero 18 y 25 de marzo 22 de abril 3 de mayo 1 y 24 de junio 15 de julio 2 y 28 de septiembre 28 y 30 de noviembre	Videoconferencia
Disposiciones clave (Key Provisions)	7 y 27 de enero 4 y 11 de marzo 21 de abril 11 de mayo 8 de junio 5 y 6 de julio 21 de septiembre 26 de octubre 15 de noviembre 1 de diciembre	Videoconferencia
Supervisión del cumplimiento (Enforcement)	20 de enero 17 de febrero 10 y 24 de marzo	Videoconferencia

Reuniones de subgrupos del Comité Europeo de Protección de datos		
Reunión	**Fecha**	**Lugar**
Supervisión del cumplimiento (Enforcement)	5 de mayo 2, 16, 17, 23 de junio 2, 5, 6, 16 y 23 de julio 22 de septiembre 27 de octubre 24 de noviembre	Videoconferencia
Tecnología	21 de enero 11 y 12 de febrero 4 y 5 de marzo 6 y 7 de mayo 3, 4, 24, 25 y 30 de junio 3 y 30 de septiembre 4 y 5 de noviembre 1 de octubre 3 de diciembre	Videoconferencia
Cumplimiento, Gobierno electrónico y Salud (Compliance, E-goverment & Health)	18 y 19 de enero 16 y 17 de febrero 3, 4 y 22 de marzo 19 de abril 5 y 12 de mayo 6, 7 y 10 de junio 6 de julio 1 de septiembre 18 y 19 de octubre 12 y 24 de noviembre 17 de diciembre	Videoconferencia
Grupo de trabajo sobre medidas suplementarias en transferencias internacionales tras la sentencia Schrems II del TJUE	23 de febrero 20 de abril 4 y 20 de mayo	Videoconferencia

Control de Agencias y Grandes Sistemas de Información UE		
Reunión	**Fecha**	**Lugar**
Grupo de Supervisión Coordinada CIS	14 de junio	Videoconferencia
Grupo de Supervisión Coordinada del SIS II	16 de junio 25 de noviembre	
Grupo de Supervisión Coordinada del VIS + EURODAC	17 de junio 24 de noviembre	
Grupo de Supervisión Coordinada de EUROPOL	23 de noviembre	

Otras Reuniones		
Reunión	**Fecha**	**Lugar**
Global Privacy Assembly **(antigua conferencia internacional de comisionados de protección de datos y privacidad)** Foro anual global donde autoridades supervisoras independientes en materia de privacidad, protección de datos y libertad de información adoptan resoluciones de alto nivel y recomendaciones dirigidas a los gobiernos y organizaciones internacionales	del 18 al 21 de octubre	Videoconferencia
Consejo de Europa - 52ª reunión de la mesa de trabajo del Comité Consultivo del Convenio 108 - 41ª Plenario del Comité Consultivo del Convenio 108 - 53ª reunión de la mesa de trabajo del Comité Consultivo del Convenio 108 - 42ª Plenario del Comité Consultivo del Convenio 108 - 54ª reunión de la mesa de trabajo del Comité Consultivo del Convenio 108	del 18 al 21 de octubre	Videoconferencia

Otras Reuniones		
Reunión	**Fecha**	**Lugar**
Comité Shengen (Evaluación Holanda)		
Visitas de evaluación Schengen in situ específica para Francia de conformidad con el artículo 10 del Reglamento (UE) 1053/2013.	del 19 al 23 de abril	Videoconferencia
Comité Schengen (Evaluación Francia)		
Visitas de evaluación Schengen in situ específica para Francia de conformidad con el artículo 10 del Reglamento (UE) 1053/2013.	del 27 de junio al 2 de julio	Videoconferencia