




# MEMORIA AEPD 2020

# prólogo

La Memoria que me complace presentar expone de forma detallada las actividades más relevantes llevadas a cabo por la Agencia Española de Protección de Datos en 2020, un año atípico para todos en el que este organismo no sólo ha tenido que enfrentarse a numerosos retos relacionados con el derecho fundamental del que es garante sino que ha tenido que hacerlo en el entorno de la pandemia derivada de la pandemia COVID-19.

Una mis primeras decisiones como directora fue establecer unas líneas de actuación estratégicas que permitieran responder al gran reto que suponía ayudar a las empresas y organizaciones de todo tipo a prepararse para el nuevo Reglamento General de Protección de Datos. Con ese objetivo se diseñó el Plan Estratégico, cuyas 150 iniciativas culminaron en 2019 dando paso a la puesta en marcha de Marco de Actuación de Responsabilidad Social y Sostenibilidad. Una de las actuaciones incluidas en ese Marco –el teletrabajo, que ya se venía aplicando en la Agencia desde 2017– ha permitido que la Agencia haya estado en unas condiciones óptimas para continuar trabajando en la situación extrema que hemos vivido este año y que requería conciliar la salud de los y las empleadas con sus obligaciones laborales. Es esta Memoria van a poder consultar con detalle las acciones realizadas en todos los ámbitos, observando cómo los tiempos de respuesta y el desarrollo de proyectos de concienciación se han mantenido e incluso mejorado respecto al año anterior, demostrando que la implantación total del teletrabajo no ha mermado la capacidad de trabajo del organismo.

Uno de los retos principales de 2020 ha sido establecer criterios y conciliar la garantía de la asistencia sanitaria y el control de la pandemia con el derecho fundamental a la protección de datos personales. Y ha sido uno de los retos porque, en paralelo, la Agencia ha tenido que seguir trabajando en la resolución de las reclamaciones planteadas por los ciudadanos, participando en las decisiones de carácter internacional, atendiendo las dudas y consultas tanto de los ciudadanos como de los sujetos obligados, publicando materiales o lanzando iniciativas de diversa índole para fomentar la privacidad. Todo ello sin descuidar la necesaria pedagogía de entender la protección de datos como un elemento de competitividad que redunde en beneficio tanto de las propias organizaciones como de las personas cuyos datos se tratan.



Así, durante 2020 estuvimos trabajando en la preparación del *Pacto Digital para la Protección de las Personas*, un proyecto que pretende promover la privacidad como un activo que las organizaciones deben tener en cuenta a la hora de diseñar sus políticas y sus estrategias.

Aquellos que tratan datos personales deben abordar la protección de datos como un activo diferenciador para sus empresas y de responsabilidad para con sus clientes. Muchas de las 150 actuaciones realizadas del Plan estratégico y las más de 100 recogidas en Plan de Sostenibilidad 2019-2024, de las que la Agencia ya ha cumplido el 65% de las acciones previstas para los cinco años, están orientadas a ayudarles en esta tarea, porque el fomento de la protección de datos no puede estar basado exclusivamente en los poderes coercitivos y sancionadores. Así, en los últimos años hemos lanzado iniciativas como la multipremiada herramienta *Facilita\_RGPD*, *Facilita Emprende*, *Gestiona*, y otras muchas recogidas en esta Memoria. Igualmente, las personas también deben ser conscientes de la importancia de proteger sus datos personales. En un mundo fuertemente tecnologizado esta tarea no es siempre sencilla, y por ello también hemos trabajado en los últimos años en herramientas para dar una respuesta rápida ante situaciones extremas. Una de las acciones con mayor impacto social de las realizadas en los últimos años ha sido el lanzamiento del *Canal Prioritario* para denunciar ante la Agencia la difusión en Internet de contenidos sensibles publicados sin el permiso de las personas que aparecen en ellos, en particular, en casos de acoso a menores o violencia sexual contra las mujeres. Como podrá verse en esta Memoria, el número de tramitaciones urgentes a través de esta vía se ha triplicado respecto a 2019, alcanzando casi el medio centenar, pero en la Agencia queremos seguir trabajando para que este Canal se convierta en una referencia de ayuda.

En todo caso, la actuación una vez que los contenidos se han publicado no deja indemne a las personas afectadas, por lo que en los últimos años también hemos trabajado en numerosas iniciativas para intentar concienciar a los jóvenes de las consecuencias de un uso inadecuado de Internet. Avanzar hacia una sociedad en la que la tecnología y los derechos fundamentales vayan de la mano supone educar de forma temprana.

Así, la LOPDGDD recogió en su artículo 83 a propuesta de la Agencia que el sistema educativo debe garantizar las competencias digitales del alumnado en las asignaturas de libre configuración, y sin duda hay que seguir trabajando en este tema. Además, en este momento se encuentra en tramitación el Proyecto de Ley Orgánica de protección integral a la infancia y la adolescencia frente a la violencia, que incluye referencia explícita a la Agencia con el fin de garantizar una protección específica de los datos personales de las personas menores de edad en los casos de violencia, especialmente cuando se realice a través de Internet, garantizando un canal de denuncia ante la existencia de contenidos ilícitos en Internet como el Canal Prioritario.

La construcción de una sociedad tecnológica sostenible a largo plazo exige sin duda dar soluciones preventivas, que permitan fomentar el desarrollo de la economía digital e impulsar el respeto a los derechos y libertades de los ciudadanos. En este sentido, debo destacar la puesta en marcha dentro de la Agencia de la División de Innovación y Tecnología, que aborda la responsabilidad proactiva en el marco de los nuevos desarrollos tecnológicos. La inteligencia artificial, el blockchain, la biometría o el internet de las cosas, con su utilidad indudable, pueden tener un importante efecto negativo sobre la privacidad de las personas si no se desarrollan correctamente. La División ha elaborado materiales y herramientas de ayuda o documentos tecnológicos con repercusión a nivel europeo, y es un tema que va a adquirir una importancia cada vez mayor.

Por último, es obligatorio agradecer de forma expresa la dedicación y el esfuerzo de las personas que trabajan en la Agencia, un equipo que no ha crecido de forma proporcional a los retos planteados, cada vez mayores tanto en número como en complejidad, y con el que siempre se puede contar para emprender nuevos proyectos. Las siguientes páginas son la mejor prueba de ello.

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

# Índice

## Memoria 2020

▲ 1. Principales Hitos de 2020	6
▲ 2. Actividades de la AEPD en la pandemia de la COVID-19	8
▲ 3. El marco de responsabilidad social de la AEPD	13
▲ 4. Desafíos para la privacidad	24
▲ 5. Al servicio de los ciudadanos	72
▲ 6. Ayuda efectiva para las entidades	91
▲ 7. La potestad de supervisión	97
▲ 8. Una estructura en permanente evolución	107
▲ 9. La necesaria cooperación institucional	112
▲ 10. Una autoridad activa en el paronama internacional	114
▲ 11. La cooperación con Iberoamérica	123

## Anexo. La agencia en cifras

▲ 1. Marco de Responsabilidad Social y Sostenibilidad	128
▲ 2. Inspección de datos	130
▲ 3. Gabinete jurídico	147
▲ 4. Atención al ciudadano y sujetos obligados	156
▲ 5. Secretaría general	168
▲ 6. Presencia internacional de la AEPD	170

## ➤ 1. Principales hitos de 2020

El principal hito de 2020 para la Agencia Española de Protección de Datos (AEPD) ha sido dar respuesta desde la perspectiva de protección de datos a la situación generada por la pandemia de la COVID-19 en una doble dimensión:

- La conciliación de las medidas a adoptar para garantizar la asistencia sanitaria y el control de la pandemia con el derecho fundamental a la protección de datos personales, en colaboración con el Ministerio de Sanidad como principal autoridad competente para la adopción de medidas en relación con dicha finalidad.
- La adopción de medidas de carácter organizativo que permitieran mantener el nivel de actividad de la Agencia Española de Protección de Datos en las circunstancias que ha exigido la COVID-19, de forma que no pudiera resentirse el sistema de garantías para los ciudadanos establecido en la normativa de protección de datos personales. Este objetivo se ha cumplido de forma satisfactoria ampliando las políticas que ya venían practicándose en la modalidad de teletrabajo.





Un segundo hito en el año 2020 ha sido la profundización en el desarrollo y cumplimiento del Plan de Responsabilidad Social Corporativa de la Agencia, alineado con los Objetivos de Desarrollo Sostenible de la Agenda 2030.

Como ya se señalaba en la Memoria del año 2019, en dicho ejercicio culminó el periodo de cumplimiento del Plan Estratégico diseñado en el año 2015, dándose cuenta en ella de los términos de dicho cumplimiento. Finalizado en julio de 2020 el mandato de 4 años de la Directora de la Agencia, no resultaba oportuno definir un nuevo plan estratégico que pudiera comprometer las decisiones de la nueva Presidencia de la entidad.

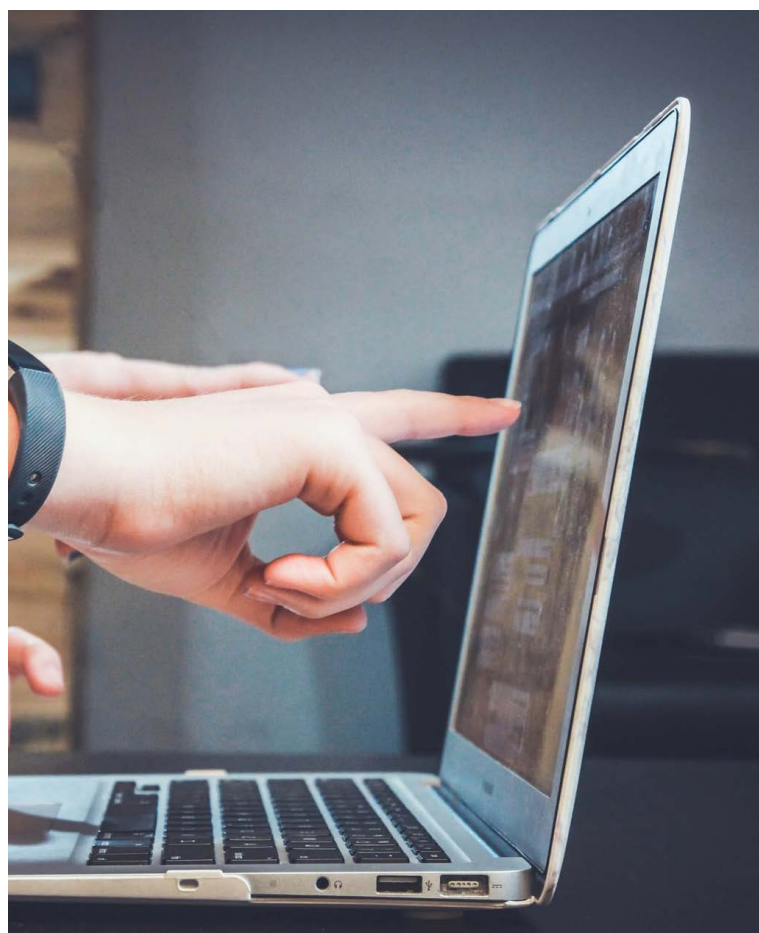
Esta circunstancia no ha sido obstáculo para el impulso del programa de RSC como compromiso ético con los ciudadanos y otros agentes (empresas, Administraciones Públicas o profesionales, entre otros) y directamente relacionado con la tutela del derecho fundamental a la protección de datos mediante la promoción y desarrollo del *Canal prioritario* para la eliminación urgente de contenidos violentos o sexuales en internet, evitando los perjuicios que implica la viralidad asociada a la difusión de tales imágenes.

En lo relativo al modelo de cumplimiento y de supervisión, regulado en el Reglamento (UE) 2016/679, General de Protección de Datos (RGPD), se han promovido procedimientos amistosos y de resolución extrajudicial de las reclamaciones, así como la adopción de medidas correctivas previstas en el Reglamento.

Y, también, como consecuencia de reclamaciones planteadas por los interesados o apreciadas de oficio por la Agencia, se ha analizado la adecuación de las políticas de privacidad y los protocolos adoptados para garantizar el cumplimiento del Reglamento y la aplicación de un régimen sancionador de carácter disuasorio respecto de los incumplimientos de la norma.

Todo ello dentro del proceso de consolidación del modelo europeo de protección de datos y del organismo previsto en el mismo para garantizar una aplicación armonizada en todo el territorio de la Unión Europea, cómo es el Comité Europeo de Protección de Datos (CEPD).

Otro de los hitos del ejercicio 2020 ha sido la consolidación de la Unidad de Evaluación y Estudios Tecnológicos (UEET), que orgánicamente se ha constituido como una División de Innovación Tecnológica (DIT) dentro de la organización de la Agencia, que ha intensificado su actividad prospectiva y divulgativa respecto de los desarrollos tecnológicos que afectan a la protección de datos personales. También es necesario destacar el desarrollo, en paralelo, de nuevas iniciativas divulgativas para facilitar el conocimiento y cumplimiento de la normativa de protección de datos. De todos estos aspectos se informará detalladamente en los diversos apartados de la memoria.



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

La situación generada por la COVID-19 ha incidido ampliamente en la aplicación de la normativa de datos personales como consecuencia, especialmente, de abordarse en un marco jurídico excepcional, como es el de la declaración del estado de alarma; implicar el tratamiento de categorías especiales de datos, como son los datos de salud para garantizar la asistencia sanitaria y el control de la pandemia; redefinir la posición jurídica de los agentes públicos y privados intervinientes y plantear iniciativas novedosas para la utilización de la tecnología en esta situación.

Es evidente que la pandemia ha acelerado el proceso de digitalización de los distintos sectores de la economía. Un ejemplo de ello es el desarrollo del teletrabajo o de la inteligencia artificial o la telemedicina en el campo de la salud, que podría permitir un ahorro significativo a los sistemas públicos sanitarios al mejorar la prevención, el diagnóstico y el tratamiento de enfermedades.

**Esta situación ha exigido que la Agencia desarrollara un amplio abanico de iniciativas para hacer efectivo el derecho a la protección de datos en los tratamientos dirigidos a garantizar la asistencia sanitaria y el control de la epidemia, en la mayor parte de las ocasiones en colaboración con el Ministerio de Sanidad.**

Sin perjuicio de las actividades realizadas por las distintas unidades de la Agencia en relación con la COVID-19, que se describen en los correspondientes apartados de la Memoria 2020, se detallan, sintéticamente, a continuación, las principales actividades desarrolladas por la AEPD:

### 2.1 Las bases jurídicas del tratamiento

El análisis de las implicaciones del tratamiento de datos personales en la pandemia de COVID-19 tiene como punto de partida la afirmación de que en este entorno el derecho a la protección de datos no está suspendido, pero no puede ser ni es un obstáculo para dar respuesta a la misma, ya que el Reglamento (UE) 2016/679, General de Protección de Datos (RGPD) permite compatibilizar ambos aspectos.

Las bases jurídicas del tratamiento de datos son la consecución de interés público esencial y la garantía del interés vital de los afectados y de terceros. En algunos casos, pueden concurrir otras bases jurídicas como el cumplimiento de obligaciones legales en el entorno laboral en el marco de la legislación de prevención de riesgos laborales.

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.



## **Responsables y encargados del tratamiento**

En el ámbito público, los responsables del tratamiento han sido el Ministerio de Sanidad y también las administraciones sanitarias de las Comunidades Autónomas, que conservan las competencias que tenían atribuidas antes de la pandemia.

Otros responsables han sido el Ministerio del Interior y las Fuerzas y Cuerpos de Seguridad del Estado, conforme a los criterios de las autoridades sanitarias.

El resto de Administraciones públicas y las entidades privadas que han colaborado con ellas tendrán la condición de encargados o subencargados del tratamiento (privados que ofrecen tecnología y que deben realizar una Evaluación de Impacto en la Protección de Datos).

## **La toma de temperatura para el control de la epidemia (Comunicado de la AEPD)**

La toma de temperatura no puede considerarse como un hecho aislado sino como parte de un proceso que tiene como finalidad evitar el contagio de la enfermedad.

El conjunto de tratamientos relacionados con la toma de temperatura implica, con carácter general, un tratamiento de datos personales y una injerencia particularmente intensa en los derechos de los afectados al referirse a datos de salud, presumir si padece o no una infección y sufrir posibles estigmatizaciones sociales (así podría suceder en el entorno educativo, laboral o comercial, por denegaciones de acceso).

Hay que tener en cuenta que, según las informaciones proporcionadas por las autoridades sanitarias, hay un porcentaje de personas contagiadas asintomáticas que no presentan fiebre, que la fiebre no es siempre uno de los síntomas presentes en pacientes sintomáticos y que puede haber personas que presenten temperaturas elevadas por causas ajenas a la COVID-19. (Falsa sensación de seguridad).

Estas medidas solo deben aplicarse atendiendo criterios definidos por el Ministerio de Sanidad. La toma de temperatura no puede ser un criterio aislado para la toma de decisiones sino, en su caso, parte de un proceso en el que haya una confirmación adicional por profesionales sanitarios.

Las directrices del Ministerio de Sanidad y el de Trabajo (mayo 2020) en el ámbito de la prevención de riesgos laborales en establecimientos con acceso de público, se han focalizado fundamentalmente en medidas organizativas, tales como el control del aforo, de la entrada de los clientes, de mantener la distancia social y de aislar mediante mamparas mostradores y cajeros.

El consentimiento no puede ser una base jurídica para estos tratamientos, que pueden suponer la denegación de servicios o el acceso a lugares, porque no sería libre. El interés legítimo podría no ser aplicable, ya que el impacto sobre los derechos, libertades e intereses de los afectados haría que no resultara prevalente.

## **La toma de temperatura para el control de la epidemia (Colegios)**

Como se ha señalado, la toma de temperatura debe enmarcarse en un protocolo de acuerdo con los criterios de las autoridades sanitarias. En los centros educativos existen protocolos aprobados por el Ministerio de Educación, Sanidad y por las Comunidades Autónomas, que incluyen la obligación de tomar la temperatura corporal a todo el alumnado y al personal previamente al inicio de la jornada.

Los protocolos citados y la LOPDGDD establecen exigencias de garantía de la confidencialidad, respecto de los datos de identidad de casos sospechosos y confirmados, a los que la ley añade garantías de no discriminación de los alumnos. En particular, al tratarse de categorías especiales de datos.

Los protocolos exigen que se designe un responsable de la COVID-19, que será quién contactará con la familia y con el centro de salud o un teléfono de referencia de la administración sanitaria.

Por tanto, si existen indicios de contagio, deben comunicarse confidencialmente sólo a este responsable.

La comunicación de casos de contagio con datos identificativos (por ejemplo, a través de grupos de Whatsapp), podrían ser lícitos si se consideran incluidos dentro de la excepción doméstica (por ejemplo, otros familiares, amistades, etc.) En otros casos, el tratamiento podría ser ilícito.

### **La toma de temperatura para el control de la epidemia (entorno laboral)**

En el entorno laboral podría tener como base jurídica la obligación que tienen los empleadores de garantizar la seguridad y salud de los trabajadores a su servicio.

Los empleadores conforme a la normativa de prevención de riesgos laborales y con las garantías que se establecen pueden conocer si los trabajadores están infectados para garantizar su salud, evitar contagias y adoptar medidas previstas por las autoridades competentes.

Los empleadores pueden comunicar esta información al resto del personal de la empresa sin identificar a la persona afectada, salvo que fuera necesario para proteger la salud de las personas trabajadoras. Es obligatorio para las personas infectadas o sometidas a aislamiento preventivo informar a su empleador, o en su caso, a los delegados de prevención de riesgos de esta circunstancia.

### **Información sobre la COVID para la oferta y búsqueda de empleo**

La información sobre la COVID y el desarrollo de anticuerpos es un dato de salud. Respecto de las bases jurídicas para su tratamiento, hay que señalar que la recogida y utilización de dicha información por la empresa carece de la misma y es ilícita. Ello es así, porque el consentimiento no sería libre, ya que no puede negarse o retirarse sin consecuencias negativas para la obtención del puesto de trabajo.

Por su parte, la relación contractual no puede ser una base jurídica lícita, ya que no se trata de un empleado y, aunque lo fuera, va más allá de los derechos y obligaciones de la normativa laboral. Se produce por tanto la paradoja de que la empresa que solicita dicha información tendría que desechar el curriculum o suprimirla.

### **Comunicación y tratamiento de datos a las Fuerzas y Cuerpos de Seguridad con la finalidad de controlar las situaciones de confinamiento obligatorio**

La Ley orgánica 3/1986, de medidas especiales en materia de salud pública legitima la adopción de medidas apropiadas por parte de las autoridades sanitarias para el control de enfermos o persona de contacto en caso de epidemia.

La base jurídica de estas cesiones a las Fuerzas y Cuerpos de seguridad sería el interés público y la garantía de intereses vitales de los afectados y de terceros para permitir la adopción de medidas por las autoridades sanitarias. La cesión debe cumplir los principios de minimización, proporcionalidad y finalidad, por lo que ha de limitarse a los datos necesarios para la identificación de los confinados y de su domicilio o lugar de residencia. No podría incluir otros datos de salud, como son los incorporados a la historia clínica.

Las Fuerzas y Cuerpos de seguridad deben cumplir con las garantías de confidencialidad no informando a terceros y, una vez cumplida la finalidad del tratamiento, no deben conservar los datos salvo en la medida en que lo exija una obligación legal.

### **Actuaciones de la Agencia en el marco del Comité Europeo de Protección de Datos: La recomendación sobre el uso de datos de localización y apps de seguimiento de contactos en el contexto de la pandemia**

La Recomendación del Comité Europeo de Protección de Datos (CEPD) destaca los siguientes aspectos:

- Las apps de contact tracing deben formar parte de una estrategia global de salud pública y tener confirmación por una persona o institución cualificada en los supuestos de contagio. Es decir, no ser objeto de decisiones automatizadas.
- Los datos de localización recogidos por las telecos y similares sólo pueden ser cedidos si han sido anonimizados por el proveedor o, si indican la posición geográfica, con consentimiento del interesado.
- El almacenamiento de información en el dispositivo del usuario o el acceso a la información ya almacenada sólo se permite si el usuario ha dado su consentimiento o si es estrictamente necesario para el servicio solicitado.
- Las autoridades podrían obtener datos de geolocalización sin consentimiento sobre la base de un interés público.
- Las apps de rastreo sólo podrían tratar información de proximidad y no movimientos (geolocalización).
- Es preferible que los datos se anonimicen y que los indicadores únicos generados por las apps se renueven cada cierto tiempo para evitar el riesgo de identificación y seguimiento.
- Es preferible que los datos se almacenen y se traten de forma descentralizada por encajar mejor con el principio de minimización.
- Sólo deben ser informadas las personas con las que el usuario contagiado ha estado en estrecho contacto (criterio sanitario) y verificarse la infección a través de un profesional sanitario para alertar a los contactos.

Los principales aspectos de la Resolución de la Dirección General de Salud Pública sobre el tratamiento de datos de vacunación son los siguientes:

Los datos de vacunación obtenidos por las Consejerías de Sanidad Comunidades Autónomas y los Servicios de Sanidad Exterior deben remitirse al Ministerio de Sanidad para facilitar el seguimiento y la vigilancia epidemiológica de la COVID-19 mediante su análisis a efectos estadísticos y de georreferenciación, previo proceso de seudonimización de los datos identificativos de las personas vacunadas.

Adicionalmente, se prevé la posibilidad de su uso para la acreditación del acto de vacunación mediante la emisión de un certificado, previa solicitud expresa e inequívoca del interesado que se haya vacunado.

No obstante, el tratamiento ulterior de estos datos por parte de terceros debe cumplir con todas las garantías de protección de datos personales y, muy especialmente, evitando su uso en situaciones que puedan generar discriminación.

En relación con los datos de vacunación, la Agencia ha promovido la cooperación con las autoridades de protección de datos de los restantes Estados miembros, con el fin de emitir recomendaciones sobre la utilización de los datos de vacunación en las iniciativas que están desarrollando la Comisión Europea y el Consejo sobre estos certificados.

### **Actividades de difusión**

Complementariamente a las actividades que se han descrito, la Agencia ha desarrollado una amplia actividad de difusión de informaciones y documentos en relación con la COVID-19, dirigidos tanto a ciudadanos como a los responsables del tratamiento de los datos. Y ha creado una sección específica en su web llamada '*Protección de datos y coronavirus*' que incluye numerosos documentos que se recogen de forma detallada en otros apartados de esta Memoria.

En lo relativo a las actividades de investigación, la Agencia ha desarrollado las iniciativas que a continuación se mencionan.

En el marco del CEPD, la Agencia ha participado en la elaboración de las Directrices sobre investigación científica en el contexto de la crisis de

COVID-19. En ellas, se indica que las excepciones a la prohibición de tratar datos de salud con fines de investigación se encuentran en el interés público en el ámbito de la salud pública y en la finalidad de investigación (artículo 9.2.i) y j) RGPD). Por tanto, las bases jurídicas del tratamiento serán, con carácter general, el interés público sin necesidad de consentimiento, aunque este puede ser necesario en determinados casos.

Los fines importantes de interés público por razones excepcionales habilitan las transferencias internacionales de datos para estas investigaciones, recomendándose que tan pronto como sea posible, se adopten las cláusulas contractuales estándar de la Comisión.

Las posibles limitaciones a los derechos de los interesados deberían regularse conforme a la legislación nacional.

En respuesta a una consulta de Farmaindustria, la Agencia elaboró un informe admitiendo la posibilidad remota de ensayos clínicos con medicamentos durante la epidemia de COVID-19.

Monitorización que responde a la necesidad de garantizar el desarrollo de determinados ensayos clínicos y, en todo caso, la salud de los sujetos participantes. El resultado final de la consulta se fundamenta en una novación del contrato inicial entre el promotor y el centro del ensayo y dos anexos: un compromiso de confidencialidad entre el promotor y el monitor y un protocolo de seguridad de conexión remota.

El primero de los documentos presentados es una adenda al contrato suscrito entre el promotor y el centro en el que se está realizando el ensayo clínico.

Se trata, por tanto, de una novación modificativa y no extintiva de un contrato preexistente en el que deben figurar todos los requisitos exigidos por la normativa de ensayos clínicos para la realización del mismo.

En la parte expositiva se destaca la habilitación por parte del centro para la utilización de un sistema de acceso remoto a la información necesaria para ejercer las labores de monitorización del ensayo. Estas labores incluyen la verificación de datos fuente, como alternativa a la monitorización presencial.

Adicionalmente, en dicha cláusula, el promotor garantiza, como responsable del tratamiento de los datos del ensayo clínico, que el monitor llevará a cabo sus funciones conforme a los procedimientos normalizados de trabajo, accediendo únicamente a la información estrictamente necesaria para la realización de sus funciones (principio de minimización). Y, a tal efecto, suscribe con el monitor, encargado del tratamiento de los datos, el acuerdo de confidencialidad que consta como Anexo I. Asumiendo, en consecuencia, la plena responsabilidad de las consecuencias que pudieran derivarse del incumplimiento, entre las que estarían en su caso, las relacionadas con la normativa de protección de datos personales.

El compromiso de confidencialidad incluye, sintéticamente, las siguientes obligaciones:

- ▶ El cumplimiento de la normativa de protección de datos personales.
- ▶ Actuar conforme a los procedimientos normalizados de trabajo establecidos por el promotor, accediendo únicamente a la información estrictamente necesaria (principio de minimización).
- ▶ Cumplir la totalidad de medidas establecidas en el protocolo de seguridad.

Por su parte, el protocolo de seguridad de la conexión remota para el entorno de monitorización de los ensayos clínicos incluye garantías detalladas sobre los requerimientos de administración de acceso para el monitor; la arquitectura y conexión propuesta; el cifrado; la gestión de “Logs” y auditoría; la gestión de vulnerabilidades; los requerimientos sobre el equipo a utilizar que deberá ser únicamente el que se le hubiera facilitado, no permitiéndose la instalación de ningún componente de software y el entorno de trabajo.

## 3. El marco de Responsabilidad Social de la AEPD

La Agencia Española de Protección de Datos ya ha realizado en su segundo año de cumplimiento el 65% de las 103 acciones previstas en su Marco de Actuación de Responsabilidad Social 2019-2024 aprobado en marzo de 2019, todas ellas alineadas con los Objetivos de Desarrollo Sostenible (ODS) de Naciones Unidas para la Agenda 2030, de los que un 70% tiene que ver con la sociedad; un 13% con empleados; un 10% con el medio ambiente y un 7% con el buen gobierno y la transparencia.

Los datos reflejan que en menos de dos años se ha alcanzado un alto grado de ejecución en todos los ejes, especialmente en lo que respecta a las iniciativas relacionadas con la ciudadanía, educación y menores e igualdad de género. Las cifras sobre el grado de ejecución del Marco de Actuación de RS de la AEPD durante 2020 está disponible en el Anexo de la presente Memoria, y en todo caso en el *espacio web* dedicado a este ámbito.

A continuación, se exponen las actuaciones más destacadas de la AEPD en 2020:

### 3.1. Igualdad de género y violencia digital

Una línea fundamental donde la Agencia ha impulsado una acción decidida en el campo de la responsabilidad social es la igualdad de género, en donde se engloban un total de 16 iniciativas en 2020. De esta forma, la AEPD refuerza su compromiso con la defensa de la mujer y la igualdad en todas sus formas, así como con el respeto de la legislación vigente en dicha materia adoptando todas las acciones necesarias, dentro de sus competencias, frente a este tipo de conductas, donde además de la agresión física o psicológica producida, se agrava sustancialmente el daño a la persona en ocasiones con la grabación de las imágenes y su difusión en las redes sociales. Es importante tener en cuenta que, además de la responsabilidad penal, los agresores cometen

infracción administrativa de la normativa de protección de datos al vulnerar además su privacidad. Estas conductas podrían ser sancionadas con multas de hasta veinte millones de euros con la nueva normativa aplicable.

Estas iniciativas se alinean primordialmente con el ODS 5, que pretende asegurar la participación plena y efectiva de las mujeres y la igualdad de oportunidades de liderazgo a todos los niveles decisorios en la vida política, económica y pública (meta 5.5).

En esta línea de actuación, se destacan a continuación las iniciativas impulsadas por esta Agencia tendentes a la promoción de la igualdad desde el punto de vista de la protección de datos y la protección de la privacidad de aquellas personas que hayan sufrido violencia digital:

#### 3.1.1 Canal prioritario para comunicar de forma urgente la difusión de contenido sensible o violento y solicitar su retirada

La Agencia Española de Protección de Datos ha creado un Canal prioritario para comunicar la difusión ilícita de contenido sensible, una herramienta con la que se pretende dar una respuesta rápida en situaciones excepcionalmente delicadas, como aquellas que incluyen la difusión de contenido sexual o violento.

En situaciones excepcionalmente delicadas, cuando las imágenes incluyan contenido sexual o muestren actos de violencia, poniendo en alto riesgo los derechos y libertades de los afectados, especialmente mujeres supervivientes a la violencia de género o menores, los canales ofrecidos por los prestadores de servicios online pueden no resultar lo suficientemente eficaces y rápidos para evitar la difusión continuada de las imágenes.



El objetivo del *Canal prioritario* es hacer frente a estas situaciones, estableciendo una vía en la que las reclamaciones recibidas son analizadas prioritariamente, permitiendo que la Agencia, como Autoridad independiente, pueda adoptar, si es preciso, medidas urgentes que limiten la continuidad del tratamiento de los datos personales.

El lanzamiento de este Canal, en septiembre de 2019, fue respaldado por la firma de seis Protocolos de colaboración con la Vicepresidencia del Gobierno, los Ministerios de Igualdad, Interior, Educación y Trabajo, la Fiscalía General del Estado y el Consejo General de la Abogacía.

En cuanto a las cifras 2020 sobre la utilización del Canal Prioritario, figuran recogidas en el Anexo de la presente Memoria.

### ▲ 3.1.2. El Canal Prioritario en Iberoamérica. Iniciativa con EurosociAL

Hay que destacar que este instrumento de lucha contra la violencia digital ha sido acogido en este año en Iberoamérica a través del proyecto sobre “Fortalecimiento de la estrategia de lucha contra la violencia de género en relación con las niñas, adolescentes y mujeres en internet”, que está financiado por el programa de la Unión Europea EurosociAL+, en su línea de género e igualdad.

Son socios de esta iniciativa las Autoridades de Protección de Datos de México (INAI, como socio líder, INFOEM e INFOCDM); España (AEPD), Colombia (SIC), Uruguay (URCDP), Perú (ANPD), Costa Rica (PRODHAB) y Portugal (CNPD).

Esta iniciativa tiene como objeto identificar posibles actuaciones de las Autoridades Iberoamericanas de protección de datos que contribuyan a erradicar, desde una perspectiva tanto preventiva como reactiva, las cada vez más frecuentes situaciones de violencia en internet con especial incidencia en la mujer y en los menores y adolescentes en el ámbito escolar.

En concreto, la iniciativa proyectada se desglosa en dos grandes ejes:

#### **A) Eje preventivo. Educación digital**

Tiene como objetivo la elaboración de materiales curriculares para lograr la incorporación de la educación digital en los planes de estudio. Fundamentalmente con esta línea de actuación se trata de promover la creación de un gran repositorio iberoamericano sistematizado y ordenado mediante criterios pedagógicos y docentes con los materiales, recursos y herramientas sobre cuestiones relacionadas con la educación digital. La referencia de este eje del proyecto es la iniciativa AseguraTIC, de la que se hablará con detalle en el siguiente apartado.

#### **B) Eje reactivo. Acciones para combatir de forma efectiva la violencia en internet**

Este segundo bloque de acciones está orientado a luchar de una forma activa, desde las competencias propias de las Autoridades de Control, contra aquellas conductas que instigan y generan violencia en internet, especialmente contra las mujeres.

Se trata de poner las competencias que legalmente tienen atribuidas las Autoridades de control al servicio de la lucha contra esta plaga que se va incrementando en internet, tanto entre los jóvenes como en los adultos. En este sentido, el Canal Prioritario de la AEPD, adaptándolo a sus peculiaridades, puede servir de referencia para las autoridades iberoamericanas de protección de datos.

El programa ha empezado a ejecutarse en octubre de 2020, y tiene un plazo de vigencia de un año. En este contexto, el pasado 26 de noviembre se celebró el webinar “El Canal Prioritario de la AEPD: una contribución de las Autoridades de Protección de Datos a la lucha contra la violencia digital en las mujeres, niñas y adolescentes”, organizado por el INAI de México en el marco de las actividades del proyecto de EurosociAL. El acto contó como ponentes con la Directora de la Agencia y la Subdirectora General de Inspección de Datos. Se desarrolló por invitación a los socios del proyecto a otras Autoridades de la RIPD e instituciones de México.



### ▲ 3.1.3. Web de ayuda a las mujeres supervivientes a la violencia de género y violencia digital

En esta web se dan pautas para que puedan detectar si alguien ha podido manipular sus dispositivos para controlar y acceder a datos sensibles y se dan recomendaciones para proteger la privacidad de los dispositivos móviles, vinculado al *Canal prioritario*, proporcionando información sobre cómo ejecutar la solicitud de retirada de contenidos en los buscadores, foros, blogs y redes sociales más populares.

Finalmente, hay un enlace a otros contenidos de interés, además de recursos de apoyo desarrollados por la Agencia y por otros organismos, orientados a proporcionar información y ayuda a las mujeres supervivientes y concienciar y sensibilizar a la sociedad en la lucha contra la violencia de género y la adquisición de la igualdad real y efectiva.

**El número de accesos de esta página durante 2020 ha superado los 17.000.**

### ▲ 3.1.4. La protección de datos como garantía en las políticas de prevención del acoso digital en el ámbito laboral: Recomendaciones de la AEPD

La Agencia, desde su doble vertiente de autoridad de control y de centro de trabajo, ha considerado procedente formular unas recomendaciones dirigidas a Empresas y Administraciones Públicas que permitan prevenir y trabajar para la erradicación de conductas que, mediante la utilización ilícita de datos personales, supongan el ejercicio de acoso sobre los trabajadores y las trabajadoras en cualquiera de sus modalidades.

En estas recomendaciones, en primer lugar, se enumeran las conductas que suponen ciberacoso, especialmente cuando se realizan mediante el uso de datos personales. Se especifica que el acoso a través del móvil entre compañeros es un riesgo laboral y que la empresa debe tener una conducta activa frente a este tipo de conductas.

El trabajador que acose puede tener responsabilidad civil, penal, administrativa por infracción de protección de datos y laboral por acoso. Se pone el acento en que su realización no supone solo la comisión de un ilícito por quien las comete, sino también para la organización que, teniendo conocimiento de estos tratamientos de datos ilícitos, no reaccione con actuaciones dirigidas a erradicarlos.

**El número de descargas de este documento durante 2020 ha sido de casi 7.400.**

## 3.2. Educación y menores

La Agencia ha desarrollado un amplio abanico de iniciativas relacionadas con la educación y los menores, parte de ellas se describen en los apartados de Herramientas de Comunicación y Educación y menores. Dichas iniciativas se completan con las que se describen a continuación:

### ▲ 3.2.1. Recomendaciones orientadas a evitar el acceso de menores a contenidos inapropiados en internet

La AEPD ha publicado una *nota técnica con recomendaciones para promover el uso seguro de internet por parte de los menores y evitar el acceso a contenidos inapropiados*, debido a que durante el confinamiento los menores han pasado más tiempo del habitual conectados a internet, en ocasiones sin supervisión adulta.

El documento, dirigido a madres y padres, entidades y desarrolladores, y editores de contenido, recoge las distintas opciones que pueden ayudar a impedir el acceso de los menores a este tipo de contenido, o al menos de limitar su exposición. Incluye también un conjunto de recomendaciones y consejos a las madres y padres sobre cómo educar a los menores acerca de los riesgos para su privacidad y su seguridad en el uso de tecnologías móviles; limitar el tiempo de uso de los dispositivos conectados, entre otras.

Respecto a la industria, la AEPD recomienda aplicar el principio de minimización de datos, estableciendo mecanismos que permitan activar y desactivar cada una de esas funcionalidades en función de las necesidades de cada familia; minimizar los permisos, no solicitando acceder a recursos del sistema que sean innecesarios para las funcionalidades que se van a utilizar; establecer garantías en los servicios en la nube, o aplicar medidas de seguridad, entre otros.

### ▲ 3.2.2. Iniciativa sobre adicciones digitales de los jóvenes

Como denuncian numerosos informes y testimonios, el uso por los menores, niños y adolescentes de las tecnologías de la información y comunicación ha aumentado en cuanto al tiempo que le dedican, llegando a adquirir en algunos casos carácter adictivo.

La AEPD ha convocado diversas reuniones de trabajo con administraciones, organizaciones y expertos en esta materia con el objetivo de ofrecer a los menores, padres, profesores y otros colectivos que participen en la vida de los menores una hoja de ruta para conseguir detectar posibles adicciones a las TIC, que constase de una herramienta de diagnóstico y medidas de prevención, así como, en la medida de lo posible, una relación de recursos a los que acudir.

## 3.3. Innovación y protección de datos

En este ámbito se pueden destacar las siguientes actuaciones de la Agencia:

### ▲ 3.3.1. Pacto Digital para la protección de las personas

La iniciativa más destacada durante 2020 ha sido la preparación de la iniciativa denominada Pacto Digital para la Protección de las Personas, lanzada en enero de 2021 y con la que se pretende poner en valor la privacidad como un activo que las organizaciones, públicas y privadas, que deberán tener especialmente en cuenta a la hora de diseñar sus políticas y sus estrategias.

Con la referida iniciativa se pretende resaltar que los derechos en el ámbito digital son necesarios y que tras un derecho puede existir también una obligación. Para ello, es necesario que todos los actores implicados en el ámbito digital, los ciudadanos y los responsables -públicos y privados- conozcan las responsabilidades en las que se puede incurrir.

La adhesión a esta iniciativa supone para las organizaciones adheridas asumir una serie de compromisos que figuran relacionados a lo largo de los tres documentos que la integran.

El documento base es la Carta de Adhesión, mediante la cual la entidad firmante se compromete, de una parte, a implantar en sus respectivas organizaciones los principios y recomendaciones contemplados en los otros dos documentos que conforman el Pacto, y, de otra, como compromisos adicionales, a difundir entre sus empleados y usuarios el canal prioritario para la eliminación urgente de contenidos sensibles y violentos en internet, así como otros recursos y herramientas que la AEPD ha puesto a disposición de los sectores público y privado y de la ciudadanía para ayudar a la sensibilización sobre el valor de la privacidad y la importancia del tratamiento de los datos personales, también en el entorno laboral.

El segundo documento es el Compromiso por la responsabilidad en el ámbito digital, que contiene las obligaciones específicas de las organizaciones en el ámbito digital y las responsabilidades ante el eventual incumplimiento de las mismas, especialmente las conductas relacionadas con la llamada violencia digital: de carácter administrativo por infracción de la normativa de protección de datos; civiles y penales; disciplinarias por infracción de la normativa laboral y de prevención de riesgos laborales, e incluso disciplinarias en el ámbito educativo por la realización de conductas como el acoso al alumnado, su intimidación, humillación, las ofensas graves, su discriminación, o de violencia realizadas a través de redes sociales y servicios equivalentes en internet.

Finalmente, el documento recoge algunos principios que, desde la perspectiva de la ética y la protección de datos, la llamada ética digital, deberían tenerse especialmente en cuenta al diseñar e implantar los nuevos desarrollos tecnológicos.

El tercer y último documento que integra la iniciativa de la AEPD, y el que, sin duda, incide con mayor intensidad en el sector editorial y, en general, de los medios de comunicación, es el Decálogo de buenas prácticas en privacidad para medios

de comunicación y organizaciones con canales de difusión propios, con el que se pretende fijar una pautas de actuación en lo que se refiere al tratamiento de imágenes de contenido violento y sensible, sin afectar en modo alguno a la libertad de información y expresión.

El proceso de adhesión se puso en marcha el 11 de noviembre, dirigido en una primera etapa a 60 organizaciones y asociaciones privadas, fundaciones, asociaciones de prensa y grupos audiovisuales. Durante el año 2020 se ha iniciado el proceso de suscripción del Pacto, cuya presentación se ha realizado en enero de 2021, con motivo del Día internacional de protección de datos.

### ▲ 3.3.2. Privacidad, Innovación y Género

#### **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 promovido a lo largo de 2020 un ciclo de seis debates (webinarios) sobre “Innovación y protección de datos. Mujer y ciencia”, con el que se pretende abrir un debate riguroso sobre temas de actualidad.

El ciclo se abrió el 28 de mayo con la ponencia “*Innovación, Protección de Datos y Salud (I). Soluciones tecnológicas para combatir la COVID-19*” a cargo de la doctora Carmela Troncoso, 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.

El 30 de junio tuvo lugar la segunda de las ponencias del ciclo “*Innovación, protección de datos y salud (II). Bioética y Derecho. Proteger la privacidad en la sociedad digital post COVID-19*”, que fue impartida por la doctora Itziar de Lecuona (línea de investigación en Bioética y Derecho). Con su presencia se ha pretendido promover un debate sobre las consecuencias que ha podido traer la COVID-19 para la privacidad, promoviendo



la reflexión sobre cómo proteger mejor el derecho fundamental a la protección de datos en la “nueva realidad”.

La tercera de las ponencias tuvo lugar el día 24 de septiembre y estuvo a cargo de Gemma Galdón con el título de *“Innovación, protección de datos y transformación digital. Inteligencia artificial ética y auditable: buenas y malas prácticas”*. Gemma Galdón es analista de políticas públicas especializada en el impacto social, legal y ético de las tecnologías intensivas en datos personales y en la auditoría de algoritmos.

El 22 de octubre la cuarta ponencia fue impartida por Soledad Antelada bajo el título *“Innovación, protección de datos y transformación digital: el futuro de la ciberseguridad”*. Soledad Antelada es ingeniera informática del departamento de ciberseguridad de Berkeley Lab, California.

Sara Degli- Esposti fue la ponente del quinto webinar que llevó por título *“Smart cities: más allá de la seguridad, la privacidad de los ciudadanos”* que se celebró el 12 de noviembre. Sara Degli es investigadora Juan de la Cierva en el Instituto de Políticas y Bienes Públicos (IPP) del CSIC.

La sexta ponencia tuvo lugar el día 1 de diciembre con el título *“Innovación, protección de datos y transformación digital: ¿Cómo la inteligencia artificial utiliza los datos?”*, que fue impartido por Elena González Blanco, que es General Manager de Europa en Insurtech Covervallet, investigadora de prestigio internacional y, entre otros proyectos, lidera POSTDATA, proyecto de investigación europeo de excelencia sobre ERC sobre tecnología lingüística y web semántica.

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 *seis webinars del Ciclo* están colgados en la página web de la Agencia. El ciclo tendrá continuidad durante 2021.

## 3.4. Compromiso con la ética y la integridad pública

### ▲ 3.4.1. Código ético. Canal ético

Con fecha 20 de enero, la AEPD aprobó su *Código Ético*, en el que recoge las normas internas de conducta, valores y principios que deben regir la actuación de sus empleados y directivos. Con la aprobación de este texto la Agencia da cumplimiento a uno de los principales compromisos asumidos en el *Marco de Actuación de Responsabilidad Social y Sostenibilidad 2019-2024*, aprobado en marzo de 2019.

El Marco de Actuación de Responsabilidad Social de la AEPD recoge en su segundo eje una sólida apuesta por impulsar una política de cumplimiento (compliance) basada en valores como la transparencia, el buen gobierno, la integridad o la rendición de cuentas, que incluye entre otras medidas la aprobación de este código ético y de conducta.

Esta iniciativa forma parte de un conjunto de actuaciones orientadas a reforzar la posición institucional de la AEPD y la confianza de los ciudadanos, entre las que se recogen la regulación de los sistemas de información de denuncias internas incluidos en la Ley orgánica 3/2018. Así, la AEPD ya ha puesto en marcha un canal interno para atender consultas y denuncias, que pueden hacerse de forma anónima y con todas las garantías de confidencialidad, tanto por los empleados, como por los propios ciudadanos, sobre cualesquiera conductas contrarias al código.

El Código Ético aprobado por la Agencia recoge asimismo prescripciones relativas al uso de los bienes y recursos por parte de los altos cargos de la Agencia, estableciendo la necesidad de observar una especial austeridad en sus gastos de representación, vinculando exclusivamente la utilización de recursos públicos con el ejercicio de las actividades y funciones públicas.

Por otra parte, el texto dispone que, con carácter general, el personal de la Agencia no acudirá en representación de la AEPD a cursos, conferencias,



jornadas o eventos similares organizados por empresas o asociaciones empresariales, salvo que en dicha asistencia haya un interés público, en cuyo caso el personal que participe no podrá percibir retribución económica alguna. Los altos cargos de la Agencia no podrán, en ningún caso, recibir una compensación económica adicional por intervenir en cualquier evento, público o privado.

Entre otras actuaciones, el Código Ético también contempla medidas para favorecer un entorno de trabajo libre de acoso e intimidación, activando las actuaciones previstas en los protocolos aprobados por la AEPD para hacer frente a situaciones de acoso laboral y sexual o por razón de sexo.

Asimismo, incluye un conjunto de normas de conducta orientadas a evitar situaciones de conflicto de interés, tales como abstenerse de utilizar el cargo para agilizar o entorpecer procedimientos o para nombrar personal con quien pueda haber un conflicto de interés familiar y, en general, para desarrollar cualquier actividad ajena a las responsabilidades de la Agencia de modo que pueda interferir o resultar contraria a los intereses públicos.

Junto con el texto del código, se ha aprobado una Guía para facilitar al personal de la AEPD la puesta en práctica de determinadas normas de conducta, con algunos de los casos que con más frecuencia se producen en las organizaciones públicas.

Finalmente, con el fin de velar por una adecuada puesta en práctica y cumplimiento de los principios de actuación y normas de conducta del Código Ético, se ha creado el Comité de Ética que, como órgano colegiado, establecerá las medidas y procedimientos necesarios para supervisar y evaluar el cumplimiento efectivo de los valores, principios de actuación y normas de conducta recogidos en el Código y las políticas internas que los desarrollen. El Comité de Ética está integrado por tres miembros: un presidente y dos vocales, personal de la AEPD.

**La AEPD se convierte así en una de las primeras organizaciones públicas de la AGE que disponen de un Código Ético y de un canal interno de denuncia.**

Durante el primer trimestre de 2021 está previsto un Taller práctico impartido por la Asociación Española de Compliance (ASCOM), con la que hay suscrito un protocolo de colaboración, para seguir capacitando y sensibilizando a los empleados y empleadas de la AEPD en el estricto cumplimiento de las medidas contempladas en el código ético.

### 3.5. Compromiso con las empleadas y empleados

#### ▲ 3.5.1. Actuaciones en favor de la igualdad de empleadas y empleados

Entre las actuaciones más destacadas de esta Agencia en relación con sus empleadas y empleados, cabe señalar las siguientes:

#### **Plan de Igualdad de la AEPD**

La aprobación de este plan ha supuesto el marco para la realización de un diagnóstico de la situación de la igualdad en el ámbito de la entidad, con la inclusión de un conjunto de medidas para impulsar este principio, favoreciendo que la igualdad de género se incorpore de forma transversal a la toma de decisiones en la AEPD.

La AEPD se compromete a desarrollar las medidas necesarias para que la igualdad entre sus empleadas y empleados sea real y efectiva, y para ello, se han adoptado hasta el momento distintas iniciativas, pero para completar estas iniciativas, en los que se refiere a los procesos internos de la AEPD, se ha considerado necesario dar un paso más con la aprobación de un plan propio que garantice el derecho a la igualdad. Este Plan es el resultado de un proceso de reflexión sobre las necesidades existentes en el organismo para garantizar la igualdad efectiva, y para ello se ha

realizado un diagnóstico de la situación y posición de mujeres y hombres dentro de la organización para identificar posibles discriminaciones y desigualdades que requieran adoptar, en su caso, medidas para su eliminación y corrección. A pesar de haber logrado objetivos importantes, sobre todo en materia de conciliación con el teletrabajo, se han detectado algunas acciones específicas que pueden contribuir a seguir impulsando dentro de la AEPD el principio de igualdad entre hombres y mujeres.

### Mayor representación de la mujer en los puestos de la AEPD (niveles 28 a 30)

La evolución en los puestos niveles 28 a 30 entre hombres y mujeres ha sido la siguiente:

Año	Hombres	%	Mujeres	%	TOTAL
2019	27	69%	11	31%	36
2020	24	62%	15	38%	39

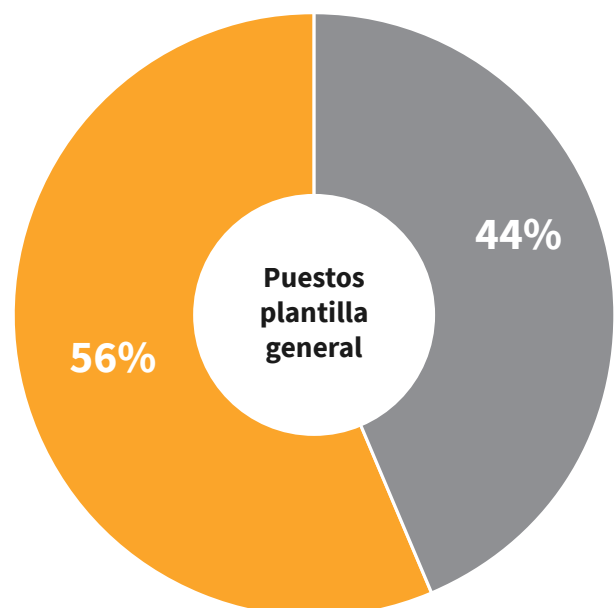
### Programa de formación específica de las empleadas y empleados de la AEPD en materia de igualdad de género

En el marco del programa de formación interna, se ha impartido la primera edición del Curso “Responsabilidad Social e Igualdad: el encaje de la privacidad” por parte del Ministerio de Igualdad. En él participaron veinte empleados y empleadas que fueron invitados por el área de Recursos Humanos en representación de cada una de las unidades de la Agencia. Continuará durante 2021.

En la plantilla en general (sin distinción de nivel):

- Mujeres
- Hombres

Hombres	94	56%
Mujeres	75	44%



### 3.5.2. Actuaciones en favor de la conciliación de la vida personal, laboral y familiar

#### ■ Ampliación del Programa de teletrabajo de la AEPD

El teletrabajo, una iniciativa que arrancó en 2017 con un programa piloto, ha contribuido durante estos tres años de manera fundamental a que la conciliación sea una realidad efectiva en la AEPD, posibilitando no sólo el incremento de la productividad de los empleados y empleadas sino también su bienestar.

Con fecha 23 de julio, se ha procedido a ampliar los términos de dicho programa, pasando la práctica totalidad de su plantilla a prestar servicios en régimen de teletrabajo continuado. Así, se flexibiliza el régimen para acogerse a este programa, contemplándose una modalidad fija (régimen general), que supone la realización de hasta el 40% de la jornada (esto es, una o dos jornadas laborales) a distancia. Se contempla, asimismo, una modalidad flexible, que supone el reconocimiento de una bolsa correspondiente a un 40% de la jornada (esto es, de un máximo de 8 días al mes), en la que el empleado podrá prestar sus servicios a distancia. Estos días podrán ser distribuidos a lo largo del calendario mensual con flexibilidad para ser ajustadas a las necesidades del servicio y otras derivadas de sus funciones. Y junto a las modalidades anteriores, se reconoce la posibilidad de prestar servicios en régimen de teletrabajo extraordinario en casos excepcionales, siempre y cuando motivos acreditados de conciliación o enfermedad lo justifiquen, así como la lejanía del domicilio en que reside de manera efectiva el empleado, siempre que concurren también motivos de conciliación. Sólo se considerarán puestos no teletrabajables las funciones de ordenanza.

La incidencia del teletrabajo en relación con la crisis sanitaria de la COVID-19 y la valoración por parte de quienes participan en el mismo se detallan en otro apartado de la Memoria 2020.

#### ■ Jornadas de Teletrabajo

Precisamente, partiendo de esa experiencia positiva, y siendo un referente en la AGE en este ámbito, la AEPD promovió la organización de las jornadas virtuales ‘Nuevos modelos de trabajo, nuevos liderazgos’ tratado de analizar el teletrabajo desde diferentes perspectivas. Organizadas en dos sesiones los días 24 y 26 de junio, la primera de ellas contó con una mesa dedicada al sector público y otra al sector empresarial, mientras que la segunda de las jornadas se dedicó a exponer algunas experiencias prácticas puestas ya en marcha por diferentes entidades.

Con la realización de estas jornadas la Agencia quiso promover el debate sobre cómo el teletrabajo contribuye al fomento de la conciliación y la productividad, analizando también los retos que se presentan para su expansión en las administraciones y empresas españolas, identificando debilidades y generando respuestas prácticas.

La primera de las sesiones contó con una mesa dedicada al sector público y otra al sector empresarial, mientras que en la segunda de las jornadas se expusieron distintas experiencias prácticas puestas ya en marcha por diferentes entidades. El Programa completo y los videos de las dos sesiones están disponible en la página web de la Agencia, en el [site sobre las jornadas](#).

### ■ Suscripción por la AEPD de la Declaración de Teletrabajo e Innovación: 12 compromisos+12 causas”, de Women in a Legal World (WLW)

La AEPD, con fecha 5 de junio, suscribió la ‘Declaración de teletrabajo e innovación: 12 compromisos + 12 causas’ de Women in a Legal World, convirtiéndose en el primer organismo de la AGE adherido a la iniciativa. Esta organización, además de promover el teletrabajo como modalidad para favorecer la conciliación de la vida familiar, personal y laboral, despliega iniciativas encaminadas a impulsar acciones para ayudar al emprendimiento específicamente por parte de las mujeres y el acceso de éstas a carreras STEM.

La ‘Declaración de Teletrabajo: 12 compromisos + 12 causas’ suscrita por la Agencia pretende lograr una conjunción equilibrada entre el teletrabajo y el trabajo presencial. En este sentido, y consciente de que la protección de los datos debe mantenerse en condiciones de teletrabajo, la Agencia ha publicado unas *Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo*, un documento en el que recoge consejos dirigidos tanto a las organizaciones como a los y las trabajadoras. El objetivo de estas recomendaciones, además de dar pautas para que las organizaciones puedan implantarlas, es que la protección de datos no se utilice como una excusa para denegar la adopción del teletrabajo.

#### ▲ 3.5.3. Programa de Voluntariado

### ■ Tablón del Voluntariado

Se ha puesto en marcha en 2020 un Tablón del Voluntariado con la finalidad de lograr una mayor implicación de todo el personal en los objetivos de responsabilidad social que se ha marcado la AEPD. El Tablón, colgado en la intranet de la AEPD, está dividido en dos secciones, la primera dedicada al voluntariado corporativo, en la que se informará de las diferentes acciones de voluntariado que va promoviendo la propia AEPD para sus empleadas y empleados, y la segunda está dedicada a difundir acciones de voluntariado, que se realizarán a título individual, propuestas por el

propio personal de la AEPD, y que consideren que puede ser interesante compartir para promover la participación de otros compañeros y compañeras que puedan tener las mismas inquietudes.

### ■ Colaboración con Cruz Roja

Durante el año 2020 se han desarrollado diferentes acciones de voluntariado corporativo en alianza de Cruz Roja orientadas a colectivos especialmente vulnerables. La primera de ellas tuvo lugar el día 16 de enero, y consistió en un apoyo logístico de 17 empleadas y empleados de la AEPD que colaboró en la clasificación de juguetes recogidos en la Sede de Cruz Roja durante la campaña de navidad de 2019.

Dentro del voluntariado corporativo se ha fomentado la colaboración con Cruz Roja adaptándola a las especiales circunstancias en las que se han desarrollado todas las actividades debido a la pandemia de la COVID-19. Por este motivo se propuso a Cruz Roja realizar actividades de divulgación online orientadas específicamente a los colectivos vulnerables. Estas actividades se materializaron en la realización de cuatro webinarios.

- El primero se celebró el día 20 de octubre y se dedicó a la explicación práctica del Canal Prioritario, dirigido a los referentes de infancia y juventud de Cruz Roja.
- El segundo tuvo lugar el día 10 de noviembre y se dedicó a explicar el funcionamiento de la herramienta FACILITA, y se dirigió a autónomos a los que Cruz Roja ayuda a emprender una actividad por cuenta propia.
- El día 23 de noviembre se celebró el tercer webinar sobre la explicación práctica de la herramienta FACILITA EMPRENDE, dirigido a emprendedores cuya actividad tiene un fuerte contenido tecnológico a los que Cruz Roja ayuda a emprender.
- El cuarto webinar se celebró el 3 de diciembre con el título “Aplicación y dudas en materia de protección de datos”, dirigido al equipo legal de Cruz Roja con el objetivo de resolver sus dudas en materia de privacidad.

### ■ Taller de Voluntariado

El día 10 de diciembre se realizó un taller del voluntariado en el que participaron unos treinta empleados y empleadas impartido por la Fundación “Personas y Empresas” con el objetivo de acercar el voluntariado a todas aquellas personas que trabajan en la AEPD, que tengan interés en este tema, y de difundir las diferentes acciones de voluntariado que pueden llevarse a cabo tanto de forma presencial como online.

### ■ Campaña de Navidad. Colaboración con el Banco de Alimentos

Para la campaña de navidad de este año, se promovió una encuesta entre el personal de la Agencia para que optaran entre cuatro organizaciones que trabajan con colectivos vulnerables, especialmente afectados por la pandemia, resultando elegida la entidad Banco de Alimentos.

A tal efecto, se abrió una cuenta para que las personas trabajadoras en la AEPD pudieran ingresar donativos, alcanzándose casi 3.000 euros correspondientes a 72 donantes, y destinando esa cantidad a la compra de alimentos.

## 3.6. Compromiso con el medio ambiente y la lucha contra el cambio climático

### ■ Cálculo de la huella de carbono

En el año 2019 la AEPD empezó a trabajar en una herramienta que le permitiera obtener una fotografía general sobre el impacto que su actividad tiene en el cambio climático para además determinar los puntos clave de reducción que contribuyan a diseñar una estrategia baja en carbono. Por ello ha calculado su huella de carbono a través de una empresa externa FACTOR CO2, para poder cuantificar y reportar las Emisiones de Gases de Efecto Invernadero (GEI) asociadas a su actividad. Los resultados han sido verificados mediante auditoría realizada por la consultora TUV Rheinland Ibérica ICT, S.A.

Se ha calculado la huella correspondiente a los años 2016, 2017, 2018 y 2019, y se ha procedido a su inscripción en la sección a) de Huella de Carbono y de compromisos de reducción de las emisiones de gases de efecto invernadero de la Oficina Española de Cambio Climático del Ministerio para la Transición Ecológica habiéndosele otorgado el derecho al uso del sello “CALCULO Y REDUZCO 2019” que reconoce el esfuerzo realizado por la organización en su conjunto para la reducción de emisiones de la AEPD.

La inscripción conlleva el compromiso de la presentación de un plan de reducción de emisiones, por lo que se ha presentado el Plan Verde 2020-2025 con el que se pretende desarrollar e implementar una estrategia baja en carbono que permita reducir e incluso compensar nuestra huella, mejorando el comportamiento medioambiental de nuestra organización, profundizando así en el compromiso con el medioambiente y la reducción de emisiones.

Las principales conclusiones del informe son:

- En el ejercicio 2019 la huella total de la AEPD fue, por tanto, de 349,43 tCO<sub>2</sub>e. Según los autores del informe, se trata de unos niveles de emisión muy bajos.
- Para el cálculo se han tenido en cuenta los tres alcances, siendo las emisiones del alcance 3, que lo componen los viajes de negocios; los desplazamientos in itinere de los empleados; los consumibles de oficina; el consumo de agua y los residuos, las que contribuyen de forma mayoritaria a la huella de carbono de la AEPD, constituyendo un 65,83% del total.

### ■ Cláusulas de contratación verde

Como consecuencia de las recomendaciones del estudio para el cálculo de la huella de carbono, se ha impulsado la contratación de una empresa comercializadora para el suministro a la Agencia de energía eléctrica 100% verde.



## 4. Desafíos para la privacidad

### 4.1. Jurídicos

#### 4.1.1. Consultas

En este ejercicio se observa cómo el Reglamento General de Protección de Datos centra las consultas ya no tanto en aspectos novedosos como el nuevo régimen del consentimiento sino en cuestiones que son fruto de la permanente adaptación a la que tanto el sector público como privado se encuentran comprometidos. En efecto, cuestiones como el principio de responsabilidad activa y sus manifestaciones tienen reflejo práctico no solo en los tratamientos de datos en sí mismo considerados, sino también en las normas que regulan procesos de los que se derivan dichos tratamientos.

El RGPD ya no es un recién llegado y muestra de ello es la revisión práctica de conceptos asentados como el responsable y el encargado del tratamiento, que requieren un análisis pormenorizado de su situación actual.

Las categorías especiales de datos y su prohibición general de tratamiento ocupan buena parte de las consultas que se plantearon durante el ejercicio, por cuanto los supuestos de levantamiento de la prohibición hacen una remisión al derecho nacional de los estados miembros, que, en ocasiones, se muestra insuficiente. Se pone así de manifiesto la necesidad de que por los poderes públicos se proceda a una completa revisión normativa, tanto en el ámbito estatal como autonómico, para adaptar determinados tratamientos a las exigencias del RGPD.

Cuestiones clásicas como los tratamientos de categorías especiales de datos, (datos especialmente protegidos) conviven junto con el análisis del riesgo y la evaluación de impacto que requieren los tratamientos de datos adaptados a la nueva realidad fáctica y jurídica. El principio de responsabilidad activa se manifiesta en las consultas que tienen por objeto la permanente revisión de los procesos y organizaciones para la adaptación al nuevo modelo de responsabilidad que supone el RGPD.

Centrándonos ya en las materias concretas que se han tratado, en el ámbito de la estadística y de la realización de encuestas se emitieron los informes que a continuación se citan en los que el Centro de Investigaciones Sociológicas (CIS) solicita el acceso a datos personales de diversas fuentes, ante la imposibilidad de realizar diversos cometidos de modo ordinario por las restricciones consecuencia de la crisis sanitaria de COVID-19.

En el Informe nº 31/2020 se plantea la a raíz de la solicitud del CIS al Instituto Nacional de Estadística (INE) de los teléfonos fijos y móviles de la población seleccionada en determinadas muestras para ejecutar las funciones atribuidas al



CIS, y que habitualmente se realizaban mediante entrevistas presenciales, mediante encuestas telefónicas. El CIS quiere que la información nominativa que proporciona el INE sea completada con los teléfonos fijos y móviles de la población seleccionada en las muestras.

El informe se indica que la consulta adolece de información esencial para ofrecer una respuesta en derecho, y que debería subsanarse a través del correspondiente informe que debe evacuar el DPD en cumplimiento de las funciones que, con carácter general le atribuyen los artículos 37 a 39 del RGPD, concretando aspectos como (i) las concretas encuestas a que se refiere, su inclusión en el Plan Estadístico Nacional y la urgencia de las mismas que impediría demorarlas hasta la finalización del estado de alarma, justificando, de este modo, el acceso a un mayor número de datos (números de teléfono) que en otros casos no son necesarios y pueden suponer una mayor intromisión en el derecho fundamental a la protección de datos personales, permitiendo, de este modo, valorar la proporcionalidad de la medida propuesta, (ii) los concretos datos que se pretenden obtener del INE y la base jurídica en virtud del cual el INE los ha obtenido, así como las finalidades concretas para los que se dispone de los mismos. Esta información es relevante en la medida que lo que pretende el escrito de autorización es que “la información nominativa que nos proporciona el Instituto Nacional de Estadística sea completada con los teléfonos fijos y móviles de la población seleccionada en las muestras”, siendo relevante a estos efectos conocer los datos que ha obtenido el INE, la finalidad y la base jurídica para el tratamiento, en la medida en que el número de teléfono (fijo o móvil) no figura entre los datos del Padrón Municipal, (iii) una breve descripción de la forma en que se realizan las encuestas por el CIS, la normativa que la regula y si la misma contempla la realización de encuestas telefónicas y (iv) la base jurídica que legitimaría la cesión de los datos del INE al CIS, analizando detenidamente si concurren los requisitos del artículo 15 de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública. (LFEP en adelante).

Asimismo, se indica que a dicha consulta debería acompañarse el análisis de riesgos realizado, así como, si se estima probable que el tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas, la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales prevista en el artículo 35 del RGPD.

Como puede observarse, al margen de las cuestiones de fondo planteadas, emerge el cumplimiento de responsabilidad activa, entre cuyas manifestaciones esta no sólo el estatus y funciones del DPD sino el análisis de riesgos, y en caso necesario la realización de la evaluación de impacto.

El Informe nº 35/2020, se plantea a raíz de una solicitud del CIS a la Comisión Nacional de los Mercados y la Competencia (CNMC) para la comunicación de datos a aquella referidos a los teléfonos fijos y móviles, para realizar los estudios previstos en el Plan Estadístico Nacional para los meses en los cuales continúe la crisis sanitaria de la COVID-19, con el compromiso del CIS de garantizar que esta información será tratada de acuerdo a los criterios de secreto estadístico y el derecho fundamental a la protección de datos personales.

Pues bien, al igual que en el informe anterior, se solicita que por parte del CIS subsane las carencias informativas apuntadas para poder otorgar una respuesta en derecho.

En el informe se indica que se observa que con la nueva solicitud cursada a la CNMC, y la del anterior informe al INE, se pretende cruzar los datos del INE con los de la CNMC, es decir, integrar datos personales procedentes de diversas fuentes y obtenidos con finalidades distintas a la ahora pretendida, lo que puede implicar una mayor intromisión en el derecho fundamental a la protección de datos personales, lo que deberá ser debidamente valorado en la información y documentos solicitados.

A continuación, el informe analiza los supuestos en los que la CNMC puede comunicar datos personales de los abonados a servicios de comunicaciones electrónicas, así como la finalidad específica para la que se recaban y se tratan dichos datos, concluyendo que en el caso planteado se está solicitando la comunicación de unos datos personales para una finalidad distinta de la que se habían obtenido.

También se tiene en cuenta que como lo que se pretende es una comunicación de datos entre organismos administrativos, el informe analiza, en primer término, lo dispuesto en la normativa específica y a la jurisprudencia emanada al respecto.

Destacando en primer lugar que la Ley de Bases del Régimen Local, al abordar el tratamiento de los datos del Padrón Municipal prevé la posibilidad de comunicar datos para la elaboración de estadísticas oficiales en los términos de la LFEP y en las leyes de estadística de las comunidades autónomas con competencia en la materia, cosa que no hace la normativa de telecomunicaciones aplicable a la base de datos de la CNMC.

El Informe indica que la información solicitada no tiene la consideración de información estadística, no se trata de información obtenida por la CNMC en el ejercicio de funciones esencialmente estadísticas, sino que la finalidad para la que se han obtenido es para permitir la elaboración de las guías de abonados y garantizar la libre competencia, tal y como se ha visto anteriormente. Y que los datos solicitados por el CIS, no lo son al objeto de su correspondiente tratamiento estadístico, es decir, no se corresponden con el contenido de la información a obtener de acuerdo con las correspondientes encuestas. Los datos serían utilizados como medio de contacto con las personas que van a participar en la encuesta, siendo los datos que ellas soliciten los que serán objeto de las correspondientes operaciones estadísticas.

En cuanto al modo de obtener información, el artículo 12 de la LFEP no comprende expresamente la obtención de la información por vía telefónica, sino que se refiere a dos formas de obtener la información, por correo o por visita personal,

por lo que sería suficiente conocer el domicilio, es decir, datos del padrón municipal y cuyo tratamiento se prevé expresamente en la LRBRL. Por lo que debería justificarse adecuadamente la imposibilidad o ineficiencia de estadística por correo, para valorar la proporcionalidad de la cesión solicitada.

Asimismo en tanto que el CIS está sometido a la Ley 39/2015, de 1 de octubre, de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, (LPACAP) el modo ordinario de comunicación con los administrados es el domicilio facilitado por los mismos o el que pueda obtener por la Administración del Padrón en los procedimientos iniciados de oficio, sin que los administrados estén obligados a facilitar su número de teléfono entre la información que necesariamente ha de contener la solicitud en los procedimientos iniciados a instancia de los mismos. Por lo que no se puede considerar que entre dentro de las expectativas de los interesados que la Administración contacte con los mismos por teléfono.

Finalmente, recuerda que la comunicación de datos entre administraciones públicas, considerando que en ningún caso puede ser masiva o indiscriminada, y que además de cumplirse el test de compatibilidad de finalidades previsto en el artículo 6.4 de RGPD.

Teniendo en cuenta la amplísima incidencia que la cesión propuesta tiene en la privacidad, reitera el Informe la necesidad de que se valoren estos y otros aspectos por el Delegado de Protección de Datos y que sus conclusiones se acompañen en una posterior consulta al objeto de determinar la adecuación de dichas comunicaciones de datos a la normativa sobre protección de datos de carácter personal.

El Informe nº 49/2020 está estrechamente relacionado con los anteriormente citados, por cuanto el CIS pretende acceder a la base de datos de la CNMC referida a los listados de número de teléfono por provincia para el fin exclusivo de la realización de las encuestas preelectorales vascas y gallegas.

En el informe se tienen en cuenta varios elementos como la urgencia derivada de la convocatoria de los procesos electorales, los problemas para ajustar en el tiempo la encuesta en el caso de realizarse por correo y el sesgo que se produciría en el caso de utilizar internet, así como que el CIS justifica, como única alternativa posible, el empleo de medios telefónicos, y concluye que, en el supuesto concreto objeto de esta consulta, y partiendo de la imposibilidad, al menos mientras así resulte de la declaración del estado de alarma, de realizar las consultas presencialmente, la realización de las encuestas telefónicamente resulta proporcionada, siempre que en la obtención de los números de teléfono se adopten garantías adicionales para garantizar la protección del derecho fundamental a la protección de datos personales, como podrán ser que los números de teléfono no están asociados a ningún titular, que no se incluirán los números de teléfono de aquellas personas que hayan ejercitado su derecho a no figurar en las guías accesibles al público, que no serán objeto de tratamiento la totalidad de los números de teléfonos de los abonados de la provincia, sino únicamente el porcentaje que se estima adecuado para garantizar que se ajusta a la muestra correspondiente, que la conservación de los datos sería durante el tiempo necesario para la realización del trabajo de campo, transcurrido el cual se procedería a su eliminación.

El informe considera necesario añadir el resto de garantías propias del ejercicio de la función estadística, como el sometimiento al secreto estadístico o la disociación de los datos desde el momento en que se realiza la encuesta, separando las respuestas dadas por los encuestados de los números de teléfono, así como el resto de medidas técnicas y organizativas apropiadas para garantizar el respeto a los derechos y libertades de los afectados y la adecuación del tratamiento a la normativa sobre protección de datos personales que corresponde adoptar al CIS como responsable del tratamiento, de acuerdo con el principio de responsabilidad proactiva.

Por lo tanto, el informe considera que es posible el tratamiento analizado y que la base legitimadora se encontraría en el artículo 6.1 e) del RGPD y que cumpliendo las cautelas y garantías indicadas, se adecuaría a los principios de limitación de la finalidad y de minimización de datos, así como a la doctrina de Tribunal Constitucional (Sentencia 17/2013, de 31 de enero) antes referida contraria a un acceso masivo e indiscriminado de datos personales en los supuestos de cesiones de datos entre Administraciones Públicas.

Siguiendo con la función estadística y la realización de encuestas, los informes que a continuación se citan analizan, al igual que en los anteriores informes, las solicitudes de acceso a la base de datos de números de abonados a servicios telefónicos de la CNMC, por otros organismos como el Banco de España, o el Ministerio de Cultura y Deporte.

El Informe nº 75/2020 plantea el acceso a la base de datos de la CNMC para realizar por teléfono la Encuesta Financiera de las Familias (la EFF), ante la imposibilidad de realizarla mediante entrevista presencial por las restricciones de la pandemia. La EFF forma parte del Plan Estadístico Nacional y se viene realizando por el Banco de España desde el año 2002.

La Ley de la Función Estadística Pública incluye, dentro de los Servicios Estadísticos del Estado, además del INE y el Consejo Superior de Estadística, a “las unidades de los diferentes departamentos ministeriales y de cualesquiera otras entidades públicas dependientes de la misma a las que se haya encomendado aquella función”, y atribuye a los servicios estadísticos de los departamentos ministeriales, entre otras competencias, en su letra la elaboración y ejecución de los proyectos estadísticos que se les encomiende en el Plan Estadístico Nacional y recuerda que se establecerán por ley las estadísticas para cuya elaboración se exijan datos con carácter obligatorio, como lo son las que formen parte del del Plan Estadístico Nacional. Y además es de aplicación lo dispuesto en el artículo 25 de la LOPDGDD.

Se está ante un supuesto de estadística de cumplimentación obligatoria, incluyéndose el número de teléfono. Por tanto, existe una obligación legal de los ciudadanos previamente seleccionados de facilitar la información solicitada.

Por lo tanto, el tratamiento se encuentra amparado por el RGPD siempre y cuando, el dato sea únicamente utilizado para la realización de la estadística en cuyo ámbito es solicitado.

En el Informe nº 78/2020, se aborda la comunicación de la base de datos de abonados a servicio telefónico de la CNMC al Ministerio de Cultura y Deporte, para la realización de la Encuesta de Hábitos Deportivos 2020, en concreto de los números de teléfono de las personas seleccionadas en la muestra de la Encuesta realizada por el Instituto Nacional de Estadística (INE). Se trata de una estadística de cumplimentación obligatoria, y que consecuencia de la crisis sanitaria de COVID-19 no es posible realizarla de manera presencial.

Al igual que en el anterior informe, es un supuesto de una estadística de cumplimentación obligatoria al estar incluida en el Plan Estadístico Nacional figurando entre la información que se debe facilitar, tal y como indica la consulta, el número de teléfono como instrumento de control de calidad de las gestiones realizadas.

Por lo que se da el visto bueno a la comunicación de datos, recordando que deben cumplirse por el responsable del tratamiento los principios establecidos en el artículo 5 del RGPD. A lo que habría que añadir el resto de las garantías propias del ejercicio de la función estadística, referidas al secreto estadístico o la disociación de los datos desde el momento en que se realiza la encuesta, separando las respuestas dadas por los encuestados de los números de teléfono, así como el resto de medidas técnicas y organizativas apropiadas para garantizar el respeto a los derechos y libertades de los afectados y la adecuación del tratamiento a la normativa sobre protección de datos personales que corresponde adoptar al Ministerio de Cultura como responsable del tratamiento, de acuerdo con el principio de responsabilidad proactiva.

Como puede observarse en relación con la materia analizada el criterio del Gabinete Jurídico de la AEPD ha sido que mientras en los supuestos en que las encuestas resultan obligatorias por ley y siempre y cuando se ofrezcan garantías adecuadas, el tratamiento es conforme a la normativa de protección de datos. Cuando nos encontramos ante otro tipo de cesiones, donde existen múltiples implicaciones en la privacidad de las personas y la existencia de posibles medios alternativos, se hace necesario un estudio profundo de las mismas por el Delegado de Protección de Datos evacuando sus conclusiones en las consultas que se dirijan al Gabinete Jurídico a los efectos de poder dar una respuesta ajustada a Derecho y en su caso, permitir el tratamiento objeto de análisis.

Los informes que se citan a continuación tienen por objeto tratamientos de datos personales relacionados con las funciones sobre la seguridad ciudadana y la persecución de delitos, que tienen encomendadas los Cuerpos y Fuerzas de Seguridad del Estado (CFSE), Jueces y Tribunales y el Ministerio Fiscal.

El Informe nº 13/2020 resuelve una consulta del INE referida a la interpretación que ha de darse a la expresión “por conducto judicial” contenida en el artículo 41.2 de la LOREG, que establece que “Queda prohibida cualquier información particularizada sobre los datos personales contenidos en el censo electoral, a excepción de los que se soliciten por conducto judicial.”, en el sentido de si debe interpretarse restrictivamente, es decir, de modo literal, o puede extenderse a otros supuestos en los que no es órgano judicial el solicitante, sino el Ministerio Fiscal o la Policía Judicial.

El informe tiene en cuenta la doctrina del Tribunal Constitucional referida a que la regulación pormenorizada por el legislador del acceso a los datos de censo electoral deriva de su carácter esencial para la ordenación del ejercicio del derecho de sufragio activo. Y en este sentido el legislador ha optado por limitar el acceso a los datos personales que figuran en el mismo, diferenciando entre aquellas finalidades que guardan relación con lo previsto en la propia LOREG de aquellas otras que no se corresponden con el mismo y a las que se refiere el citado artículo 41.2



Por tanto, partiendo de que la regla general que establece el citado precepto es la prohibición del acceso, la interpretación que debe darse al concepto “conducto judicial”, debe ser restrictiva, entendiendo que el mismo se refiere exclusivamente al acceso por parte de la autoridad judicial.

El informe considera que los límites al derecho fundamental a la protección de datos personales deben establecerse por una norma con rango de ley, previa ponderación por el legislador de los intereses en pugna atendiendo al principio de proporcionalidad, definiendo todos y cada uno de los presupuestos materiales de la medida limitadora mediante reglas precisas, que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, y estableciendo las garantías adecuadas. En el caso analizado, el legislador ha establecido el conducto judicial como una garantía para que pueda procederse al acceso a los datos censales, acceso que, faltando dicho conducto judicial, estaría prohibido. De modo que los principios de certeza y previsibilidad, derivados del principio de seguridad jurídica, exigen interpretar el mismo de manera restrictiva, exigiendo la intervención de un órgano judicial.

También en apoyo a esta conclusión el informe cita la jurisprudencia Constitucional (STC 292/2000; STC 76/2019; STC 14/2003) y europea tanto del Tribunal de Justicia de la Unión Europea como del Tribunal Europeo de Derechos Humanos que acogen el mismo criterio. Así como el criterio de la Junta Electoral Central sobre la interpretación que hace del artículo 41.2 LOREG que es de carácter restrictivo.

A efectos comparativos, el informe pone de manifiesto que en otras normas (la Ley General Tributaria, Ley General de la Seguridad Social, o incluso la Ley Básica de Autonomía del Paciente), se equipara, en determinados supuestos, el régimen de acceso a los datos personales por los órganos jurisdiccionales y el Ministerio Fiscal para la investigación y persecución de los delitos públicos, e incluso existen otras normas en las que se incluye específicamente a la policía judicial, como la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN, sin embargo esa circunstancia no se da en la LOREG.

Por todo, en tanto en cuanto no se proceda a la modificación del artículo 41.2 de la LOREG, el acceso pormenorizado a los datos del censo electoral por el Ministerio Fiscal y la policía judicial requerirá del mandamiento judicial previo, debiendo interpretarse el concepto “conducto judicial” de manera restrictiva, limitado a los supuestos en los que ha habido una intervención judicial previa.

El Informe nº 25/2020 se plantea la comunicación por las FCSE a la Comisión Estatal contra la Violencia, el Racismo, la Xenofobia y la Intolerancia en el Deporte, la Liga Nacional de Fútbol Profesional (“LaLiga”) y los Clubes de primera y segunda división de la competición organizada por la Liga Nacional de Fútbol Profesional, de los datos personales de aquellos aficionados identificados y/o detenidos por las FCSE con motivo de su participación en actos violentos relacionados con el deporte.

Respecto a la base jurídica que sería aplicable, el informe se centra en que los tratamientos de datos de carácter personal que se lleven a cabo por las Administraciones públicas encontrarán su legitimación, con carácter general, en las letras c) y e) del artículo 6.1 del RGPD y quedan sujetos al resto de principios contenidos en el artículo 5.1. del mismo.

La ley aplicable al presente caso, es la Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte, y por lo tanto, los únicos supuestos de los invocados que legitimarían la comunicación a las personas organizadoras de las competiciones deportivas los datos personales de personas físicas identificadas sería el previsto en la letra h) del artículo 3.2., en cuanto impone una obligación respecto de las personas “que hayan incurrido” en las conductas tipificadas por la norma, así como el artículo 3.3, sobre la prohibición de acceso a recintos deportivos, establecida en sus artículos 24 y 25.

Asimismo, el informe señala que se prevé la existencia de un Registro de Central de Sanciones donde se inscribirán los datos personales de los sancionados, estableciéndose que las sanciones serán comunicadas por el órgano sancionador al propio registro y a los organizadores de los

espectáculos deportivos, con el fin de que éstos verifiquen la identidad en los controles de acceso por los medios que reglamentariamente se determinen.

Por consiguiente, el informe considera que el acceso a los datos del registro y la comunicación de las sanciones en los términos vistos se encontraría legitimadas en dichos preceptos, en los términos previstos reglamentariamente y respetando siempre, como señala el propio artículo 29, la normativa de protección de datos personales siempre que las sanciones resulten ser firmes, ya que son las que figuran en el registro.

De este modo, no está legitimada la comunicación de los datos de las personas identificadas o detenidas por las FCSE con motivo de su participación en actos violentos relacionados con el deporte a la citada Comisión a la LaLiga y a los Clubes de primera y segunda división, estando únicamente prevista la comunicación a las personas organizadoras, por el órgano competente para sancionar, de las resoluciones firmes que impongan la prohibición de acceso a los recintos así como su inscripción en el Registro de sanciones, al que tendrán acceso los particulares que tengan un interés directo y manifiesto, así como las entidades deportivas a efectos de colaboración con las autoridades en el mantenimiento de la seguridad pública con motivo de competiciones o espectáculos deportivos.

Por tanto, la comunicación de los datos personales de los infractores a los clubes y personas organizadoras de los eventos deportivos estaría legitimada en los términos anteriormente señalados, no estando permitida su comunicación en los supuestos en que el procedimiento administrativo no haya finalizado mediante resolución sancionadora dictada por la autoridad competente, ya que la Ley no prevé la cesión de los datos de los presuntos responsables, que no figuran en el registro, que queda limitada, a los órganos competentes para sancionar, salvo que la inscripción se realice en el marco del procedimiento que aún no finalizado lo entienda conforme a la adopción de una medida cautelar.

Otro aspecto que ha sido sometido a consulta ha sido el uso de técnicas de reconocimiento facial y su incidencia en el derecho a la protección de datos personales.

Así, en el Informe nº 36/2020 se plantean una serie de cuestiones por el Consejo Rector de Universidades Españolas (CRUE) relativas al uso de técnicas de reconocimiento facial en la realización de pruebas de evaluación online, partiendo de las restricciones derivadas de la crisis sanitaria ocasionada por la COVID-19, que ha determinado la migración de todas las actividades docentes a entornos online.

La consulta parte de un elemento determinante en la prestación del servicio público de educación superior consiste en la verificación objetiva de los conocimientos de los estudiantes, la presencia física en el aula del profesorado impide que, por ejemplo, un estudiante pudiera abandonar su sitio siendo suplantado en su identidad por otra persona, o que un estudiante realizara la prueba de evaluación haciéndose pasar por otro. Sin embargo, esta posibilidad de control y vigilancia se desaparece por completo cuando se trata de realizar un examen online desde el propio domicilio del estudiante.

Las técnicas de reconocimiento facial permiten asegurar la identificación unívoca de la persona examinada e incluso detectar expresiones faciales que identificaran un comportamiento anómalo.

En su nivel más simple son capaces de establecer un patrón facial de la persona que inicia el examen frente a una pantalla y garantizar tanto que la persona no se ha desplazado o abandonado su sitio frente al terminal durante el periodo asignado a la realización de la prueba, como que no ha sido sustituida por persona distinta.

Como punto de partida el informe comienza señalando que la AEPD ya se ha pronunciado en relación a los tratamientos de datos personales derivados de la necesaria evaluación de los alumnos, entendiendo, con carácter general, que los mismos se encontrarían amparados por el artículo 6.1.e) del RGPD, como consecuencia de la existencia de un interés público derivado de

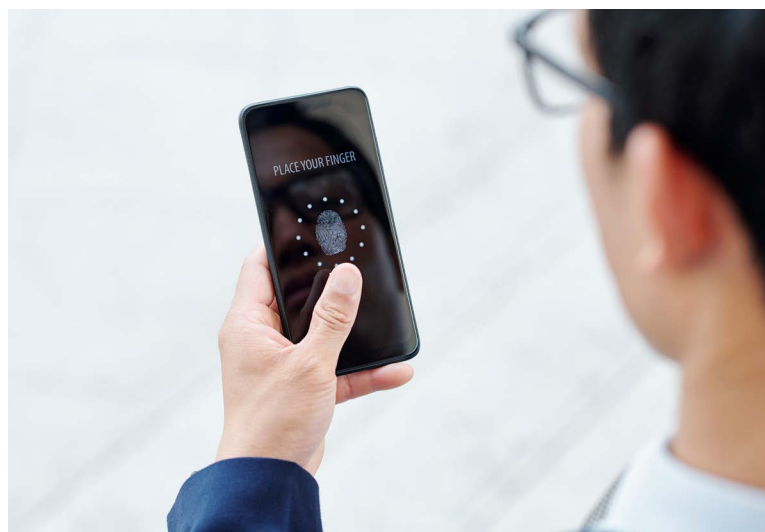
la configuración de la educación superior como un servicio público por la Ley de Ordenación Universitaria (LOU), si bien deben respetarse en todo caso los principios relativos a la protección de datos recogidos en el artículo 5 del RGPD, correspondiendo a cada universidad, en virtud de su autonomía y del principio de responsabilidad proactiva, velar por el adecuado cumplimiento de los mismos. (Informes 30/2019 y 63/2019). Y recuerda el necesario respeto del principio de proporcionalidad en relación con el tratamiento que se pretende llevar a cabo.

Así la existencia de un interés público 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, (Artículo 6. 2 y 3 del RGPD) así como a los ya citados principios del artículo 5 del RGPD, especialmente a los de limitación de la finalidad y minimización de datos. Y en el caso de que vayan a ser objeto de tratamiento algunos de los datos personales incluidos en las categorías especiales de datos a los que se refiere el artículo 9.1. del RGPD, que concurra alguna de las circunstancias contempladas en su apartado 2 que levante la prohibición de tratamiento.

Dicho lo anterior, los datos biométricos solo constituirían una categoría especial de datos en el caso de que se sometieran a un tratamiento técnico específico dirigido a identificar de manera unívoca a una persona física.

El informe cita la distinción entre identificación biométrica y verificación/autenticación biométrica que establecía el Grupo del Artículo 29 en su Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, al objeto de aclarar las dudas interpretativas que surgen respecto a la consideración de los datos biométricos como categorías especiales de datos:

**Identificación biométrica:** la identificación de un individuo por un sistema biométrico es normalmente el proceso de comparar sus datos biométricos (adquiridos en el momento de la identificación) con una serie de plantillas biométricas almacenadas en una base de datos (es decir, un proceso de búsqueda de correspondencias uno-a-varios).



**Verificación/autenticación biométrica:** la verificación de un individuo por un sistema biométrico es normalmente el proceso de comparación entre sus datos biométricos (adquiridos en el momento de la verificación) con una única plantilla biométrica almacenada en un dispositivo (es decir, un proceso de búsqueda de correspondencias uno-a-uno).

Por lo que debe interpretarse que el concepto de dato biométrico incluiría ambos supuestos, tanto la identificación como la verificación/autenticación. Sin embargo, y con carácter general, los datos biométricos únicamente tendrán la consideración de categoría especial de datos en los supuestos en que se sometieran a tratamiento técnico dirigido a la identificación biométrica (uno-a-varios) y no en el caso de verificación/autenticación biométrica (uno-a-uno).

Teniendo en cuenta que en la consulta no se concretan qué métodos de reconocimiento facial al objeto de proceder a la verificación de la identidad se utilizan, se analiza las técnicas que, en la práctica, están utilizando las universidades, y se observa que se busca evitar la suplantación de su identidad, no solo en el momento inicial, sino a lo largo del desarrollo de toda la actividad, para lo cual se graba la misma y se van realizando diferentes capturas que se comparan con la información biométrica previamente almacenada en sus bases de datos. Además, se incluye el tratamiento de otro tipo de datos biométricos (como las pulsaciones en el teclado) y de datos no

biométricos, como la grabación del entorno en el que se encuentra el alumno, así como el acceso al micrófono para la grabación de sonidos.

Por tanto, atendiendo a las circunstancias concretas, que implican el tratamiento de diferentes tipos de datos biométricos y en los que el reconocimiento facial no se realiza en un momento determinado sino que se realiza de manera continuada, lo que puede implicar, asimismo, el tratamiento de los datos biométricos de un tercero para su comparación con los del alumno al objeto de identificar una posible suplantación, el informe concluye que los procesos de reconocimiento facial empleados para la realización de evaluaciones online implican el tratamiento de datos biométricos con la finalidad de identificar unívocamente a una persona física.

Por lo que estamos ante un tratamiento de categorías especiales de datos, lo que implica que para que el tratamiento sea conforme al RGPD debe darse algún supuesto que levanta la prohibición de tratamiento de este tipo de datos.

El informe considera adecuado el consentimiento siempre y cuando se dieran los requisitos que el RGPD establece, y se centra en su carácter de “libre” que implica elección y control reales por parte de los interesados. Es decir, si el sujeto no es realmente libre para elegir, se siente obligado a dar su consentimiento o sufrirá consecuencias negativas si no lo da, entonces el consentimiento no puede considerarse válido. No sería admisible, en ningún caso, es que como consecuencia de la denegación del consentimiento se denegara la posibilidad de matriculación o de acceder a la evaluación o cualquier otra consecuencia negativa importante para el alumno.

El informe recuerda el principio de autonomía universitaria en el sentido de que corresponde a estas determinar en sus normas de evaluación y en sus planes de formación los procedimientos de evaluación que acrediten la igualdad entre los alumnos que consientan el tratamiento de sus datos biométricos y los que no lo hagan. Únicamente de este modo, el consentimiento podría legitimar de dicho tratamiento.

A continuación, se analiza la posibilidad de entender la concurrencia de un interés público esencial a los efectos de excepcionar la prohibición de tratamiento de las categorías especiales de datos. Donde cobra especial relevancia el adjetivo de “esencial” que viene a cualificar dicho interés público, habida cuenta de la importancia y necesidad de mayor protección de los datos tratados.

El informe cita la doctrina constitucional que interpreta este carácter de esencial y establece como debe ser la norma en que se base su aplicación (Sentencia núm. 76/2019 de 22 mayo y Sentencia núm. 14/2003, de 28 de enero), para concluir que el tratamiento de datos biométricos al amparo del artículo 9.2.g) RGPD requiere que esté previsto en una norma de derecho europeo o nacional con rango de ley que respete en todo caso el principio de proporcionalidad. Donde, además, se especifique el interés público esencial que justifica la restricción del derecho a la protección de datos y en qué circunstancias puede limitarse, estableciendo las reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, sin que sea suficiente, la invocación genérica de un interés público. Estableciéndose las garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos.

Así, el informe considera insuficiente la previsión que hace el artículo 46.3 de la LOU que en relación con la evaluación de los alumnos indica únicamente que “las Universidades establecerán los procedimientos de verificación de los conocimientos de los estudiantes”. Por lo que hasta que no haya amparo legal con las características que recoge la doctrina del Tribunal Constitucional, no podrá ampararse el tratamiento objeto de consulta en el supuesto de excepción previsto en el artículo 9.2 g) RGPD.

Finalmente, se concluye que, en cualquier caso, ya se base el tratamiento en el consentimiento, o con la debida previsión legal, en el interés público esencial, se deberán adoptar aquellas garantías que resulten del correspondiente análisis de riesgos y de la evaluación de impacto y que

deberá valorar el responsable del tratamiento, en el presente caso, la universidad que pretenda implantarlo. Por su parte, el Informe 31/2019 aborda los sistemas de reconocimiento facial en los servicios de videovigilancia al amparo del artículo 42 de la Ley de Seguridad Privada (LSP)

El informe analiza en primer lugar el sometimiento de determinados tratamientos de datos personales que lleven a cabo las empresas de seguridad al RGPD, concluyendo que en la medida en que no están incluidos en el ámbito de aplicación de la Directiva 2016/680, quedan por tanto sujetos a lo dispuesto en el RGPD. En el mismo sentido el artículo 22.6 de la LOPDGDD sitúa bajo esta normativa el tratamiento de datos que no rija por la citada ley de transposición de la citada Directiva.

A continuación, igual que en el anterior informe citado, se analiza la doctrina del Tribunal Constitucional, para concluir que los tratamientos de videovigilancia regulados en la LOPDGDD y en la LSP, se refieren exclusivamente a los tratamientos dirigidos a captar y grabar imágenes y sonidos, pero no incluyen los tratamientos de reconocimiento facial, que es un tratamiento radicalmente distinto al incorporar un dato biométrico, como recuerda el propio RGPD en su Considerando 51.

Asimismo, indica que no puede admitirse que la legitimación reconocida para los sistemas de videovigilancia, dirigida solo a la captación y grabación de la imagen y el sonido, abarque otras tecnologías mucho más intrusivas para la privacidad como pueda ser el reconocimiento facial u otras medidas biométricas como el reconocimiento de la forma de andar o el reconocimiento de voz.

El informe concluye que la regulación actual se considera insuficiente para permitir la utilización de técnicas de reconocimiento facial en sistemas de videovigilancia empleados por la seguridad privada, al no cumplir los requisitos señalados, siendo necesario que se aprobara una norma con rango de ley que justificara específicamente en qué medida y en qué supuestos, la utilización de dichos sistemas respondería a un interés público esencial, definiendo dicha norma legal, previa ponderación por el legislador de

los intereses en pugna atendiendo al principio de proporcionalidad, todos y cada uno de los presupuestos materiales de la medida limitadora mediante reglas precisas, que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, y estableciendo las garantías técnicas, organizativas y procedimentales adecuadas, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos.

A continuación, se citan informes en los que se pone de manifiesto la relevancia del contenido del principio de responsabilidad activa que atañe a los responsables del tratamiento, en el sentido de que les corresponde un ejercicio de análisis y evaluación previa y continua de los tratamientos de datos que van a llevar a cabo, y que, en muchas ocasiones, su resultado debe plasmarse incluso en el texto de la norma de la que se deriven dichos tratamientos.

En el Informe 44/2020 se aborda la adecuación a la normativa de protección de datos de carácter personal de una propuesta de reforma de las Leyes de Seguridad Vial, de Autonomía del Paciente (LAP en adelante) y General de la Seguridad Social a fin de habilitar un mecanismo legal que posibilite la transmisión de datos médicos a las Jefaturas Provinciales de Tráfico en caso de pérdida de aptitudes psicofísicas para la conducción.

Esas limitaciones son detectadas por médicos de atención primaria o especialistas en el ejercicio de sus funciones cuando advierten que un determinado paciente, en posesión de un permiso o licencia para conducir, padece una enfermedad o deficiencia de las previstas en el Anexo IV del Reglamento General de Conductores (RGCon) como causa de denegación o de restricción. Los problemas se detectan particularmente en la tercera edad, generando en ocasiones graves riesgos para la seguridad del interesado y de los demás usuarios del tráfico rodado.

La consulta pone de relieve la dificultad en “canalizar” tal información desde las entidades gestoras de la Seguridad Social o desde los centros médicos hasta las Jefaturas de Tráfico para que a su vez pueda incoarse el procedimiento previsto en el referido art. 70, sin vulnerar la LOPDGDD, ni la LAP.



En el informe se citan otros (Informe 150/2011, Informe 438/2012) en los que se concluye que en tanto que son datos especialmente protegidos se necesitaría habilitación legal, o consentimiento expreso de los afectados.

En la actualidad, la propuesta de modificación legal que recoge el tratamiento que se pretende llevar a cabo, permitiría amparar el tratamiento de datos personales sobre la base jurídica de la obligación legal, conforme a lo previsto en el artículo 6.1.c) del RGPD y el artículo 8 de la LOPDGDD, siempre que dicha disposición legal se ajuste a los criterios del RGPD y a la doctrina del Tribunal Constitucional sobre el principio de proporcionalidad.

El informe señala que, atendiendo a lo dispuesto en el RGPD, hay que tener en cuenta dos limitaciones fundamentales: en primer lugar, que implica el tratamiento de datos de salud, y, en segundo lugar, que supone el tratamiento de datos personales para una finalidad distinta de la que se habían obtenido, debiendo determinarse si dicha finalidad resulta compatible con la inicial.

Teniendo en cuenta que la comunicación de los datos de salud que plantea la consulta lo son al objeto de iniciar un procedimiento administrativo de declaración de la pérdida de vigencia de una autorización de la misma naturaleza, no siendo su finalidad ni el diagnóstico médico ni la valoración de la capacidad del trabajador, que son los supuestos que habilitan su tratamiento inicial por los centros médicos y el INSS conforme a la letra h) del artículo 9.2 del RGPD, dicho tratamiento debería fundamentarse en lo señalado en su letra g, referido a **razones de un interés público esencial**.

Para lo que debe cumplirse todo lo señalado al respecto en los informes analizados en los párrafos anteriores de la presente Memoria para apreciar la concurrencia del interés público esencial, proporcionalidad y compatibilidad de la finalidad.

A continuación el informe analiza por separado los dos supuestos que se plantean, de un lado, la posible comunicación por parte del personal médico de atención primaria o especialistas, que, en el ejercicio de sus funciones, advierten

que un determinado paciente, en posesión de un permiso o licencia para conducir, padece una enfermedad o deficiencia de las previstas en el Anexo IV del Reglamento General de Conductores como causa de denegación o restricción, y de otro, la comunicación a realizar en los supuestos de tramitación de los procedimientos de reconocimiento o revisión de la situación de incapacidad permanente total o absoluta para el trabajo que realice el INSS.

En relación al primero, se indica que debería valorarse por las autoridades competentes en qué medida el objetivo propuesto no puede alcanzarse reduciendo los plazos de validez de la autorización para conducir a partir de una determinada edad, aumentando, de esta manera, la frecuencia de las revisiones médicas a realizar por los correspondientes centros de reconocimiento de conductores y si la medida a adoptar es adecuada o ponderada por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto, singularmente en relación con el derecho a la protección de la salud.

En relación con el segundo, y del mismo modo que se ha señalado anteriormente respecto de la asistencia sanitaria, corresponderá a las autoridades competentes, incluido en el presente caso el Ministerio de Trabajo, valorar la compatibilidad de dicho tratamiento con la comunicación de los datos médicos a las Jefaturas Provinciales de Tráfico, así como realizar el correspondiente juicio de proporcionalidad, pudiendo reiterarse lo señalado anteriormente.

Tratándose de conductores profesionales, cuestión que se cita expresamente en la consulta, y siendo la finalidad del procedimiento de declaración de incapacidad el de apreciar, precisamente, su capacidad para conducir, existiría una relación más estrecha con la revisión de su autorización por la Jefatura Provincial de Tráfico, lo que podría justificar dicha comunicación. Ahora bien, esta relación podría apreciarse solo en los casos estrictamente relacionados con actividades profesionales que requieran la conducción de vehículos a motor, y no con carácter general en todos los supuestos de declaración de incapacidad perma-

nente, que es lo que se recoge en la redacción del artículo 70.2.bis propuesto.

Finalmente, el informe indica que se podría considerar procedente la tramitación de la correspondiente modificación legal por considerar que no se trata de finalidades incompatibles, que existe un interés público esencial y que la medida propuesta supera, a priori, los principios de idoneidad, necesidad y proporcionalidad en sentido estricto.

Añadiendo que en la medida en que dicha medida supondrá un tratamiento a gran escala de categorías especiales de datos, debería realizarse la evaluación de impacto en la protección de datos personales a la que se refiere el artículo 35, y deberá respetarse, en todo caso, el principio de minimización y especificarse en el texto legal al menos en sus principales características, la forma en la que se va a proceder a remitir la información a la Jefaturas Provinciales de Tráfico, en particular los mecanismos de interconexión y la necesidad, o no, de que intervengan los Colegios Profesionales, atendiendo al resultado del análisis de riesgos y de la Evaluación de impacto, y justificándose debidamente la solución adoptada. Y que, en todo caso, en el momento de la obtención de los mismos, los facultativos y el personal del INSS cumplirán con el deber de información regulado en el artículo 13 del RGPD, advirtiendo a los afectados de que sus datos podrán ser tratados con esta finalidad.

Los informes que a continuación se citan tienen el carácter de preceptivo por cuanto analizan proyectos disposiciones de carácter general desde su adecuación a la normativa de protección de datos. El Informe nº 74/2020 se refiere al Anteproyecto de Ley de Memoria Democrática, el Informe nº 77/2020 se refiere a al Anteproyecto de Ley Orgánica de lucha contra el dopaje en el deporte, y el Informe 97/2020 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. Tienen como denominador común que en todos ellos sobrevuela el análisis del riesgo y la evaluación de impacto como manifestaciones del principio de responsabilidad proactiva, que deben de

tenerse en cuenta por parte de las autoridades competentes para la tramitación de la norma, tanto en los departamentos ministeriales donde nace el proyecto o anteproyecto, como en última instancia en las consideraciones a tener en cuenta por el legislador o en su caso, por el órgano que finalmente las apruebe.

En los informes, tras el análisis pormenorizados de sus preceptos, se sugiere, desde una perspectiva práctica, que las circunstancias relativas a la protección de datos personales de los tratamientos que se derivan de la norma se recojan por ejemplo en un Anexo o una Disposición Adicional a la ley, de modo que sea este Anexo o disposición el que de manera conjunta recoja, entre otras cuestiones, las bases jurídicas que el legislador entiende que justifican el tratamiento de datos personales; en su caso, cuál es el supuesto que permite levantar la prohibición de tratamiento de datos personales de categorías especiales, y las medidas adecuadas y específicas que se establece para proteger los intereses y derechos fundamentales de los interesados; y por último, en caso de establecerse limitaciones al ejercicio del derecho fundamental de protección de datos personales, recoger, como mínimo, las circunstancias previstas en el art. 23.2 RGPD, o clarificar si en realidad no estamos ante una limitación del derecho fundamental sino ante la predeterminación legislativa de los motivos legítimos imperiosos que permitirían al responsable del tratamiento vencer el derecho de oposición ejercido por el interesado.

Finalmente indicar que, se recuerda el criterio de la AEPD (Informe 44/2020) de la conveniencia de que se realice, previo Análisis de riesgos (AR) una Evaluación de Impacto de Protección de Datos (EIPD) y que se incluya en la Memoria de Análisis de Impacto Normativo (MAIN).

Otro aspecto que ha sido objeto de consulta es el referido a la interpretación del concepto de responsable y encargado del tratamiento y su aplicación práctica.

En el Informe nº 74/2020 se aborda la posición jurídica que pueda corresponder a las empresas que subcontrata la Sociedad Estatal Correos y Telégrafos SA (en lo sucesivo, Correos) para el

transporte del correo desde un centro logístico de Correos a otro centro logístico de Correos, al objeto de determinar si la empresa subcontratada ostenta la condición de encargado del tratamiento o se trataría de un servicio sin acceso a datos de carácter personal por parte del transportista.

Con carácter previo se determina las diferentes posiciones jurídicas que puede ostentar Correos atendiendo a los diferentes servicios que presta, en relación con otros informes emitidos con anterioridad (Informes 49/2004, 331/2017 y 11/2020) y el propio Dictamen 1/2010, del Grupo de Trabajo del Artículo 29, sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», para así establecer un criterio común y clarificador de la postura de la AEPD en este sector.

El informe parte de la premisa de que, en cualquier caso, una de las novedades del RGPD es identificar al encargado del tratamiento como destinatario de las obligaciones que se deriven, no solo de su relación el responsable, sino del cumplimiento del propio RGPD, tal como se ejemplifica en las Directrices 07/2020 del Comité Europeo de Protección de Datos (CEPD) sobre los conceptos de responsable del tratamiento y encargado en el RGPD.

En segundo lugar, pone de manifiesto la posibilidad de que Correos pueda ostentar diferente condición respecto a los distintos tratamientos que lleve a cabo, por lo que será preciso analizar cada uno de ellos atendiendo a las obligaciones legales que le incumben y a las circunstancias del caso concreto, al objeto de determinar si se actúa como responsable o como encargado de tratamiento.

Cuando sea una persona física el cliente de Correos, actuara amparada bajo la denominación “excepción doméstica”, en cuyo caso Correos tendrá la consideración de responsable del tratamiento, tal y como se indica en el Considerando 18 y deberá cumplir además del RGPD, las obligaciones legales que le impone Ley 43/2010, de 30 de diciembre, del servicio postal universal, de los derechos de los usuarios y del mercado postal, entre las que se incluyen las contenidas en sus artículos 5 (secreto de las comunicaciones

postales), 6 (inviolabilidad de los envíos postales), 7 (protección de datos), 10 (derecho de reclamación), 11 (derecho de denuncia), 12 (derecho a percibir indemnización) 13 (derecho a la propiedad de los envíos postales), 17 (derecho de reexpedición y rehúse de los envíos postales) y 18 (derecho a la protección de los envíos no entregados).

Es decir, en los casos en los que la ley impone obligaciones específicas que implican el tratamiento de datos de carácter personal para la adecuada prestación del servicio y la exigencia, en su caso, de posibles responsabilidades, Correos ostentará la condición de responsable del tratamiento.

Además, Correos debe cumplir con las obligaciones específicas que le corresponden en cuanto operador designado por el Estado para prestar el servicio postal universal. En este ámbito, la capacidad negocial entre Correos y sus clientes respecto a la forma en la que se debe prestar el envío está muy limitada, siendo el legislador nacional el que ha establecido las mismas, lo que en relación con la normativa de protección de datos implica que los tratamientos se realizan al amparo de lo previsto en las letras 6.1.c) y e) del RGPD, siendo la propia norma la que, al amparo de lo previsto en los apartados 2 y 3 del citado artículo 6, introduce especificaciones respecto al tratamiento de datos personales, delimitando los fines y medios del tratamiento y asignándoselo a Correos que, de este modo, tendrá siempre la consideración de responsable respecto de los tratamientos de datos personales necesarios para prestar el servicio postal universal, de acuerdo con lo previsto en el artículo 4.7) del RGPD *in fine*: “si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembro”.

Por otro lado, señala el informe que cuando Correos sea contratado por una entidad sujeta a la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, ostentará la condición de encargado al amparo de lo previsto en su disposición adicional vigesimoquinta, siempre que no se trate de prestaciones incluidas en el servicio postal universal en cuyo caso será responsable del tratamiento.

Por último, en los casos en los que el cliente sea una persona jurídica o una persona física que no se encuentre amparada por la “excepción doméstica” y no se trate del servicio postal universal, podría darse el caso de que Correos actuara como encargado del tratamiento, siempre que concurren en el caso concreto los requisitos necesarios para ello y se haya suscrito el contrato previsto en el artículo 28.3 del RGPD. se identifican en el informe ejemplos como , una compraventa), en los que los datos personales son recabados por el responsable con una finalidad específica (en el supuesto del ejemplo, dar cumplimiento a sus obligaciones como vendedor, entre las que se encuentra la de proceder a la entrega en la forma pactada entre las partes), decidiendo el responsable el medio a través del cual se va a proceder a dicha entrega, y, por tanto, contratar con Correos la entrega del objeto vendido atendiendo a los datos personales que, a este objeto, le ha facilitado el afectado e impartiendo a Correos las instrucciones precisas para el tratamiento de datos personales previa suscripción del contrato del artículo 28.3. del RGPD, tal y como se indicaba en el Informe 11/2020. Todo ello sin perjuicio de que, al igual que ocurre en todos los supuestos de encargo del tratamiento, Correos tenga la consideración de responsable respecto de los tratamientos que hace de sus propios clientes si contienen datos referidos a personas físicas identificadas o identificables.

Finaliza el análisis de las distintas posibilidades señalando que podrán darse supuestos en los que Correos trate los datos personales para sus propios fines, como la gestión de las reclamaciones del destinatario por una prestación defectuosa del servicio y al objeto de exigir las indemnizaciones pertinentes, incluida la geolocalización del envío, o para la prestación de servicios adicionales, como la app “Correos”, en los que ostentará la condición de responsable.

Sobre la consulta concreta, se indica que la prestación del servicio no requiere el tratamiento de datos personales, reconociendo la propia consultante que el posible acceso a los datos personales únicamente se produce en circunstancias excepcionales, de modo que el adecuado desarrollo de la tarea subcontratada puede realizarse sin

acceder a los datos personales citados y sin que ese acceso de carácter excepcional vaya a implicar un tratamiento total o parcialmente automatizado de los datos o esté destinado a incluirlos en un fichero, por lo que no cabe entender que el acceso a los mismos debiera realizarse actuando por cuenta de Correos, ya que en este caso se trataría de un tratamiento excesivo en cuanto no necesario y contrario al principio de minimización.

Por ello, los transportistas deben ser considerados como terceros, que el artículo 4.10) del RGPD define por exclusión como “persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado”, debiendo Correos como responsable del tratamiento (o, en el caso de que actúe como encargado, haya sido autorizado para dicha subcontratación por el responsable y en los términos en que haya sido autorizado), adoptar todas las medidas de seguridad necesarias para evitar que tengan acceso a los datos y establecer un deber de confidencialidad en caso de que accedan accidentalmente a datos personales, de acuerdo con lo previsto en el artículo 32 del RGPD. A continuación, se citan dos informes que tienen en común el planteamiento de sistemas de tratamiento de datos basados en la localización de dispositivos móviles.

En el Informe 17/2019 se plantean las implicaciones en la normativa de protección de datos de la puesta en marcha de un sistema de escáneres en el interior de instalaciones y establecimientos -ya sea aprovechando la infraestructura Wi-Fi del propietario o implementando una nueva-, que detecte todas las señales que emiten los dispositivos electrónicos cuando tienen el Wi-Fi encendido. Se explica en la consulta que el hecho de conocer qué zonas provocan más interés en los clientes, a través de la localización por Wi-Fi, puede permitir la creación de nuevas estrategias de marketing o promociones a los clientes con el fin de mejorar su participación en el mercado y posicionar las marcas a nivel más competitivo.

Tras el análisis de la normativa, anteriores informes y los Dictámenes del Grupo de Trabajo del Artículo 29 se llega a la primera conclusión de que la dirección MAC (identificador único que posee cada dispositivo inteligente conectado a la red) es un dato de carácter personal, debiendo su tratamiento estar sujeto a esta normativa. Y específicamente en cuanto a los datos de localización, ya sea a través de su introducción como los tratados por las aplicaciones, se afirma que pueden incidir significativamente en la vida privada de los usuarios y otras personas se incluye la localización.

La segunda conclusión es que parece inferirse que es la consultante la que decide la forma en la que se va a realizar el tratamiento, instalando sus receptores directamente o aprovechando la red Wifi del establecimiento, y que es la que define el proceso de seudonimización, las redes de transmisión y el modelo de almacenamiento, procediendo directamente al análisis de los datos según criterios previamente definidos por ella, ostentando así la consideración de responsable y no de mero encargado.

En cuanto a la base jurídica del tratamiento, el informe indica que en el caso de que el responsable no haya obtenido el consentimiento de los afectados, debería valorar si concurre el supuesto de interés legítimo recogido al artículo 6.1 f) RGPD.

En relación con el interés legítimo, el informe establece la necesidad de realizar la ponderación de acuerdo con el Considerando 47 RGPD, que no se acompaña a la consulta, y proporciona algunos criterios de carácter general que deberán tener en cuenta los responsables, sin perjuicio de aquellas medidas que el responsable tendrá que implementar en función de la gestión del riesgo para los derechos y libertades de los afectados : por ejemplo, la adopción de medidas que garanticen la anonimización temprana de los datos; analizarse el ámbito en el que se realiza el wifi tracking, atendiendo especialmente a la existencia de una relación comercial, de modo que se trate de clientes o potenciales clientes, evitándose, en todo caso, su empleo en la vía pública. Así como aquellos ámbitos puedan suponer una injerencia excesiva en la privacidad de la persona, como

podiera ser, por ejemplo, en el caso de los aseos, o salvo que se obtenga el consentimiento, en aquellas zonas en que puedan revelar categorías especiales de datos, como por ejemplo, las que tengan productos relacionados con la salud; tampoco se podrán cruzar los datos de geolocalización así obtenidos con otros datos procedentes de otras fuentes (como, por ejemplo, los pagos con tarjeta de crédito o las imágenes captadas por los sistemas de videovigilancia) que puedan permitir la identificación de la persona; asimismo deberá garantizarse que los interesados tienen pleno conocimiento de que se está procediendo al tratamiento de sus datos personales, así como de su derecho a oponerse. Finalmente, el informe concluye resaltando el cumplimiento del deber de transparencia y el derecho a la información de los afectados, que en cualquier caso deberá cumplirse, y la necesidad de tener en cuenta el análisis de riesgos y en su caso, la realización de una evaluación de impacto.

En el Informe 43/2019 se plantea la aplicación de la normativa de protección de datos al sistema que pretenden desarrollar la entidad consultante, consistente en el tratamiento de la señal emitida por los terminales móviles, que identifican su IMSI -Identificador Internacional de Abonado Móvil- como identificador único del teléfono móvil que se guarda en la SIM, al objeto de conocer los recorridos o tránsitos que realizan dichos dispositivos dentro de un recinto determinado.

Al igual que el anterior informe, la primera conclusión a la que se llega es que es de aplicación la normativa de protección de datos personales, en la medida en que el sistema propuesta trata información que ha de considerarse dato de carácter personal, ya que debe considerarse como tal el IMSI. En segundo término, también se señala que para que el tratamiento encuentre acomodo en el RGPD, deberá encontrar una base jurídica en el artículo 6 del RGPD, señalándose especialmente la referida al consentimiento y la referida al interés legítimo. Indicándose al igual que en el anterior informe algunos criterios a tener en cuenta para que el responsable del tratamiento lleve a cabo el ejercicio de ponderación o sopesamiento que requiere la aplicación del interés legítimo como base jurídica del tratamiento.



Otro tema que en cada ejercicio se analiza es el relativo al tratamiento de datos de salud a través del uso de la Historia Clínica y cuya reiteración pone de manifiesto la relevancia de esta materia.

En el Informe 101/2019 se analiza el alcance de la interpretación de la Disposición Adicional Decimoséptima de la LOPDGDD en relación a las leyes que se citan en la misma, si debe considerarse un listado cerrado o puede interpretarse que tienen cabida otras normas no indicadas, a los efectos de levantar la prohibición de tratamiento de categorías especiales de datos prevista en el artículo 9.1 del RGPD, y en segundo término, la posibilidad de que por parte de los servicios de Inspección Médica de la Comunidad Autónoma de Canarias, pueda accederse a las historias clínicas tanto de atención primaria como de atención especializada a los efectos realizar sus funciones de verificación control, confirmación y extinción de la incapacidad temporal.

En relación con la primera cuestión, el informe indica que si bien el RGPD establece unos supuestos que excepcionan la prohibición de tratamiento de categorías especiales de datos, a través del derecho de los Estados miembros se pueden introducir regulaciones ad hoc a fin de adaptar la realidad de los sectores implicados para garantizar una protección efectiva de los derechos de los ciudadanos de la unión.

Para resolver el alcance de la citada disposición se acude a lo dispuesto en el artículo 3.1 del Código Civil y a lo indicado en la propia Exposición de Motivos de la LOPDGDD al respecto “También en relación con el tratamiento de categorías especiales de datos, el artículo 9.2 consagra el principio de reserva de ley para su habilitación en los supuestos previstos en el RGPD. Dicha previsión no sólo alcanza a las disposiciones que pudieran adoptarse en el futuro, sino que permite dejar a salvo las distintas habilitaciones legales actualmente existentes, tal y como se indica específicamente, respecto de la legislación sanitaria y aseguradora, en la disposición adicional decimoséptima. El RGPD no afecta a dichas habilitaciones, que siguen plenamente vigentes, permitiendo incluso llevar a cabo una interpretación extensiva de las mismas, como sucede, en particular, en

cuanto al alcance del consentimiento del afectado o el uso de sus datos sin consentimiento en el ámbito de la investigación biomédica.”, para llegar a una primera conclusión referida a que la citada disposición adicional identifica determinados apartados del artículo 9.2 del RGPD, aquellos tratamientos de datos que se deriven de la aplicación de las leyes que se citan, lo que no implica que los tratamientos de datos personales que se lleven a cabo como consecuencia de la aplicación de otras normas no encuentren acomodo en las excepciones del citado precepto, pues la referencia a la reserva de ley que contiene el artículo 9.2 LOPDGDD permitirá que pueda haber normas que no estén incluidas, incluso aquellas que aún no se hayan aprobado, que puedan dar cobertura a la excepción de prohibición de tratamiento de categorías especiales de datos.

Es decir, el marco regulador actual permite que puedan encontrar amparo determinados tratamientos de datos en otras normas y en otros supuestos a pesar de no deducirse de la disposición adicional analizada. Y recuerda la doctrina ya señalada en los informes antes citados de la Sentencia núm. 76/2019 de 22 mayo del Tribunal Constitucional, sobre las características de las leyes que pretendan regular el tratamiento de categorías especiales de datos.

El informe concluye el primer aspecto indicando que si bien la disposición adicional decimoséptima de la LOPDGDD incluye una lista taxativa, dicha circunstancia no impide que el tratamiento de datos de salud pueda ampararse en otras normas que no se citen en la misma siempre y cuando que se de alguna de las circunstancias previstas en el artículo 9.2 del RGPD y la regulación establecida al efecto tenga rango de ley y cumpla las garantías que el Tribunal Constitucional considera esenciales cuando estamos ante el tratamiento de categorías especiales de datos.

En relación con el segundo aspecto objeto de consulta, tras el análisis de la normativa estatal y autonómica, concluye que el acceso a las historias clínicas, tanto de atención primaria, como especializada por parte de los servicios de inspección médica a los efectos de evaluar la capacidad laboral en relación con los procesos

de incapacidad temporal, encuentra su amparo en dicha normativa. Y cuyo tratamiento debe completarse con la observancia de los principios recogidos en el artículo 5 del RGPD, cuya consecuencia es que acceso que se realice servirá única y exclusivamente a la finalidad de evaluación, control y seguimiento de los procesos de incapacidad temporal con las limitaciones cualitativas y cuantitativas propias de la finalidad a la que sirve el acceso.

En definitiva, concluye que no estaría amparado un acceso (indiscriminado) a toda la historia clínica referido a acontecimientos que por su cualidad y temporalidad no estuvieran relacionados con el proceso de incapacidad temporal que se pretenda evaluar. Como tampoco podrá darse una finalidad distinta y en todo caso ha de respetarse la confidencialidad de la información a la que se accede.

En el Informe 79/2020 se aborda el uso de la historia clínica, cuando el profesional que es responsable de la misma ha cesado en su actividad. Y en concreto cuando ha fallecido y cómo deben proceder sus herederos.

Se tienen en cuenta los artículos 659 y 661 del Código Civil, para analizar la sucesión de la obligación de custodia del profesional fallecido en favor de sus herederos, y que se convierten en responsables de la conservación y seguridad de las historias clínicas, como mínimo, cinco años contados desde la fecha de alta de cada proceso asistencial. Y al menos durante ese plazo son responsables del tratamiento de los datos que se contengan en las historias clínicas, y en relación con el objeto de la consulta, serán a quienes corresponda atender, y en su caso, satisfacer, el ejercicio de los derechos previstos en la normativa, como el derecho de acceso, cuya materialización dependerá de distintos factores.

Asimismo, se recuerda la obligación que les incumbe a los herederos, de acuerdo con el artículo 14 del RGPD referida a la Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado.

En el informe se analizan distintas situaciones que pueden darse, dependiendo de la condición de profesional de la medicina o no, que puedan ostentar los herederos. Ya que solo en caso afirmativo, podrían acceder a la historia clínica, para satisfacer los derechos previstos en la normativa, y en particular el de acceso.

En caso contrario, la primera opción pasaría por acudir a un profesional de la medicina, y donde se abren dos posibilidades desde la perspectiva de la protección de datos, o bien la comunicación o cesión de los datos previo consentimiento de los afectados, o bien mediante la figura del encargado del tratamiento.

Señala el informe que otra posibilidad, sería acudir a los colegios profesionales de médicos que ofrecen determinados servicios cuando un facultativo ha cesado en su actividad profesional. El tratamiento de datos que conllevarían estos servicios sucedería al amparo de una relación jurídica, donde los herederos seguirían siendo responsables del tratamiento y el colegio profesional, al igual que en el supuesto anterior, se instituiría en encargado del tratamiento debiendo cumplir las obligaciones derivadas de tal condición y en especial lo dispuesto en los artículos 28 del RGPD y 33 de la LOPDGDD.

Finalmente se indica en el informe que, si los herederos son también profesionales de la medicina, podrían acceder a las historias clínicas a los efectos de satisfacer los derechos que se ejerzan. En este supuesto es fundamental recordar que el principio de limitación de finalidad, que en el artículo 5.1 b) RGPD indica que los datos personales serán recogidos con fines determinados, explícitos y legítimos y no serán tratados ulteriormente de manera incompatible con dichos fines.

También en relación con datos de salud, pero en procesos selectivos a la función pública, se emitió el Informe 86/2020 que analiza la posibilidad de que en procesos selectivos donde se prevén pruebas de aptitud psicofísica o pruebas médicas, puedan conocer el resultado completo de las mismas, no solo el servicio médico que las realiza, sino también el Tribunal Calificador. Es decir, si el conocimiento de este puede ir más allá de la

consideración de apto o no apto en relación con el cuadro de exclusiones medicas que se prevé en la convocatoria.

En tanto que se trata de categorías especiales de datos, el informe analiza las posibles excepciones a la prohibición general de tratamiento que prevé el artículo 9.1 RGPD, comenzando por el consentimiento, y llega a la conclusión de que la prestación de este no puede considerarse “libre” en el sentido de que pueda no otorgarse o revocarse, sin sufrir ningún perjuicio. Es decir, sin ser excluido del proceso selectivo. Por lo que el consentimiento, desde la perspectiva del derecho a la protección de datos, resultara inadecuado para legitimar el tratamiento de datos de salud, tanto el que realicen los servicios médicos establecidos al efecto para hacer la prueba, como el referido al posible acceso por el Tribunal Calificador.

Posteriormente analiza la aplicación de los supuestos previstos en los apartados b) y h) del artículo 9.2 del RGPD, en tanto que el supuesto de consulta trata del eventual nacimiento de una relación laboral y aunque la función pública no se rige, en puridad, por normas laborales sino por el derecho administrativo estatutario de los funcionarios públicos, la interpretación que de ella se deriva, comparte, en términos generales, la misma naturaleza jurídica.

Ambos apartados requieren para su aplicación, que el ordenamiento jurídico de la unión Europa o el derecho nacional, establezcan las suficientes garantías para el respeto a la protección de datos de los afectados.

El informe analiza el ordenamiento jurídico aplicable identificando garantías y salvaguardas que permitirían la aplicación de las excepciones previstas en los apartados b) y h) del citado artículo 9.2 del RGPD, pero también, poniendo de manifiesto la dispersión normativa actual y la necesidad de abordar reformas legislativas en la materia para dotar de mayor uniformidad, coherencia y en última instancia, seguridad jurídica, al régimen de garantías en el tratamiento de datos de salud, derivado de los procesos selectivos a la función pública. Finalmente, tras levantar la prohibición de tratamiento de datos especiales,

encuentra la base jurídica para el tratamiento en los apartados, b) c) y e) del artículo 6 del RGPD.

En segundo término, el informe basándose en la jurisprudencia referida a la motivación de las resoluciones que resuelven procesos selectivos y en particular, de aquellas que versan sobre el ejercicio de la función policial, como la de la consulta, propone una ponderación de los derechos fundamentales en juego, de un lado el artículo 24 y el artículo 23.2 de la Constitución, sobre la tutela judicial efectiva y el derecho a utilizar los medios de defensa, que parten del contenido de la motivación, y el acceso a cargos públicos en condiciones de igualdad, y de otro el artículo 18.4 de la Constitución, referido al derecho a la protección de datos.

El resultado de la ponderación y la aplicación del principio de proporcionalidad, hacen que se permita el acceso a datos de salud, por parte de los Tribunales de Calificación a los efectos de motivar la calificación de no apto de un participante, “la jurisprudencia referida a los procesos de selección de empleados públicos en los que existen pruebas de aptitud psicofísica, vienen exigiendo que el Tribunal Calificador no sólo conozca la causa de exclusión en los casos que debe ser calificado un aspirante como no apto, sino que esté en condiciones de explicar en qué medida y de qué modo dicha circunstancia impide el desarrollo profesional del puesto de trabajo de que se trate”.

Finalmente recalca la importancia de cumplir los principios de limitación de finalidad y minimización que deben darse en dicho acceso, al indicar que el acceso debe interpretarse de modo restrictivo tanto en los supuestos que lo permiten como en la información a la que podrá accederse. Por lo que el tratamiento de datos de salud que lleve a cabo el Tribunal Calificador debe estar limitado a esa finalidad, es decir, cuando el aspirante deba ser excluido del proceso selectivo, cuando la calificación deba ser de no apto, dicho órgano podrá acceder a los datos de salud a fin de cumplir ese cometido y para poder explicar (motivar) la razón de la misma.

Pero dicho conocimiento debe estar limitado a lo estrictamente necesario, es decir, a poder explicar en qué medida el aspirante se encuentra impedido para la función profesional (limitación de finalidad y minimización). Los principios citados impiden que el tratamiento tenga otra finalidad y que el conocimiento de datos de salud exceda de los referidos únicamente a la causa de exclusión, por lo que el Tribunal Calificador no podrá conocer el contenido completo del informe o acta que emita el servicio médico.

Además, los principios y garantías en el tratamiento se completarán con la observancia del principio de confidencialidad e integridad previstos en los artículos 5.1 f) del RGPD y 5 de la LOPDGDD.

Y resuelve el caso concreto indicando que no estaría justificado el acceso al contenido completo del informe médico por parte del Tribunal Calificador, sino sólo en casos de motivar la exclusión del aspirante y en la medida en que sea necesario para dicha motivación.

#### 4.1.2. Informes preceptivos

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

Entre las disposiciones informadas en el año 2020 cabe mencionar las siguientes:

- Proyecto de Orden de la Consejería de Economía, Empleo y Competitividad, por la que se aprueban las bases reguladoras para la concesión de ayudas a municipios de la Comunidad de Madrid para el desarrollo de actividades de promoción comercial y ferial.
- Proyecto de Real Decreto de comunicaciones comerciales de las actividades del juego.
- Proyecto de Real Decreto de modificación del Reglamento de planes y fondos de pensiones.

- Proyecto de Orden por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo urgente y operación de una aplicación para la crisis sanitaria ocasionada por la COVID-19.
- Proyecto del Real Decreto Ley por el que se adoptan medidas complementarias, en el ámbito laboral, para paliar los efectos derivados de la COVID-19.
- Anteproyecto de Ley Orgánica de protección de datos personales tratados con fines de prevención, detección, investigación o enjuiciamiento de infracciones penales y de ejecución de sanciones penales, así como de protección y prevención frente a las amenazas contra la seguridad pública.
- Enmiendas proyecto de ley de distribución de seguros por ADECOSE.
- Proyecto de Orden EDT de regulación del crédito revolvente por la que se modifica la Orden ECO 697/2004, de 11 de marzo, sobre la central de información de riesgos.
- Proyecto de Orden de medidas de vigilancia epidemiológica de la infección por SARS COV2 durante la fase de transición hacia la nueva normalidad.
- Anteproyecto de Ley de residuos y suelos contaminados.
- Proyecto de Real Decreto por el que se regulan las condiciones en que realizan sus funciones los servicios de auxilio en las vías públicas.
- Proyecto de Orden por la que se regula el registro electrónico de apoderamientos de la Seguridad Social.
- Anteproyecto de Ley Orgánica de garantía integral de la libertad sexual.
- Anteproyecto de Ley de Precursores explosivos.

- Proyecto de Orden de la Consejería de Economía, empleo y competitividad de la Comunidad de Madrid por la que se establecen las bases reguladoras para la concesión de ayudas para la digitalización de Asociaciones 2020.
- Anteproyecto de Ley de trabajo a distancia.
- Anteproyecto de Ley de Memoria democrática.
- Proyecto de Real Decreto por el que se regula el régimen de certificación fitosanitaria oficial para la exportación de vegetales y productos vegetales.
- Anteproyecto de Ley Orgánica de Lucha contra el Dopaje en el Deporte.
- Proyecto de Orden por la que se aprueba la política de seguridad de la información en el ámbito de la administración digital del ministerio de Hacienda.
- Anteproyecto de Ley por el que se modifica la ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
- Proyecto de Circular del Banco de España por la que se modifican la Circular 1/2013 de 14 de mayo, sobre la central de información de riesgos y la Circular 5/2012 de 27 de junio a entidades de crédito y proveedores de servicios de pago.
- Proyecto de Real Decreto por el que se regulan las funciones de los servicios de auxilio en vías públicas.
- Proyecto de Real Decreto por el que se modifican diversos RRDD de Agricultura.
- Proyecto de Orden sobre los métodos de identificación no presencial para la expedición de certificados electrónicos cualificados.

- Proyecto de Orden por la que se modifica la Orden INT/1922/2003, de 3 de julio sobre libros de registro y partes de entrada de viajeros en establecimientos de hostelería y otros análogos.

#### ▲ 4.1.3. Sentencias

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

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

Durante el año 2020 se han dictado por la Sala de lo contencioso-administrativo de la Audiencia Nacional 77 resoluciones<sup>1</sup>, de las cuales:

- 49 fueron desestimatorias de los recursos formulados contra resoluciones de la Agencia (que quedaron plenamente confirmadas) (63%).
- 10 estimaron parcialmente los recursos (13%).
- 11 estimaron íntegramente las pretensiones anulatorias de las resoluciones de la Agencia (14%).
- 7 inadmitieron los recursos interpuestos contra resoluciones de la Agencia (10%).

---

<sup>1</sup> Únicamente se refiere a Sentencias, quedando por tanto excluidos los autos 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.



En cuanto a los sectores de actividad de los recurrentes, de 77 sentencias que resuelven recursos frente a las resoluciones de la AEPD, la mayor parte han sido interpuesto por particulares (47). 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 aprecia no solo la AEPD sino también el propio tribunal. En cuanto a las estimatorias, y parcialmente estimatorias, debe indicarse que responden a una variada casuística donde materias como el ejercicio de los derechos cobran especial relevancia y en especial aquellas que versan sobre la cancelación de antecedentes policiales. Seguido del sector de sistemas de información crediticia (7) (ficheros de solvencia patrimonial y crédito), y los servicios de la sociedad de la información, entre los que se engloban los prestados a través de internet (6). Tras ellos figura el sector de las telecomunicaciones (4) y el sector de banca y seguros (3). Los restantes sectores como energía, asociaciones sindicales, o distribución y venta de productos, son los menos significativos cuantitativamente y se mantienen en términos similares al ejercicio anterior.

Destaca el sector de la publicidad y prospección comercial en el que no se ha resuelto ningún procedimiento frente a la Audiencia Nacional, frente a los 18 del ejercicio anterior. Ahora bien, en este ejercicio buena parte de aquellos asuntos se han visto frente al Tribunal Supremo que ha confirmado el criterio de la AEPD.

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

En relación con las categorías especiales de datos que define el artículo 9.1 del RGPD, (datos especialmente protegidos en la terminología utilizada por la Directiva 95/46 y la LOPD actualmente derogadas), procede citar, en primer lugar, la Sentencia de 12 de marzo de 2020 recaída que resuelve el Recurso nº 157/2018, y que analiza un supuesto de tratamiento de datos de ideología y religión sin consentimiento.

Los hechos se refieren a la realización de un estudio sociológico a partir de una encuesta por parte de una empresa contratada por el Ayuntamiento de Valencia, que se refería a preguntas, confeccionadas por dicha corporación local, sobre la fiesta de las Fallas tras su declaración como patrimonio inmaterial de la humanidad por la Unesco. Entre las preguntas se incluían algunas que versaban sobre la identidad territorial (¿se siente más español que valenciano? Y viceversa), sobre la definición religiosa del encuestado (¿cómo se define en materia religiosa? Católico, no católico, no creyente, ateo, etc...), sobre el comportamiento lingüístico referido al uso del idioma valenciano o castellano o incluso sobre el partido político en el que se sentía el encuestado más identificado, mostrando una lista de partidos o dónde se situaba en una escala desde la extrema derecha hasta la extrema izquierda.

Al final de la encuesta se solicitaba el nombre, dirección y teléfono móvil, siendo únicamente obligatorio éste último. La Sentencia dice que no puede entenderse que los datos se recabaran con el consentimiento de los afectados. Rechaza por completo la existencia del consentimiento tácito, que alega la corporación local que se desprende de la participación en la encuesta. La infracción cometida es la referida a tratar datos especiales sin consentimiento expreso y por escrito tal y como exigía el artículo 7.2 de la hoy derogada LOPD aplicable a los hechos analizados.

Siguiendo con las categorías especiales de datos, destaca la Sentencia de 24 de noviembre de 2020 recaída en el Recurso nº 791/2018, referida a datos de salud. Los hechos se refieren a la publicación de una resolución por parte de la Agencia Española de Protección de la Salud en el Deporte, sin una adecuada anonimización que tenía por objeto sancionar a un deportista por el uso de sustancias prohibidas, y que suponían un caso de dopaje. El debate se centra en considerar los datos relativos al dopaje como datos de salud y por tanto incluirlos en las categorías especiales de datos.

La recurrente manifestaba que dentro de la definición legal de dopaje (artículo 4 de la L.O. 3/2013, de protección de la salud del deportista y lucha contra el dopaje en la actividad deportiva), no puede incluirse información que revele un estado de salud, patología, historia clínica o afectación de dolencia alguna, y que por tanto se esté ante datos de salud.

El Tribunal considera datos de salud la información referida al dopaje, a la luz de la interpretación extensiva que se deriva del Considerando 35 del RGPD, ya que éstos abarcan también **“la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas...”**;

Siguiendo con datos de salud, en este ejercicio vuelven a analizarse tratamientos de datos referidos a la historia clínica cuya regulación se encuentra principalmente en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente (LAP) y que tiene múltiples implicaciones desde la perspectiva de la protección de datos personales.

Comenzando por la Sentencia de 22 de septiembre de 2020 recaída en el Recurso nº 186/2019, se denuncia falta de medidas de seguridad al permitir el acceso a la historia clínica por facultativos de una mutua de accidentes de trabajo en relación con una incapacidad laboral de carácter temporal.

El Hospital privado presta servicios médicos a pacientes con aseguramiento privado del servicio Gallego de Salud (SERGAS), y también en régimen de concierto con diferentes mutuas. Los profesionales del Hospital registraban toda la actividad de los usuarios que acudían al mismo, tanto por la Seguridad social como por seguro privado. Lo que conllevaba que tanto los profesionales del hospital, los de la mutua y los del SERGAS podían ver todos los actos asistenciales que recibía un paciente.

La infracción denunciada se basa en que la información que contiene la historia clínica no distingue en función de que dicha información

derive de la asistencia médica privada o de la asistencia médica a través de la Seguridad Social, del SERGAS. Lo que conlleva que los servicios de inspección en las propuestas de alta, puedan ver datos derivados del servicio privado prestado.

La sentencia razona que el principio de vinculación permite el acceso a los facultativos de la mutua que a través del servicio de inspección médica accedieron a la historia clínica del paciente, por entender que sí tenían relación asistencial. Todo responde a que la historia clínica única en cada centro hospitalario tiene el objetivo de la máxima integración de la documentación clínica de cada paciente y por tanto se adecua tanto a la LAP como a la LOPD.

En segundo lugar, conviene destacar la Sentencia de 26 de junio de 2020 que resuelve el Recurso nº 713/2018, referida al uso de la información contenida en la historia clínica.

El profesional prestaba servicios médicos en una clínica en la que era el único médico integrante del cuadro médico y, por tanto, único responsable del tratamiento farmacológico que podían recibir los pacientes. Al dejar de prestar servicio en la clínica, se puso en contacto con los pacientes a los efectos de informarles de la posibilidad de continuar el tratamiento con él y de una posible prescripción farmacológica inadecuada por parte de la clínica.

Se denuncia por parte del dueño de la clínica, que el facultativo no disponía del consentimiento para realizar ese tratamiento de datos consistente en el uso de los datos de los pacientes a tal fin.

La sentencia razona que no han sido los pacientes los que han entendido vulnerado su derecho a la protección de datos y la carencia del consentimiento, sino que ha sido el dueño de la clínica, que además tiene una mala relación con el facultativo que se pone de manifiesto en la existencia de una querrela del facultativo contra el denunciante por varios delitos de apropiación indebida, falsedad documental, suplantación (usurpación de funciones e intrusismo) y delito contra la salud pública. A lo que añade que el principio del consentimiento es personal e individual.

Por lo tanto, considera que no hay constancia de que el tratamiento de los datos de los pacientes se haya realizado sin su consentimiento, además de que corresponde al facultativo responsable del tratamiento, velar por el correcto abordaje de la patología tratada, por lo que necesita de los medios de comunicación suficientes con los pacientes para no poner en grave riesgo su salud.

En relación con los sistemas de información crediticia (ficheros que ofrecen información sobre solvencia patrimonial o coloquialmente conocidos como ficheros de morosos), destacan las Sentencias de 6 de noviembre de 2020, y 13 de marzo de 2020, (recaídas en los recursos 730/2018, 735/2018 y 1123/2018 respectivamente) en las que el tribunal estima que no se cumplen los requisitos para la inclusión en los ficheros de solvencia patrimonial, siendo el denominador común a todas ellas, la inexistencia de la deuda, al provenir la misma de un producto o servicio contratado irregularmente. Se pone el acento en la diligencia a la hora de contratar para evitar la suplantación de identidad y por tanto atribuir la deuda a una persona que nada tiene que ver con los hechos.

Asimismo, deben citarse las Sentencias de 2 de marzo de 2020 y de 30 de junio de 2020, recaídas en los Recursos nº 760/2018 y 759/2018 respectivamente, que, si bien versan sobre los sistemas de información crediticia, se analiza además la competencia territorial de la AEPD.

Se alega que la entidad compradora de la deuda, y por tanto nueva acreedora que decide la inclusión en los sistemas de información crediticia, no está establecida en España, sino en Luxemburgo por lo que la AEPD no tiene competencias para su conocimiento. La Audiencia Nacional recuerda las Sentencias del Tribunal Supremo, reiterando la doctrina de la de 5 de febrero de 2019, -casación 627/2018- que fundamenta la competencia de la AEPD, esencialmente en el criterio del establecimiento, pues aunque la entidad estaba domiciliada en otro Estado Miembro, dirigía de forma regular actividades y operaciones a través de medios instrumentales radicados en España, adoptando decisiones relativas a los fines y medios del tratamiento de datos, al haberse acreditado

que era la responsable de impartir las órdenes para que se incluyeran los datos personales del afectado en el fichero de solvencia patrimonial.

Señala la importancia de que la cesión de datos personales, que motivó la denuncia del afectado, se asocia a un contrato de compraventa de una cartera de créditos celebrado en España, que era gestionada por otra empresa, domiciliada en España, que se encargaba de las reclamaciones e incidencias en relación con las obligaciones de pago que resultaban incumplidas, y que la cesión de datos se efectuaba para la inclusión en un fichero de solvencia patrimonial del que era responsable la empresa EXPERIAN BUREAU DE CRÉDITO, S.A., que operaba en España.

En relación con las bases jurídicas que dan licitud al tratamiento de datos, es preciso destacar la Sentencia de 10 de octubre de 2020 recaída en el Recurso nº 1058/2018, donde se analizan los supuestos legitimadores como el consentimiento o el interés legítimo y que confirma la sanción que impone la AEPD a los Testigos Cristianos de Jehová, por la creación y uso irregular de una base de datos de médicos afines a sus creencias.

Los hechos son que miembros de la citada organización realizan visitas a hospitales para realizar entrevistas y conocer el grado de colaboración del personal facultativo sanitario respecto a la práctica de cirugías sin transfusiones, y crear una base de datos a fin de informar a otros miembros cuando necesitaban ese tipo de intervención.

Se alegaba por la sancionada que los datos son incidentales y que la finalidad era contactar con el hospital en caso de necesitarlo, sin embargo la sala comparte el criterio de la AEPD que sostiene que se evidencia que su clasificación obedece a la identificación de cada profesional con sus características y que se incluyen aquellos que tienen interés para la organización y que la finalidad es contactar con ellos directamente para conocer su postura en relación con las creencias de la organización.

Se alega también la excepción a la prestación del consentimiento, en base al artículo 6.2 LOPD en relación con la constancia de datos en fuentes

accesibles al público, artículo 3.f LOPD. Argumento que se rechaza puesto que la información ni era la misma, ni se mostraba igual que en la publicación de facultativos que podía encontrarse en fuentes accesibles al público.

Se estima que no existe consentimiento de los facultativos para que sus datos sean tratados con esa finalidad por la organización sancionada. Por el contrario, se alega por la sancionada que existe un “interés legítimo” y que no se precisa del consentimiento, ya que confluyen dos derechos fundamentales, el derecho a la vida e integridad física de los miembros de la confesión y el derecho a la libertad religiosa, e invoca el juicio de ponderación entre dichos derechos fundamentales y el derecho a la protección de los datos personales de los facultativos.

La Sala rechaza estos argumentos indicando que la interpretación que del derecho a la vida ofrece la recurrente es desde un punto de vista meramente subjetivo y también, porque las circunstancias en las que los datos se recogen, desde 2014, a través de entrevistas y sin haber informado a su titular sobre la finalidad, sin ofrecer garantías ni transparencia que les hubieran permitido acceder a su cancelación o ejercer algún derecho reconocido en la LOPD, hacen que prevalezca el derecho a la protección de datos de éstos, frente a los derechos que aduce la sancionada.

Por su parte, la Sentencia de 18 de febrero de 2020 recaída en el Recurso 57/2019, analiza un caso de tratamiento sin consentimiento, pero estrechamente relacionado con el ámbito de aplicación material de la normativa de protección de datos, y en concreto con la denominada “excepción doméstica”, principal alegación del sancionado y que de estimarse impediría considerar que se exige el consentimiento.

Los hechos son que un médico pediatra envió varios mensajes a su pareja a través de la aplicación WhatsApp, entre los que se contenían fotos de los pacientes en la camilla de la consulta, fotos de la agenda con nombres, apellidos y teléfonos de los pacientes, y videos en los que se ve a menores con su madre.

Se alega que los mensajes tienen un neto carácter personal o doméstico y en tal concepto se envían, por lo según el artículo 2.2 a) de la LOPD queda fuera de su ámbito de aplicación. Los mensajes se enviaron en el curso de un intercambio de fotos de su vida cotidiana y en ese contexto a título de ilustración de su especialidad de pediatra, de su trabajo como una faceta más de su personalidad. Además, añade que los envíos se producen antes del inicio de la jornada laboral y que las imágenes no permiten identificar a nadie.

La Sala rechaza estos argumentos, citando la Sentencia del TJUE de 6 de noviembre 2003, caso Lindqvist, que recuerda que la excepción debe interpretarse en el sentido de que contempla únicamente las actividades que se inscriben en el marco de la vida privada o familiar de los particulares, y sostiene que el tratamiento excede de su ámbito privado, estando conectado con su actividad profesional, resulta indiferente a la hora que se enviaron, pues lo cierto es que las fotos de su agenda profesional contenían datos de los pacientes que iba a atender en esas fechas.

El sancionado aportó en su defensa dos escritos con manifestaciones de los padres de los menores que aparecen en las fotos y videos otorgando su consentimiento, sin embargo, la Sala rechaza la eficacia de esas pruebas, pues es la madre de los menores quien aparece en las imágenes, sin que conste presencia de ningún varón adulto. Y cierra el asunto indicando que, en cualquier caso, no consta el consentimiento de las personas que figuraban anotadas en la agenda.

Otra materia recurrente en los casos que llegan a la Audiencia Nacional es lo referido al tratamiento de datos realizado a través de dispositivos de captación de imágenes, videocámaras y sistemas de video vigilancia, donde elementos como la proporcionalidad, la finalidad o la mera existencia de tratamiento cobran especial relevancia.

Comenzando por la Sentencia de 27 de noviembre de 2020 recaída en el Recurso nº 271/2018, que analiza el tratamiento de datos a través de cámaras ocultas y que confirma el archivo resuelto por la AEPD.

Los hechos que se denuncia son que la empresa adjudicataria del servicio de bar-cafetería en varios hospitales de la provincia, colocaron cámaras ocultas en las instalaciones dedicadas a la prestación de dicho servicio sin informar a la Gerencia pública de salud y titular de las instalaciones, sin informar a los trabajadores, ni tampoco al resto de usuarios de la cafetería. La AEPD declara el archivo de las actuaciones al considerar legítimo el uso de cámaras ocultas con el fin de obtener pruebas para corregir irregularidades o iniciar procedimientos disciplinarios, con independencia de que finalmente se iniciaran los mismos. La denunciante recurrente pone de manifiesto que fueron insuficientes las actuaciones de investigación llevadas a cabo por la AEPD.

La Sala comparte el criterio de la AEPD por cuanto justifica la adecuación, idoneidad y proporcionalidad de la medida, por el tiempo determinado y para recabar pruebas de desviaciones económicas apreciadas por la empresa de catering.

Por su parte las Sentencias de 13 de marzo de 2020 y de 11 de noviembre de 2020 que resuelven los recursos nº 10/2018 y 1470/2020 confirman el archivo de la resolución de la AEPD, por entender que no hay pruebas suficientes del tratamiento denunciado y su falta de adecuación al principio de proporcionalidad. Asimismo, tratan otros aspectos como el cumplimiento de los requisitos de la Ley de Propiedad Horizontal respecto de los acuerdos de la comunidad de propietarios para autorizar una instalación de videocámaras, resolviendo que son cuestiones ajenas a la competencia de la AEPD.

Otra materia para destacar es la aportación de datos personales a procesos judiciales, se dictaron las Sentencias de 2 y 10 de marzo, y de 2 de octubre y 9 de diciembre, todas de 2020, (Recursos nº 190/2018, 907/2018, 225/2019 y 161/2019 respectivamente), se estima que hay una colisión de los derechos fundamentales a la protección de datos, de un lado, y de otro, con el derecho a la tutela judicial efectiva. Las sentencias citadas confirman las resoluciones de archivo y de inadmisión que combaten los recurrentes, y se reitera la doctrina referida a la aplicación del hoy derogado artículo 11.2 d) de la LOPD referida a la comunicación de

datos, sin consentimiento cuando los destinatarios sean los Tribunales de Justicia. En dicha excepción, pueden incluirse 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. Y recuerda lo indicado en la Sentencia de 14 de diciembre de 2017, que determina que los derechos fundamentales no son absolutos y que precisamente la previsión legal del art. 11.2 d) LOPD es uno de los límites al derecho a la protección de datos en favor del derecho a la tutela judicial efectiva, acogiendo los argumentos del Abogado del Estado en el sentido de que dicho tratamiento está amparado en la posibilidad de utilizar los medios de prueba que sean pertinentes para la defensa del interesado siempre que estos no hayan sido obtenidos de forma ilícita y así lo declarase el Tribunal.

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 aquellos que tratan sobre el denominado derecho de supresión en internet o derecho al olvido.

En efecto, las Sentencias 13 de marzo, 8 de junio, 16 de julio y 30 de octubre, todas de 2020, recaídas en los Recursos nº 421/2017, 683/2018, 1203/2018, 1627/2019 y 278/2018 respectivamente, se estiman total o parcialmente los recursos presentados por los recurrentes, en los que se combate las resoluciones de la AEPD que consideran adecuada la respuesta dada por la Dirección General de la Policía (DGP) al denegar la cancelación de antecedentes policiales. 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 policiales. La Sala considera insuficiente la motivación ofrecida por la administración requerida.



Indican las sentencias que en las resoluciones objeto de recurso, únicamente se reproduce el contenido de los artículos 22.4 y 23.1 de la LOPD, y que, en las resoluciones de la DGP, no se hace referencia a los motivos específicos por los que se considera que no procede la cancelación solicitada, creando una situación de indefensión. Sin que se establezca de forma clara y concreta cuál es ese peligro real y cierto que pudiera derivarse para la seguridad pública de tal cancelación.

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 4 de enero de 2020 que resuelve el Recurso nº 389/2018 interpuesto por la entidad responsable del motor de búsqueda, tiene por objeto una resolución de la AEPD en un procedimiento de Tutela de Derechos que estima la reclamación de un afectado, consistente en la eliminación de los resultados de búsqueda de cuatro enlaces referidos a la publicación de candidaturas a elecciones generales del año 2003 y 2004.

La empresa alega que la publicación de candidaturas es una obligación legal y sirve como garantía de una opinión pública informada. Los ciudadanos tienen derecho a conocer el pasado político e ideológico de sus representantes y candidatos, así como la historia de los partidos políticos y qué personas han sido candidatos electorales. Asimismo, es un tratamiento referido a la actividad política de una persona, lo que excede el ámbito personal o privado. La información no es obsoleta, ya que si el afectado vuelve a ser candidato en ese u otro partido, cobra interés la militancia anterior.

La Sala confirma la resolución de la AEPD indicando que en la actualidad el afectado no ejerce cargo público ni permanece activo como militante de ningún otro partido, y ha manifestado que se encuentra alejado de las siglas del partido por el que concurrió a las elecciones en 2004. La reclamación ante la AEPD es de 2017.

Es un tratamiento inicialmente lícito y que en principio justificaría la prevalencia del interés público general, pero que por las circunstancias expuestas y el transcurso del tiempo (2003) se han convertido en obsoletos y no concurre el interés preponderante del público en tener acceso a esa información.

La Sentencia de 18 de junio de 2020 que resuelve el Recurso nº 631/2017 interpuesto por la entidad responsable del motor de búsqueda tiene por objeto una resolución de la AEPD en un procedimiento de Tutela de Derechos que estima la reclamación de un afectado, consistente en la publicación de unas noticias del año 2012 referidas a una denuncia por violencia doméstica contra otra persona a la que acompañaba y contra él mismo por desobediencia y prevaricación. El afectado en aquellas fechas era un cargo relevante de la policía nacional en su comunidad autónoma.

La Sala confirma el criterio de la AEPD indicando que la información es excesiva y afecta a la vida privada del reclamante es obsoleta y carece de relevancia pública y, además, desde el punto de vista de los fines para los que fueron tratadas, por el tiempo que ha transcurrido y no concurre el interés preponderante del público en acceder a su contenido. Los hechos, de gran repercusión en la época dado el cargo del codemandado, fueron contundentemente tratados en el procedimiento penal ya que el fiscal pidió la absolución, acogida por la sentencia, en la que se le desvincula por completo de los hechos; estos, además, sucedieron cinco años antes del inicio del procedimiento ante la AEPD.

Concluye la sentencia “Las noticias a que se refieren los enlaces, desde el momento en que se dictó la sentencia por el Juzgado de Instrucción, se revelan como excesivas e inexactas por cuanto hacen referencia a unos confusos hechos conteni-

dos en la denuncia que se califican como prevaricación o desobediencia e incluso se asocian a un caso de supuesta violencia conyugal, cuando la sentencia absolutoria únicamente menciona la inexistencia de una falta contra el orden público del artículo 634 del Código Penal. Además, los hechos son relativamente lejanos en el tiempo y el interesado ya no ejerce su profesión en la localidad en que sucedieron.”

La Sentencia de 2 de marzo de 2020 que resuelve el Recurso nº 189/2018 interpuesto por el afectado y desestimándolo, tiene por objeto una resolución de la AEPD en un procedimiento de tutela de derechos que desestima la reclamación de un afectado consistente en la eliminación de una noticia referida a su persona como presidente de las juventudes de un partido político y que había celebrado la muerte de dos militantes de ideología política contraria y protagonizó un incidente durante la marcha homenaje a uno de aquellos, y la existencia de unas actuaciones judiciales por injurias contra el alcalde de una corporación local.

La Sala rechaza la eliminación de los enlaces y confirma el criterio de la AEPD razonando “nos encontramos ante noticias que pueden tener una notable relevancia pública, pues, pese a que el recurrente haya manifestado que su persona carece de dicha relevancia pública, lo cierto es que desempeña un cargo en un partido político y no manifiesta haber cesado en su cargo. Por otro lado, el actor se ha limitado a alegar que las informaciones no son veraces y contienen auténticas falsedades sobre su actividad, pero sin acreditar nada al respecto. Por el contrario, las resoluciones judiciales que se han aportado al expediente acreditan, al menos, la existencia de unas actuaciones judiciales respecto a las supuestas injurias contra el alcalde de Burjasot, que ciertamente fueron sobreseídas en el año 2016, en relación al hoy recurrente y otras personas. También la existencia de otro procedimiento penal relativo a denuncia falsa y obstrucción de la justicia en la que igualmente se vio involucrado.(...) las noticias no pueden reputarse como obsoletas, pues datan del año 2013, y las resoluciones judiciales de 2014 y 2016, mientras que la reclamación presentada por el recurrente fue en 2017”.

La Sentencia de 25 de septiembre de 2020 que resuelve el Recurso nº 252/2018, interpuesto por el afectado es de especial interés en la medida en que aborda un aspecto del contenido del derecho al olvido que hasta ahora no se había planteado.

La reclamación resuelta por la AEPD determina que deben eliminarse ciertos enlaces de internet, por afectar a la vida privada del afectado que no tiene relevancia pública y que además son obsoletos, del año 2008.

Pero lo interesante de este supuesto tiene por objeto que el reclamante comprobó que eran accesibles los enlaces utilizando la versión de EEUU del buscador realizando la búsqueda desde España, “engañando” al buscador para que geolocalice la misma en aquel estado (modificando la IP como si la búsqueda se realizase en EEUU). El debate se centra en si el derecho al olvido abarca también esos supuestos. Es decir, si los efectos del derecho son extensibles a otras versiones del buscador en países fuera de la Unión Europea.

La Sala utiliza en su argumentación la Sentencia del TJUE de 24 de septiembre de 2019, C-507/17, Google LLC contra la Commission Nationale de l'Infomartique et des Libertés que impuso a Google Inc. una sanción de 100 000 euros, porque cuando dicha empresa estimó una solicitud de retirada de enlaces, se negó a proceder a tal retirada en todas las extensiones de nombre de dominio de su motor de búsqueda.

La Sala finalmente se inclina por la retirada de los enlaces aunque se utilice la versión del buscador estadounidense, al indicar que “Debemos añadir, que Google reconoce que su sistema de geobloqueo es eficaz en el 99,4% de los casos, y que existen tecnologías -como los servicios VPN o servicios proxy ofrecidos por terceros- que permiten a los usuarios ocultar su verdadera dirección IP a través de un servidor localizado en otro Estado, burlar el sistema de aprendizaje automático de geolocalización de Google, admitiendo que el citado sistema de geobloqueo no puede imposibilitar por completo el acceso a quien emplee para ello medios técnicos para eludir el mismo.

Por lo que, en virtud de lo expuesto, procede estimar la pretensión del actor, de bloquear en el motor de búsqueda de Google, los enlaces controvertidos, cuando las búsquedas se realicen en España, en el uso de una funcionalidad aplicable en Google, que permite al buscador geolocalizar la búsqueda en EEUU, a pesar de encontrarse el usuario que realiza la búsqueda en España.”

La Sentencia de 6 de noviembre de 2020 que resuelve el Recurso nº 731/2018 interpuesto por la entidad responsable del motor de búsqueda tiene por objeto una resolución de la AEPD en un procedimiento de Tutela de Derechos que estima la reclamación de un afectado consistente en la eliminación de unos enlaces que versan sobre una noticia referida al asesoramiento que realizó el afectado a unos clientes sobre la constitución de un entramado de sociedades en paraísos fiscales.

La AEPD considera que no es una persona de “relevancia pública”, sino que se trata de un profesional que presta determinados servicios a terceras personas, sin que la condición de relevancia pública de alguno de sus clientes traslade esa condición al profesional que pone sus servicios a disposición de aquéllos y añade que la información facilitada confunde la actividad profesional del reclamante con los intereses y objetivos perseguidos por sus clientes, de modo que podría deducirse que también son suyos, por lo que no se puede afirmar que dicha información sea atribuible exclusiva o principalmente a dicha actividad profesional, por lo que prima el derecho a la protección de los datos personales – derecho al olvido- frente al derecho a la libertad de expresión y estima la reclamación. La Sala rechaza estos argumentos indicando que debe tenerse en cuenta que lo publicado en el enlace controvertido es relativamente reciente, de 2013, y la actividad empresarial es de esos años, inmediatamente anterior a la solicitud de tutela presentada ante la Agencia el 16 de julio de 2017.

Asimismo, se trata de una persona que realiza una actividad profesional, a la que exclusivamente se refiere la noticia publicada, por lo que existe un interés legítimo de los internautas en tener acceso a dicha información, que ha sido publicada en la prensa. Al respecto, frente a las

alegaciones del codemandado, conviene precisar que en la publicación predominan los juicios de valor sobre los hechos relatados, por lo que son más bien resultado del ejercicio de la libertad de expresión que de la libertad de información, con las consecuencias que derivan sobre la veracidad del contenido.

Y concluye que el enlace cuyo bloqueo acuerda la resolución impugnada está amparado por el derecho fundamental a la libertad de expresión del artículo 20 de la Constitución, que comprende, la crítica de la conducta de otro, aun cuando la misma sea desabrida y pueda molestar, inquietar o disgustar a quien se dirige, pues así lo requiere el pluralismo, la tolerancia y el espíritu de apertura de la sociedad democrática. A la libertad de expresión no es aplicable el límite interno de veracidad que si es aplicable a la libertad de información.

La Sentencia de 10 de marzo de 2010 que resuelve el Recurso nº 218/2018 interpuesto por entidad responsable del motor de búsqueda tiene por objeto una resolución de la AEPD en un procedimiento de Tutela de Derechos que estima la pretensión del afectado cuyo objeto es la retirada de unos enlaces referentes a unas noticias sobre las declaraciones que el afectado -alcalde de una corporación local- realizó a la salida del juzgado sobre un procedimiento por acoso laboral y acoso sexual a una exconcejala de la misma corporación. La AEPD estimó la reclamación en base a que tras el Auto de sobreseimiento de la causa la información ha devenido inveraz y, además, afecta a la vida privada del reclamante, y por ello debe ceder el derecho a la libertad de información.

La Sala rechaza estos argumentos en base a que el factor tiempo tiene gran relevancia respecto a la ponderación de intereses a realizar, debe tenerse en cuenta que lo publicado es relativamente reciente, pues cronológicamente la última noticia publicada en el País, se refiere al Auto de la Audiencia Provincial de Pontevedra, de 8 de junio de 2016, desestimando el recurso de apelación presentado contra el Auto del Juzgado de Villagarcía de Arosa, de 15 de marzo de 2016, que decretaba el sobreseimiento provisional de la causa.

Asimismo, se trata de una persona que desempeñaba el cargo de alcalde en una localidad de Pontevedra, que se vio implicado por una denuncia presentada contra él por una exconcejala del propio Ayuntamiento y en relación a un delito de abusos sexuales y acoso laboral por hechos sucedidos en los años 2007 y 2008, por lo que existe un interés legítimo de los internautas en tener acceso a dicha información, que ha sido publicada en la prensa local y nacional. Es tratamiento de datos inicialmente lícito por parte del buscador que, dado el contenido de la información, las vicisitudes de una persona dedicada a una actividad pública y respecto de hechos con una trascendencia social relevante, junto al poco tiempo transcurrido, continúan siendo necesarios en relación con los fines para los que se recogieron o trataron.

Finalmente concluye al igual que en anterior supuesto que “El enlace cuyo bloqueo acuerda la resolución impugnada está amparado por el derecho fundamental a la libertad de expresión del artículo 20 de la Constitución, que comprende, la crítica de la conducta de otro, aun cuando la misma sea desabrida y pueda molestar, inquietar o disgustar a quien se dirige, pues así lo requiere el pluralismo, la tolerancia y el espíritu de apertura de la sociedad democrática. A la libertad de expresión no es aplicable el límite interno de veracidad que si es aplicable a la libertad de información”

Por su parte, el **Tribunal Supremo dictó un total de 18 resoluciones**, de las cuales 17 de ellas confirman el criterio de la AEPD y una es contraria. De las primeras conviene destacar que 10 de ellas son interpuestas por el mismo recurrente, una empresa de acciones de mercadotecnia, frente a las sentencias de la Audiencia Nacional que confirmaron el criterio de la AEPD (cuya reseña consta en la Memoria de la AEPD del año 2019) y que versan sobre tratamiento de datos en acciones de mercadotecnia.

En esta instancia, en los 10 recursos planteados por la empresa de mercadotecnia, debe resaltarse que se analiza entre otras cuestiones, la incidencia que la aprobación del RGPD pudiera tener en los hechos enjuiciados, y que la recurrente entiende

que ha sobrevenido la atipicidad de los mismos, por ser favorable la aplicación retroactiva de la norma europea actualmente en vigor. Todo ello en base a lo indicado en el Considerando 47 del RGPD referido al interés legítimo en acciones de mercadotecnia.

La Sala centra el debate en si puede considerarse lícito el tratamiento de datos personales con fines de mercadotecnia directa cuando, a pesar de no haber otorgado el interesado su consentimiento, concurre un interés legítimo en el responsable del tratamiento.

La recurrente sostiene que el responsable del tratamiento «no necesita efectuar una ponderación de los intereses que concurren para valorar cuál de ellos debe prevalecer conforme a la regla del art. 6.1.f), sino que siempre que los datos se utilicen para alguna de las finalidades indicadas, el tratamiento puede basarse en el interés legítimo. Y, entre esas finalidades, se incluye el "envío de comunicaciones comerciales"». Se rechazan esos argumentos en base que el uso de los datos personales para cumplir ese fin legítimo exige, según el RGPD, que el interesado haya tenido la oportunidad de oponerse a dicho tratamiento, y que este derecho se le haya comunicado explícitamente, tal como se dispone en el considerando 70 y en el art. 21 de dicha norma.

Respecto de la aplicación retroactiva del RGPD, recuerda la jurisprudencia que determina que para saber si una norma es más favorable, el análisis que debe hacerse es de la norma en bloque, in toto, al caso concreto, pues solo así se le puede considerar de manera efectiva una norma más favorable para el supuesto en sí.

Por lo tanto, en el supuesto enjuiciado ni se le pidió al interesado el consentimiento expreso y previo, como requería la LOPD de 1999 que se aplicó a los hechos, ni se le comunicó debidamente la utilización de sus datos en una campaña de mercadotecnia al objeto de que pudiera manifestar su oposición tal como prevé el RGPD en el artículo 21.4 y recoge la LOPDGDD de 2018 en su artículo 18.

Asimismo, deben citarse otras 4 sentencias que resuelven los recursos interpuestos por el mismo recurrente, una empresa de servicios de telecomunicaciones y servicios de ocio a través de aplicaciones móviles.

La Sala centra el interés casacional en delimitar qué debe considerarse como un tratamiento de datos de ámbito exclusivamente personal o doméstico a efectos de su exclusión del ámbito de protección que dispensa la LOPD; en qué circunstancias (o con qué alcance) la voz de una persona puede considerarse como un dato de carácter personal; y finalmente en qué términos debe llevarse a cabo la ponderación del interés legítimos del responsable del tratamiento y la protección de los datos de carácter personal del interesado.

La entidad ofrecía un servicio de ocio a través de aplicaciones móviles que consistía en que un usuario que descargaba la aplicación podía gastar una broma a un tercero a través del envío de una locución que producía una conversación con dicho tercero y cuyo resultado se almacenaba en los servidores de la entidad y se podía descargar en el dispositivo del usuario de la aplicación y posteriormente reproducir, descargar y compartir el fichero de audio que contiene la grabación. El usuario introducía el nº de teléfono del tercero para el envío de la “broma” y este proporcionaba su voz en la conversación en la que se resolvía la broma. Al final de la misma se ofrecía información sobre protección de datos indicando que el nº de teléfono lo había proporcionado “un amigo o conocido suyo” y que salvo que se muestre la oposición, los datos personales formaran parte del fichero del que la empresa es responsable. El tercero destinatario de las bromas manifestaba que no había prestado su consentimiento para tal fin, ni respecto del número de teléfono, ni respecto de su voz.

Sobre la aplicación de la excepción doméstica, la recurrente indicaba que era un mero “facilitador” de una actividad que realiza el usuario en el ámbito estrictamente personal o doméstico, pone los medios, no usa la información para ningún otro propósito que prestar el servicio contratado por el cliente y si la grabación se difunde, es por decisión del usuario. La Sala rechaza el argumento

pues para aplicar la excepción se requieren dos requisitos, que el tratamiento de datos lo haga un particular y que lo haga en el marco de una actividad exclusivamente particular o doméstica. Algo que no se da en ninguno de los supuestos enjuiciados.

Sobre la voz como dato personal, la sancionada sostiene que no permiten la identificación de la persona, no al menos sin plazos o esfuerzos desproporcionados. La Sala rechaza el argumento pues precisamente para garantizar el derecho de oposición al que informa en la locución sería imposible llevarlo a cabo únicamente con la voz, es decir, los datos que almacena son además de la voz, el nº de teléfono y en su caso, la dirección de correo desde la que se realiza el citado derecho. Además, el tratamiento de datos personales identificables no se proyecta únicamente frente al titular de la base de datos, sino también frente a terceros. En primer término, al usuario de la aplicación, que, en relación con el consentimiento para el tratamiento de los datos del destinatario de la broma, únicamente se le hace una pregunta en una locución. Además, en cuanto al consentimiento prestado por el afectado al final de la grabación, éste es un consentimiento pasivo otorgado de forma negativa, que no cumple las características que exige la normativa de protección de datos.

Finalmente, sobre la ponderación de intereses la Sala rechaza por completo los argumentos de la recurrente al indicar que en ningún caso podría prevalecer la realización de una actividad de ocio frente a la protección de datos personales en relación con un tratamiento informático de los mismos. Y añade que el interés de la recurrente no es única ni principalmente el proporcionar un medio de ocio, sino el beneficio comercial que obtiene con ello. Dicho interés comercial es sin duda alguna legítimo, pero desde luego no puede prevalecer sobre la protección de los datos de las personas afectadas, la cual requiere su pleno y libre consentimiento informado para que tales datos sean sometidos a tratamiento informático.

Otra Sentencia que merece atención es la relativa a una sanción impuesta a una entidad aseguradora por el tratamiento de datos en acciones de mercadotecnia que contrato con un tercero la realización de una campaña publicitaria.



El debate se centra en si la entidad beneficiaria de la publicidad debía proporcionar a la tercera entidad el fichero de exclusión de acciones publicitarias generado a partir de los derechos de oposición que frente a ella se hubieran llevado a cabo. La recurrente afirma que la existencia de un fichero de exclusión al amparo del artículo 48 del RDLOPD no implica la obligación de su comunicación a las terceras entidades con las que contrate una campaña publicitaria, pues supondría una cesión sin consentimiento.

La Sala rechaza este argumento por cuestiones fácticas y jurídicas. Las primeras en la medida en que en una comunicación del afectado, éste indica que se comunique sus derecho de oposición a cualquier entidad que “trabaje para ellos” y la segunda en la medida en que la entidad aseguradora era responsable del tratamiento ya que era la beneficiaria de la publicidad y en último término determina los fines y medios del tratamiento y por tanto obligada, a procurar la efectividad de la oposición al tratamiento de datos manifestado por su cliente, aún en el supuesto de externalización de su actividad publicitaria.

En relación con el ejercicio del derecho al olvido, el Tribunal Supremo dictó la Sentencia nº 1624/2020 de 27 noviembre, que resolvía un recurso de casación en el que se analizaba “la extensión del derecho al olvido” bajo la vigencia de la Directiva 95/46 y la LOPD, en el sentido de que si se podía entender incluido en el mismo, cuando la búsqueda en Internet se hacía únicamente con los dos apellidos y no con el nombre. La Sala tras analizar la doctrina del Tribunal de Justicia de la Unión Europea, del Tribunal Constitucional y del propio Tribunal Supremo, indica que no resulta coherente, con esa doctrina jurisprudencial, reconocer el derecho al olvido cuando la búsqueda se efectúe a partir del nombre (completo) de una persona y negarlo cuando se efectúa sólo a partir de los dos apellidos de esa persona, pues ello implica no tener en cuenta uno de los principios generales del Derecho de la Unión Europea, que propugna la interpretación uniforme en todos los Estados miembros de la normativa comunitaria europea”.

Por lo que concluye que el ejercicio del derecho de oposición, rectificación o cancelación y en su caso del derecho al olvido “faculta a la persona interesada a exigir del gestor de un motor de búsqueda que elimine de la lista de resultados, obtenida como consecuencia de una búsqueda efectuada tanto a partir de su nombre completo o de sus dos apellidos, vínculos a páginas webs, publicados legalmente por terceros, que contengan datos e informaciones veraces, relativos a su persona, cuando la difusión de dicha información, relativa a su persona, menoscabe el derecho al honor, a la intimidad, o a la propia imagen del interesado, y carezca de interés público, y pueda considerarse, por el transcurso del tiempo, obsoleta, en los términos establecidos por la jurisprudencia del Tribunal de Justicia de la Unión Europea, del Tribunal Constitucional y del Tribunal Supremo.”

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 11 de noviembre de 2020 (Asunto C-61/19 Orange Romania) que trata del consentimiento prestado en una cláusula contractual. El Tribunal recuerda que corresponde al responsable del tratamiento de los datos demostrar que el interesado ha manifestado su consentimiento para el tratamiento de sus datos personales mediante un comportamiento activo y que ha recibido, previamente, información respecto de todas las circunstancias relacionadas con ese tratamiento, con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, que le permita determinar sin dificultad las consecuencias de dicho consentimiento, de modo que se garantice que este se otorga con pleno conocimiento de causa.

El contrato no será válido cuando la casilla referente a dicha cláusula haya sido marcada por el responsable del tratamiento de datos antes de la firma del contrato, o cuando las estipulaciones contractuales de dicho contrato puedan inducir al interesado a error sobre la posibilidad de celebrar el contrato en cuestión pese a negarse a consentir en el tratamiento de sus datos, o cuando la libre elección de oponerse a dicha obtención y dicha conservación se vea indebidamente obstaculizada por ese responsable, al exigir que el inte-

resado, para negarse a dar su consentimiento, cumplimente un formulario adicional en el que haga constar esa negativa.

Pero sin duda la resolución de más relevancia en el ámbito europeo ha sido la Sentencia de 16 de julio de 2020 en el Asunto C-311/18 (Sentencia Schrems II), que declara contraria a Derecho la Decisión 2016/1250 de la Comisión europea relativa al Escudo de Privacidad y que considera adecuada, la Decisión 2010/87 de la Comisión europea relativa a las Cláusulas Contractuales Tipo.

El contenido de la sentencia y sus implicaciones prácticas se abordan en otros apartados de este Memoria.

## 4.2. El Comité Europeo de Protección de Datos

**El RGPD es directamente aplicable en todos los Estados Miembros y no puede ser modificado por las legislaciones nacionales.**

La adopción del Reglamento General de Protección de Datos (RGPD) y, aunque en menor medida, de la Directiva sobre Ámbito Penal (DAP) han supuesto un punto de inflexión en la forma en que se abordan las políticas en materia de protección de datos en los Estados Miembros de la Unión Europea.

Si bien es cierto que la anterior legislación europea en la materia, la Directiva 95/46, ya imponía una armonización para las normas nacionales de protección de datos y establecía un mecanismo de intercambio de información, cooperación y orientación en la materia a través del Grupo Europeo de Autoridades de Protección de Datos (el llamado Grupo del Artículo 29 – GT29), el marco legal que entró en aplicación en mayo de 2018 ha supuesto un cambio cualitativo cuyos efectos todavía no se han desplegado plenamente.

El principal, y más obvio, es que el RGPD, que es la norma de más amplio alcance, es directamente aplicable en todos los Estados Miembros y no puede ser modificado por las legislaciones nacionales. Estas legislaciones tampoco pueden incluir normas de desarrollo o aplicación que contradigan al RGPD o vayan más allá de sus previsiones, salvo, en este último caso, en que el propio Reglamento lo autorice.

**Consecuentemente, la presencia del RGPD obliga a que cualquier desarrollo normativo interno que afecte a la protección de datos deba llevarse a cabo dentro de los límites y de acuerdo con las previsiones que el Reglamento establece.**

Un solo ejemplo puede ilustrar este papel del RGPD como referente normativo. Su artículo 23 prevé que el derecho de los Estados Miembros o de la Unión pueda establecer limitaciones a los derechos de los interesados y a las correlativas obligaciones de los responsables que el Reglamento recoge en su capítulo tercero cuando tales limitaciones sean necesarias y proporcionadas en una sociedad democrática para salvaguardar una serie de objetivos que, en la mayoría de los casos, se relacionan con intereses públicos relevantes.

Esa posibilidad que se abre para los Estados Miembros (o la Unión), y que ya estaba contemplada en la Directiva del 95, va, sin embargo, acompañada en el Reglamento de una serie de requisitos que se imponen para las normas en las que se regulen esas limitaciones a los derechos.

Más allá de este caso, evidente por la claridad con la que el RGPD señala los requisitos a cumplir y los supuestos a los que se aplican, lo cierto es que la tarea de identificar las implicaciones en materia de protección de datos y de ofrecer las soluciones que se adapten al Reglamento se extiende a todos los sectores de actividad, en la medida en que las normas a adoptar tengan incidencia en materia de protección de datos.

En esa misma línea, la existencia de una norma única que persigue asegurar un nivel uniforme de protección en toda la Unión Europea implica la necesidad de asegurar que la interpretación y aplicación de sus disposiciones se lleva a cabo también de forma consistente en todos los Estados Miembros.

**El Comité Europeo de Protección de Datos (CEPD) garantiza la aplicación coherente del RGPD y es la mejor expresión del cambio de enfoque derivado de la adopción del RGPD.**

A conseguir ese objetivo contribuyen, de forma destacada y desde sus respectivas competencias, la Comisión Europea y el Tribunal de Justicia de la Unión Europea. Pero el Reglamento establece, además, un organismo, el Comité Europeo de Protección de Datos (CEPD), cuya función expresa es garantizar la aplicación coherente del RGPD.

El Comité, organismo de la Unión con personalidad jurídica propia y capacidad de adoptar decisiones vinculantes para las autoridades de protección de datos que lo integran, es la mejor expresión del cambio de enfoque derivado de la adopción del RGPD.

En el pasado, el predecesor del CEPD, el GT29, se presentaba como un grupo de expertos sin personalidad jurídica cuyas opiniones o recomendaciones llegaron a tener una indudable autoridad moral, llegando a ser citadas por tribunales nacionales y europeos, pero no producían efectos jurídicos. El Comité, por el contrario, es un organismo de la Unión y cualquiera de sus posicionamientos, con variaciones en función del tipo de instrumento que se use, tiene unas consecuencias que se derivan del hecho de que suponen la interpretación del organismo del organismo expresamente encargado de asegurar una aplicación consistente del Reglamento.

El Comité se pronuncia a través de diversos tipos de documentos que pueden agruparse en tres grandes categorías.

Por una parte están las recomendaciones, directrices y buenas prácticas previstas en el artículo 70 del RGPD. Estos documentos son similares en su forma a los dictámenes que emitía el GT29 y comparten con ellos el hecho de no ser jurídicamente vinculantes. Sin embargo, existen importantes diferencias de matiz.

En primer lugar, mientras que la Directiva hacía una referencia genérica a que el GT29 podría pronunciarse sobre cualquier aspecto relacionado con la protección de datos en la Unión y los Estados Miembros, el RGPD al utilizar expresiones como “examinará”, “emitirá”, o “formulará” (recomendaciones, directrices o buenas prácticas) establece una cierta obligación para que el Comité se pronuncie sobre los temas a considerar y le atribuye una suerte de competencia delegada para desarrollar el Reglamento en estas materias, si bien a través de documentos sin una relevancia jurídica formal.

Por otro lado, la lista de cuestiones sobre la que el Comité está llamado a pronunciarse es muy extensa, e incluye tanto referencias genéricas, comparables a las que hacía la Directiva (“el Comité examinará (...) cualquier cuestión relativa a la aplicación del presente Reglamento y emitirá recomendaciones, directrices o buenas prácticas a fin de promover la aplicación coherente del presente Reglamento”), como otras muy específicas relativas a artículos o apartados concretos del RGPD (“emitirá recomendaciones, directrices o buenas prácticas (...) a fin de especificar más los criterios y requisitos de las decisiones basadas en perfiles en virtud del artículo 22, apartado 2”).

Finalmente, entre estos “mandatos” que recibe el Comité, se encuentra no solo la elaboración de documentos de orientación sino, también, la promoción, en diversas formas, de la cooperación entre sus miembros. Existen, además, algunos casos en que, junto con los tres instrumentos de guía ya mencionados, el Comité emite dictámenes, distintos de los previstos en el artículo 64 que luego se abordará, fundamentalmente para proporcionar criterios a la Comisión Europea sobre una pluralidad de materias, incluidas las declaraciones sobre el nivel de adecuación de países terceros.

Una de las principales consecuencias de estos instrumentos es que, pese no ser formalmente vinculantes, producen el efecto de generar expectativas legítimas en los operadores económicos que llevan a cabo tratamientos de datos. La interpretación que el Comité hace de los temas en los que se pronuncia refleja no solo la posición concertada de sus miembros sino, como se ha dicho anteriormente, la postura del Comité en la materia. Por ello, cuando responsables, encargados o ciudadanos los aplican, se basan en una confianza legítima en que están actuando de una forma correcta, acorde con las previsiones del RGPD, dado que el Comité tiene justamente la función de actuar para garantizar la coherencia en la aplicación del Reglamento. Ello supone que las autoridades nacionales deben tener en cuenta sus contenidos a la hora de ejercer sus funciones de supervisión.

Los comentarios anteriores sirven para subrayar la importancia que para las autoridades de protección de datos de los Estados Miembros tiene participar de forma activa en la elaboración de todos estos instrumentos de orientación o consulta, ya que su contenido condiciona de forma decisiva su actividad en toda la gama de materias en que el Comité está llamado a pronunciarse.

Aunque su contenido concreto se aborda en otra sección de esta Memoria<sup>2</sup>, cabe señalar aquí que durante el año 2020 el Comité ha aprobado un total de 12 directrices o recomendaciones en temas tan variados como las implicaciones para la protección de datos de varias de las medidas aplicadas para luchar contra la COVID-19, los conceptos de responsables, corresponsables y encargados, los vehículos conectados o las transferencias internacionales después de la Sentencia Schrems II del Tribunal de Justicia de la Unión Europea.

Un segundo bloque de decisiones que puede adoptar el Comité son las que derivan de la aplicación de una de las dos modalidades del mecanismo de coherencia, la prevista en el artículo 64 del RGPD.

---

<sup>2</sup> Ver Sección “Una autoridad activa en el panorama internacional”.

Este mecanismo de coherencia supone una novedad cualitativa respecto a la situación existente con el GT29, ya que en este caso el Comité tiene una función de autorización respecto de determinadas decisiones que pueden adoptar las autoridades nacionales.

Por una parte, el Comité tiene que pronunciarse sobre un listado de decisiones de las autoridades nacionales que pueden tener impacto en el conjunto de la Unión. Son decisiones de autorización de determinados instrumentos de transferencia internacional, de herramientas de co-regulación como son los códigos de conducta o las certificaciones, y también los listados de tratamientos que requerirán necesariamente de Evaluación de Impacto en la Protección de Datos.

Por otro lado, el Comité deberá emitir dictamen, si no lo ha hecho ya con anterioridad sobre el mismo asunto, siempre que uno de sus miembros, su presidente o la Comisión Europea lo soliciten en relación con materias que produzcan efectos generales o que afecten a la libre circulación en la Unión.

En este caso, el Comité se manifiesta a través de dictámenes que no tienen un carácter formalmente vinculante, pero que sí obligan materialmente a las autoridades a las que se dirigen. Efectivamente, en caso de que una autoridad se separe del criterio del Comité, se activará el mecanismo de coherencia en su segunda modalidad, que permite tomar decisiones jurídicamente vinculantes para asegurar el cumplimiento por parte de la autoridad afectada.

En este caso es aún más evidente que en el anterior la importancia que la dimensión europea cobra para la actividad cotidiana de las autoridades nacionales y, en realidad, para el desarrollo de las políticas en materia de protección de datos. Los criterios para poder aprobar, por ejemplo, Normas Corporativas Vinculantes (BCR por sus siglas en inglés) o para acreditar organismos de supervisión de códigos de conducta, se van configurando a partir del trabajo del Comité en su análisis y valoración de las propuestas que presentan las autoridades nacionales y deben ser seguidas por éstas.

De nuevo nos encontramos en una situación en que, ante la solicitud por parte de un operador de autorización para usar unas cláusulas contractuales ad hoc para una transferencia internacional o para aplicar un acuerdo administrativo suscrito con un ente público de un país tercero para el intercambio de datos personales, la negociación para cada autoridad no se limita al plano de sus relaciones con ese operador, sino que se extiende a, y está influida por, las discusiones que tendrán que mantenerse en el Comité.

Durante 2020 el Comité ha emitido 31 dictámenes sobre varias Normas Corporativas Vinculantes, criterios de acreditación de organismos de supervisión de códigos de conducta y de acreditación de entidades de certificación y cláusulas tipo para contratos de encargo de tratamiento. Entre las BCR dictaminadas favorablemente por el Comité se encuentran dos en las que la Agencia Española ha sido la autoridad líder en el procedimiento, sobre las compañías Iberdrola y Fujikura Europe Group.

Las decisiones jurídicamente vinculantes que el Comité puede adoptar para resolver las controversias entre autoridades nacionales de supervisión conforman el tercer grupo de instrumentos a través de los que ejerce sus funciones y están contempladas en el artículo 65 del RGPD.

Estas decisiones están previstas, fundamentalmente, para aquellos casos en que existen discrepancias entre la autoridad principal en un procedimiento desarrollado en el marco del mecanismo de cooperación que establece el RGPD y una o varias de las autoridades afectadas por ese procedimiento. Aparte de ello, también se pueden adoptar este tipo de decisiones para resolver las diferencias en la identificación de la autoridad principal encargada de coordinar uno de esos procedimientos y siempre que una autoridad no siga los dictámenes que el Comité adopta en la primera de las modalidades del mecanismo de coherencia que se ha descrito anteriormente.

Estas decisiones son quizás el rasgo más distintivo del Comité frente a su antecesor, en la medida en que solo un organismo con personalidad jurídica propia puede tomar decisiones con relevancia jurídica. Las decisiones, como el propio

Reglamento, en aplicación de las previsiones de los Tratados, establece, son recurribles ante el Tribunal de Justicia de la Unión Europea y también, indirectamente, ante los tribunales nacionales.

Su importancia dentro de las funciones del Comité ha hecho que durante 2020 se haya dedicado una parte relevante de su actividad a regular su funcionamiento. Por una parte, el Comité adoptó en el mes de octubre unas *Directrices sobre la noción de Objeción Pertinente y Motivada*. Estas objeciones son el punto de partida para el procedimiento del artículo 65, ya que su inicio se produce cuando la autoridad principal decide no aceptarlas o las considera no relevantes o no motivadas. Por ello, y de cara al funcionamiento del Comité, se ha considerado necesario definir con precisión la interpretación que puede hacerse de la definición que el Reglamento hace de estas objeciones, con especial atención a su posible alcance y contenido.

En esa misma línea, el Comité acordó desarrollar un documento sobre el procedimiento a seguir para el desarrollo del artículo 65, que amplíe y complemente las previsiones que ya se contienen en las Reglas de Procedimiento Interno del Comité. Su aprobación está prevista para el mes de abril de 2021.

Con todo, el principal hito en este ámbito durante 2020 es que el Comité ha adoptado su primera decisión vinculante, relativa a una decisión sobre la compañía Twitter.

En este caso, la autoridad principal era la Comisionada irlandesa y eran autoridades afectadas la práctica totalidad de autoridades de la Unión, dada la extensión de la actividad de la compañía afectada por el procedimiento.

Puede resumirse el caso señalando que Twitter sufrió una quiebra de seguridad en 2014. La quiebra se debió a una modificación en la programación de los servicios de Twitter y se extendió hasta que, en 2018, y a través de un programa para la detección de errores establecido por Twitter Inc. (la empresa matriz estadounidense) esta tuvo conocimiento de su existencia.



Hubo varios problemas de notificación a Twitter Irlanda, que aparentemente actúa como establecimiento principal del responsable en la UE, y eso determinó que la notificación de la quiebra a la autoridad irlandesa se produjera sin respetar los criterios establecidos en el RGPD.

La autoridad irlandesa abrió un procedimiento por la notificación tardía, mientras que la quiebra como tal fue abordada, según la autoridad irlandesa, en el marco de otros procedimientos abiertos en relación con otras quiebras que afectaron a la misma compañía en ese periodo. La autoridad irlandesa remitió a las demás autoridades su propuesta de decisión en el mes de junio y las autoridades de Francia, Alemania (Hamburgo), Holanda, Italia, Hungría y España presentaron objeciones.

Antes de resumir el contenido de la decisión final, conviene señalar que en este caso concurrieron varios condicionantes que han tenido una gran influencia en el resultado final, entre ellas la de tratarse de la primera decisión del Comité, el hecho de que las objeciones se formularan antes de finalizar las Directrices sobre Objeciones Pertinentes y Motivadas antes mencionadas o la evidencia de que el plazo previsto por el RGPD para este procedimiento es muy breve.

A la vista de estos condicionantes, se optó por un enfoque centrado en alcanzar un resultado equilibrado, que tuviera en cuenta todas las limitaciones asociadas al hecho de ser esta la primera decisión, al tiempo que satisficiera razonablemente a todas las partes y que respondiera a unos criterios de rigor jurídico suficientes para soportar el escrutinio al que va a ser sometida esta primera decisión. Debe señalarse que tanto en la definición de este enfoque como en su plasmación práctica la AEPD, como co-coordinadora del subgrupo de Enforcement, ha jugado un papel central, junto con el Secretariado del Comité.

El resultado final fue que la mayoría de las objeciones se rechazaron por motivos formales. Para ello, el Comité se amparó en la previsión del RGPD que exige que las objeciones demuestren la importancia que entrañaría para los derechos y libertades de los interesados el mantener la decisión de la

autoridad irlandesa. La mayoría de las objeciones no habían abordado esa cuestión (entre otros motivos porque su importancia solo se puso de relieve en el contexto de las repetidas Directrices sobre Objeciones Pertinentes y Motivadas), lo que permitió desestimarlas.

Este rechazo por razones formales incluía la objeción de la AEPD respecto a la posición de Twitter Inc. y Twitter Irlanda.

Por otro lado, en todos los casos en que se ha desestimado una reclamación por motivos formales se ha incluido un párrafo subrayando esos motivos formales y estableciendo que el Comité no ha entrado en el fondo de la objeción y que podrá hacerlo en el futuro, incluso con los mismos actores, si se presenta una objeción que sea “admitida a trámite”

Se han incluido varios párrafos sobre la obligación de cooperar durante el procedimiento. Ese mismo mensaje se incluyó también en las Directrices sobre concepto de objeciones pertinentes y motivadas. En este caso, se condiciona la posibilidad de poder rechazar objeciones por no pertinentes al hecho de que la autoridad líder haya cooperado adecuadamente durante la tramitación del procedimiento. Esta inclusión era particularmente importante para las autoridades objetantes, incluida la española, ante los problemas que ha planteado la autoridad irlandesa para establecer una cooperación eficaz en este tipo de procedimientos.

Se aceptaron tres objeciones que pedían elevar la multa. La aceptación no fija una cifra fija, sino que tan solo señala que la sanción prevista por la autoridad líder no satisface los criterios de eficacia, proporcionalidad y efecto disuasorio y que, por tanto, tiene que recalcularse y elevarse. De nuevo en este punto se incluye la ya mencionada cláusula señalando que esta valoración se hace sin cuestionar el hallazgo de la autoridad irlandesa sobre la infracción. El Comité solo dice que, si la infracción detectada es esa, la sanción debiera ser más alta. Pero no entra en si la infracción pudiera ser otra.

La AEPD considera que, a la vista de las circunstancias que rodearon este caso, el resultado es razonablemente satisfactorio. La decisión final no adopta posiciones sobre el fondo de la objeción planteada, lo que permite volver posteriormente sobre la misma cuestión, y, al mismo tiempo, se incluyen elementos relacionados con la actuación de la autoridad líder en el procedimiento.

De acuerdo con el artículo 65 RGPD, la decisión se comunica a la autoridad principal y a las autoridades objetantes y no es publicada hasta que el CEPD recibe (en el plazo de un mes desde la comunicación) la notificación de la autoridad principal en el sentido de que ha aplicado la decisión del Comité. Por ello, y aunque la decisión se adoptó el 9 de noviembre, *su publicación se retrasó hasta el mes de diciembre*.

Es de esperar que a lo largo de 2021 el Comité se vea en la necesidad de adoptar varias decisiones vinculantes para resolver conflictos en el marco del mecanismo de cooperación. Hay varios procedimientos que afectan a importantes compañías de Internet cuya actividad tiene un gran impacto en toda la Unión Europea que es probable que finalicen en este año y cuyo contenido es presumible que dé lugar a diferentes interpretaciones y posiciones entre las autoridades afectadas.

Conviene señalar aquí, aunque se trate de una cuestión no inmediatamente relacionada con la actividad del Comité, que el mecanismo de cooperación al que se viene haciendo referencia es otra de las manifestaciones de la dimensión supranacional que el Reglamento ha impuesto a la práctica totalidad de las actividades de las autoridades de supervisión.

No es este el lugar para describir con detalle este procedimiento, también conocido como de “ventanilla única”. Pero sí es necesario señalar que las condiciones que determinan la aplicación de este mecanismo hacen que los procedimientos de investigación y sancionadores que se inicien respecto a todas las grandes compañías que operan en la Unión Europea tengan que desarrollarse de acuerdo con esta modalidad de “ventanilla única”.

En términos prácticos, como se comenta con más detalle en el apartado 6 de esta Memoria dedicado a la actividad de inspección de la Agencia (ver Sección 7 “La potestad de supervisión”), ello supone un importante incremento en la carga de trabajo de las autoridades de supervisión. No sólo por la necesidad de cumplir con todos los trámites de comunicación y valoración de propuestas que conlleva un procedimiento coordinado entre una pluralidad de autoridades, sino también por el hecho de que el proceso de decisión incluye una negociación entre la autoridad líder y las autoridades afectadas que no existe en los casos en que solo interviene una autoridad.

Además, incluso en los casos en que no se aplica este procedimiento de cooperación y cada autoridad de supervisión actúa separadamente, esta actuación está también condicionada por los criterios y posiciones que el Comité haya podido adoptar a través de algunos de los instrumentos que se han expuesto anteriormente.

El hecho de que el centro de gravedad de las políticas de protección de datos se esté desplazando desde las capitales europeas a Bruselas se manifiesta también en otros aspectos de la actividad del Comité.

En este sentido, cabe señalar que, en el periodo transcurrido desde mayo de 2018, e incluso ya con anterioridad, el Comité ha ido evolucionando paulatinamente en sus métodos de trabajo, avanzando en su tránsito desde la forma de grupo de trabajo a su consolidación como organismo de la Unión.

Esta evolución se constata en muchos aspectos. Por ejemplo, el Comité ha pasado de trabajar sobre la base de un programa de trabajo anual, que tenía como principal objetivo ordenar su actividad a lo largo de su vigencia, a elaborar una Estrategia que pretende dirigir su actuación hacia unos objetivos considerados prioritarios. Dicho en otros términos, mientras que en el pasado el programa de trabajo era el resultado de la suma de las acciones previstas para un año por parte de todos los subgrupos que integraban el GT29 (y en sus primeras etapas también el Comité) a partir de 2020, cuando se aprobó la *Estrategia 2021-2023*, el

Comité decidirá qué acciones concretas desarrolla en sus subgrupos para implementar una serie de objetivos que considera estratégicos.

Del mismo modo, el Comité ha tomado una serie de medidas que derivan de esa nueva condición de organismo de la Unión. Una de ellas ha sido la aprobación, en octubre de 2020, del Marco Coordinado de Supervisión (*Coordinated Enforcement Framework*). Como el propio marco señala, su objetivo es “facilitar acciones conjuntas de manera flexible pero coordinada, que van desde la sensibilización conjunta y la recopilación de información hasta «barridos» de aplicación e investigaciones conjuntas. El propósito de las acciones coordinadas anuales periódicas es promover el cumplimiento, facultar a los titulares de los datos a que ejerzan sus derechos, fomentar la sensibilización y/o aumentar el conocimiento de las autoridades de supervisión”.

El Comité, como organismo de la Unión, no tiene atribuidas funciones de supervisión del cumplimiento (“enforcement”). Sin embargo, y en el contexto de sus tareas para asegurar la aplicación coherente del RGPD y examinar cualquier cuestión que afecte a éste, así como la de promover la cooperación entre sus miembros, el Comité ha considerado oportuno desarrollar un marco de supervisión propio, que se proyecte en materias de interés común.

Para lograrlo, este MCS (CEF, en sus siglas en inglés), permitirá identificar cada año tanto áreas de actuación como tipos de acciones a desarrollar de forma coordinada entre las autoridades de los Estados Miembros. Las áreas pueden incluir desde un determinado sector de actividad o una tecnología hasta la aplicación de una concreta disposición del RGPD. Las acciones, por su parte, pueden abarcar desde una simple prospección simultánea y coordinada hasta una actividad formal de “enforcement” que puede finalizar en la imposición de medidas correctivas.

**El Comité Europeo de Protección de Datos (CEPD) solo establece el marco para alcanzar acuerdos sobre el ámbito de la acción conjunta y coordinar su desarrollo y las autoridades nacionales de supervisión llevan a cabo la actividad de que se trate.**

Es importante destacar que no es el Comité el que lleva a cabo esas acciones. El Comité tan solo establece el marco para alcanzar acuerdos tanto sobre el ámbito de la acción conjunta y para coordinar su desarrollo. Son las autoridades nacionales de supervisión las que llevan a cabo la actividad de que se trate y las que ejercen sus potestades en la aplicación de las medidas que en cada caso se contemplan.

**En 2021 tendrá lugar la primera de estas acciones bajo la coordinación del Comité.**

Otra iniciativa que el Comité ha puesto en marcha ha sido la creación de un “Support Pool of Experts” (una traducción aproximada de este nombre al español podría ser la de “Grupo de Apoyo de Expertos”), *cuya creación se aprobó en diciembre de 2020*. El objetivo de esta iniciativa es establecer un listado de expertos, tanto de las propias autoridades nacionales como expertos externos, que puedan ser desplegados, a solicitud de una o varias autoridades y en casos de interés común, para apoyar las actuaciones de “enforcement” de esas autoridades.

La coordinación de este Grupo correrá a cargo del Secretariado del Comité y está previsto que en 2021 se lance un proyecto piloto para testar en la práctica el funcionamiento de este Grupo.

Con todo, las circunstancias en que transcurrió 2020 han servido para poner de manifiesto por la vía de los hechos que el Comité es algo diferente a un mero foro de encuentro de las autoridades de supervisión europea.

La pandemia de la COVID-19 interrumpió la posibilidad de celebrar las habituales reuniones presenciales del Comité, tanto en formato plenario como a nivel de subgrupo de expertos, ya desde febrero de 2020. Sin embargo, el Comité decidió no solo mantener su actividad habitual a través de métodos de trabajo en remoto, sino intensificarla para estar en condiciones de responder a las exigencias que la pandemia traía aparejadas.

Para ello, el Secretariado del Comité, a la vista de que los sistemas de videoconferencia empleados hasta entonces no respondían a las nuevas necesidades, asociadas a un uso generalizado de esta forma de comunicación, negoció la utilización por parte del Comité de un sistema de videoconferencia más avanzado empleado habitualmente por el Parlamento Europeo.

Con este sistema, unido una potenciación de otros recursos ya empleados anteriormente para el trabajo en común de los miembros del Comité, el Comité ha podido desarrollar a lo largo de 2020 más de 270 reuniones, de las cuales corresponden 27 corresponden a reuniones plenarias del Comité y 145 a reuniones de sus subgrupos de expertos. El resto son reuniones de los equipos de redacción de los borradores de los documentos que, posteriormente, son discutidos en los subgrupos y remitidos al plenario para su aprobación definitiva.

La Agencia Española ha participado en todas las reuniones plenarias y de subgrupo, así como en más de la mitad de las reuniones de grupos de redacción. Al mismo tiempo, y como se ha repetido en anteriores memorias, asume la coordinación de dos de estos subgrupos de expertos, 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”).

Hay que destacar que estas reuniones virtuales comenzaron siendo de una duración limitada (no más de tres horas), ante la falta de experiencia de los participantes y las dificultades impuestas por el anterior sistema de videoconferencia empleado. Sin embargo, en poco tiempo, y coincidiendo además con la implantación del nuevo sistema, este tipo de reuniones han pasado a tener características similares a las que se celebraban presencialmente en Bruselas, es decir, reuniones de un día, día y medio o, incluso, dos días, tanto a nivel de plenario como de subgrupo.

### 4.3. Tecnológicos

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

En el año 2020 la Unidad de Evaluación y Estudios Tecnológicos se adscribe al organigrama de la AEPD con la denominación de División de Innovación Tecnológica (DIT) formando parte de la Unidad de Apoyo de la Dirección y bajo la responsabilidad de un Director, lo que supone la consolidación definitiva de lo que fue la UEET en la estructura de esta Agencia. De esta forma, la AEPD ha seguido el ejemplo de otras autoridades como la CNIL francesa, que dispone de una Dirección de Tecnologías e Innovación, o el ICO británico, que dispone de una Dirección Ejecutiva de Innovación y Política Tecnológica, entre otros.





Desde esta Unidad se han desarrollado actividades de cooperación con asociaciones y universidades con el objetivo de promover el modelo de cumplimiento que plantea el RGPD.

En julio de 2020, la antigua UEET toma su denominación actual. A fecha de cierre de esta Memoria, la DIT está compuesta por siete miembros, todos funcionarios: un nivel 30, tres niveles 28, dos niveles 26 y un auxiliar (está pendiente cubrir un nuevo nivel 26). El perfil de los funcionarios del grupo A1 y A2 es tecnológico, con profundos conocimientos en protección de datos.

Las competencias asumidas por la DIT han sido las siguientes:

- Asesorar a la dirección de la AEPD, así como a sus distintas unidades, sobre los temas tecnológicos que tienen relevancia en la protección de datos de carácter personal. 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 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.

Las actividades más destacadas de la DIT durante el año 2020 se describen a continuación:

#### ▲ 4.3.1. Elaboración de guías y modelos

Uno de los desafíos planteados durante 2020 ha sido el de dar respuesta desde la AEPD a los diferentes condicionantes que la pandemia ha generado en todos aquellos contextos que se han visto afectados y en los que se ponían de manifiesto cambios relacionados con los tratamientos de datos o con las medidas de seguridad, contexto laboral, sanitario, educativo, económico, etc. En particular desde la DIT se han llevado a cabo la elaboración de los siguientes materiales.



Con relación a guías y nota técnicas, se ha publicado el siguiente material:

- *Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo*
- *Nota sobre el uso de las tecnologías en la lucha contra la COVID-19*
- *Guía de Protección del menor en Internet*
- *Recomendaciones para el despliegue de aplicaciones móviles para el control del acceso a espacios públicos*

Otro material publicado ha sido:

- Post en el blog de la AEPD sobre *Notificación de brechas de seguridad de los datos personales durante el estado de alarma*
- Post en el blog de la AEPD sobre *Tratamientos de Datos Personales en Situaciones de Emergencia*.
- Post en el blog de la AEPD sobre *Campañas de phishing sobre la COVID-19*
- **Infografía:** *Protección del menor en Internet*

**Estos contenidos han registrado un número de más de 115.000 usuarios de la página web de la AEPD, destacando la Nota sobre el uso de las tecnologías en la lucha contra la COVID19 con 33.000 accesos.**

Por otra parte, a través de la participación de la DIT en el subgrupo de Tecnologías del Comité Europeo de Protección de Datos (EDPB), se ha trabajado en la elaboración de los documentos:

- Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-19. Adoptadas el 21 de abril de 2020.

- Statement on the data protection impact of the interoperability of contact tracing apps. Adopted on 16 June 2020

Además, se han realizado numerosas acciones específicas en relación con la pandemia, como han sido el asesoramiento técnico a la dirección, en la realización de informes jurídicos, en las reuniones externas y colaboración con otras entidades y en la elaboración de guías y recomendaciones de otras unidades de la AEPD, la respuesta a consultas previas específicamente relacionadas con la pandemia y colaboración con el canal @informa.

#### ▲ 4.3.2. Elaboración guías, estudios y notas técnicas

Otra de las áreas de actividad en la que se encuentra implicada la DIT es la elaboración de guías, estudios y notas técnicas en las que se vierten recomendaciones de carácter técnico con relación a actividades concretas en las que existe un tratamiento de datos personales, en particular se han desarrollado las siguientes actuaciones.

- Guías y notas técnicas:

1. *Guía de Tecnologías en las Administraciones Públicas*
2. *Guía de Protección de Datos por Defecto*, este último incluye la elaboración de un listado de medidas.
3. *Guía de Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial*
4. *Guía de Protección del menor en Internet*
5. *Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo*
6. *Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para el Sector Privado*
7. *14 equívocos con relación a la identificación y autenticación biométrica*, en colaboración con el EDPS
8. *Introducción a las tecnologías 5G y sus riesgos para la privacidad*

9. *Medidas para minimizar el seguimiento en Internet*

10. *Recomendaciones para el despliegue de aplicaciones móviles en el acceso a espacios públicos, en colaboración con la EPFL-Suiza*

11. *El uso de las tecnologías en la lucha contra la COVID-19*

12. *Orientaciones para la aplicación de la disposición adicional octava y la disposición final duodécima de la LOPDGDD*

➤ **Infografías:**

1. *Infografía de la herramienta Facilita-Emprende*
2. *Infografía sobre Protección del menor en Internet*
3. *Infografía sobre medidas para minimizar el seguimiento en Internet*



Se han iniciado trabajos con relación a orientaciones en Administración Digital en colaboración con la Secretaría General de Administración Digital (SGAD), una Guía sobre Auditoría en Inteligencia Artificial con la colaboración de diversas instituciones, la unificación y actualización de las Guía de Gestión de Riesgo y Guía de Evaluación de Impacto para la Protección de Datos, una nota técnica conjunta con el EDPS y se están trabajando en futuro material relativo a IoT, Blockchain y 5G.

**Las guías y notas técnicas publicadas durante el año 2020 han sido descargadas por más de 163.000 usuarios.**

#### 4.3.3. Mantenimiento y desarrollo de herramientas

En el marco del impulso a la protección de datos, en particular, en el aspecto del desarrollo y mantenimiento de herramientas de ayuda para el cumplimiento por parte de estos, además del mantenimiento de las herramientas Facilita y Gestiona, publicadas en años anteriores, se han realizado las siguientes acciones:

- Publicación de la nueva Herramienta Facilita-Emprende para facilitar a start-ups y emprendedores la adecuación al RGPD de tratamientos de bajo riesgo.
- Publicación de la Herramienta Comunica-Brecha para asesorar a los responsables con relación a la obligación de comunicar a los interesados las brechas de seguridad.
- En el marco de la colaboración con el Ministerio de Trabajo y con la Gerencia de Informática de la Seguridad Social para la adaptación de las herramientas ASSI y SIOM a los requisitos de del RGPD se continúa trabajando para la puesta a disposición de las AAPP a través de la SGAD de herramientas de gestión RGPD.

**El conjunto de herramientas ha tenido más de 45.000 ejecuciones<sup>3</sup> desde el 1 de enero al 30 de noviembre de 2020. En particular, la herramienta Comunica-Brecha, publicada en octubre de 2020, ha tenido en poco más de un mes más de 14.000 ejecuciones.**

<sup>3</sup> Ejecuciones de la herramienta hasta la generación de un informe final. Accesos a las herramientas ha habido más de 90.000

#### ▲ 4.3.4. Otras acciones de impulso a la responsabilidad proactiva

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

Se ha incrementado el contenido técnico del blog de la AEPD con las siguientes publicaciones desde el 1 de enero de 2020 al 30 de noviembre de 2020 (que acumulan aproximadamente 105.000 descargas de usuarios): Blockchain (II): Conceptos básicos desde la protección de datos; Privacidad de grupo; Gobernanza y política de protección de datos; Protección de datos y seguridad; Tratamientos de datos personales en situaciones de emergencia; Vehículos conectados; Recibo del consentimiento: Una herramienta de transparencia y responsabilidad proactiva; ¿Conoces Gestiona?; Cifrado y Privacidad IV: Pruebas de conocimiento cero; Cifrado y Privacidad III: Cifrado Homomórfico; Cifrado y Privacidad II: El tiempo de vida del dato; Riesgos para la privacidad al iniciar sesión con tus cuentas de redes sociales en otras aplicaciones; Los acortadores de URLs y la protección de datos; Recomendaciones para prevención del acoso digital; Brechas de seguridad: el correo electrónico y las plataformas de productividad online; Brechas de seguridad: El Top 5 de las medidas técnicas que debes tener en cuenta; Notificación de brechas de seguridad de los datos personales durante el estado de alarma; Campañas de phishing sobre la COVID-19; Brechas de seguridad: comunicación a los interesados.

➤ Mantenimiento de las siguientes secciones en la página web de la AEPD:

1. Renovación de la sección *Innovación y Tecnología*, con un apartado específico sobre Responsabilidad Proactiva y otro con las publicaciones relativas a AAPP que incluye, entre otros, un apartado de herramientas para las pymes, emprendedores y desarrolladores, guías técnicas y recopilación de las entradas de blog de la AEPD con carácter técnico, en sus dos versiones en castellano e inglés.

2. Renovación de la sección de *Lucha Contra la Violencia de Género y la Violencia Digital con una actualización publicada el 25 de noviembre.*

3. *Brechas de seguridad*

4. *Videovigilancia*

➤ La DIT, como el resto de las unidades de la AEPD, participa activamente en los encuentros para DPD que se coordinan desde el RGPD.

➤ Acciones formativas de divulgación de la responsabilidad proactiva en las que participa la DIT son:

- Participación en el Ciclo de Debates (webinarios) de la AEPD “Innovación y Protección de Datos - Mujer y Ciencia” en la coordinación de los debates.
- Formación para DPD’s y funcionarios de las administraciones públicas en colaboración con el INAP, participación en programas de formación de los funcionarios en diversas administraciones locales, o en el Centro de Estudios Jurídicos (CEJ).
- Máster de Protección de Datos en el ámbito del convenio entre AEPD y la UNED que inició su andadura en enero de 2019 en el que participan y codirigen miembros de esta Unidad.
- Tutorización de nuevos funcionarios en el Máster Universitario en Sistemas y Tecnologías de la Información para la Administración del Estado del INAP
- Universidad del País Vasco en temas de videovigilancia
- Universidad de Vigo sobre Teletrabajo
- Ponente en FIDE con relación a la Guía de Inteligencia Artificial
- AMETIC sobre Inteligencia Artificial
- Encuentro con Farmaindustria para presentar las garantías de los procedimientos de monitorización remota de ensayos clínicos.
- Jornadas 2020 Tech & Privacy Summit. Gobierno y Seguridad de los Datos

- Eventos de divulgación de las herramientas Facilita y Facilita-Emprende organizados por la Cruz Roja
- 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: como el observatorio BIDA-Banco de España, miembro del comité científico del III Digital Law World Congress.
- Reuniones con entidades que presentan iniciativas tecnológicas o precisan asesoramiento tecnológico, entre otros: Ministerio de Educación, Ministerio del Interior, Ministerio de Justicia, Ministerio de Asuntos Exteriores, SGAD, Centro de Investigaciones Sociológicas, Junta de Comunidades de Castilla La Mancha, Gobierno de Canarias, Comunidad de Madrid, Autocontrol, Alastria, Telefónica, Truata, AENA, AELEC, Asociación de Fundaciones, Asociación de Hosteleros, Farmaindustria, APEP, FUNDAE, CEOE, SERLAB, Iberpay, Veridas, Caixabank, Amazon, Facebook, Google y contacto con diversos investigadores.

#### 4.3.5. Notificaciones de violaciones de seguridad (brechas de seguridad)

El artículo 33 del RGPD establece la obligación y condiciones para que el responsable del tratamiento notifique a la autoridad de control competente toda violación de la seguridad de los datos personales, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. El artículo 34 establece las condiciones por las que será obligatorio la comunicación de una violación de la seguridad de los datos personales al interesado.

Por otro lado, el artículo 32 del RGPD establece que el responsable y el encargado aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. Para evaluar el nivel de riesgo es necesario tener particularmente en cuenta los riesgos que presente el tratamiento de datos como consecuencia de la destrucción, pérdida o alteración accidental o ilícita, o la comunicación o acceso no autorizado a dichos datos.

En determinados casos, tras la notificación de la brecha es necesario trasladar la notificación de la brecha de seguridad a los servicios de inspección para que éstos 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.



Para determinar qué brechas de seguridad serán trasladadas a los servicios de inspección, es necesario disponer de un criterio uniforme y consistente para decidir dicho traslado, y éste ha de ser consistente con los criterios utilizados para determinar la gravedad de una infracción que se derive de la existencia de una brecha de seguridad. Para ello, en el marco de uniformidad en la aplicación del RGPD del Comité Europeo de Protección de Datos se están siguiendo los criterios comunes que se están valorando para elaboración de futuras directrices. La valoración queda circunscrita a los datos limitados que proporciona el responsable en el formulario de notificación de brecha de seguridad de datos personales, y a lo sumo, a la información disponible en la Autoridad de Control sobre los antecedentes del responsable de tratamiento.

La AEPD publica, en la sección sobre *Brechas de Seguridad* de la página web de la AEPD, 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.

En el año 2020, en cuanto a la tipología de las brechas notificadas, hay que destacar las relativas al ransomware. Esta es una ciberamenaza con gran impacto sobre los datos personales que es bien conocida y cada vez más común. En el marco de la COVID-19, este tipo de ataques están afectando de forma significativa a tratamientos de datos de salud. 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. Estas medidas se han de orientar en tres direcciones: intentar evitar su materialización, tener capacidad para su detección temprana y rápida evaluación de las consecuencias y 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 seguridad se pueden resumir de la siguiente forma:

- 1.370 notificaciones de brechas de seguridad se han gestionado durante el periodo entre el 1 de enero de 2020 y el 31 de diciembre de 2020.
- Establecimiento de los siguientes criterios internos de gestión de brechas de seguridad:
  - Respuesta a responsables de tratamiento ante notificaciones de brechas de seguridad de los datos personales
  - Criterios para el traslado a inspección de una notificación de brecha de seguridad de los datos personales
  - Criterios para obligar a comunicar a los interesados una brecha de seguridad
  - Nuevo formulario brechas de seguridad

Otras tareas relacionadas con la gestión de brechas de seguridad son:

- Mantenimiento de la sección sobre brechas de seguridad 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 seguridad.
- 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 seguridad.



#### ▲ 4.3.6. Evaluaciones de impacto y consultas previas

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

- Hasta el 30 de noviembre de 2020 se han remitido a la AEPD y gestionado un total de 12 solicitudes de consulta previa.
- Seguimiento de la herramienta de gestión de solicitudes de consultas previas.

El número de consultas previas recibidas, y la calidad de las evaluaciones realizadas, evidencia que tanto la aplicación del artículo 35 “Evaluación de impacto relativa a la protección de datos” y 36 “Consulta previa” tiene que ser mejor entendido por los responsables del tratamiento.

La gestión del riesgo es uno de los pilares de la gestión de cualquier organización. El RGPD hace referencia al término “riesgo” en los 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. El riesgo para los derechos y libertades atañe principalmente a los derechos a la protección de datos y a la intimidad, más aún, las Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento **«entraña probablemente un alto riesgo»** a efectos del Reglamento (UE) 2016/679 del Comité Europeo de Protección de Datos interpretan que la protección se ha de extender a otros derechos fundamentales. Específicamente, se señalan la libertad de expresión la libertad de pensamiento, la libertad de circulación, la prohibición de discriminación, y la libertad de conciencia y de religión.

La Evaluación de Impacto para la Protección de Datos (EIPD) forma parte del proceso de gestión de riesgos para los derechos y libertades añadiendo un grado más elevado de profundidad en el análisis, de accountability (por ejemplo, documentación) y de control por parte de las autoridades de control. Sin embargo, la EIPD no es obligatoria para todos los tratamientos: solo será obligatoria en caso de tratamientos de alto riesgo.

De igual forma, no es obligatorio realizar la consulta previa para todos los tratamientos, ni siquiera para todos los que hayan llevado a cabo una EIPD. El proceso de consulta previa tiene como objeto evaluar acciones para el caso de que un tratamiento con obligación o necesidad de realizar una EIPD entrañe, por la forma de implementarlo, la extensión de los datos, o el contexto, y sin olvidar el conjunto de las garantías implementadas, un nivel de riesgo residual para los derechos y libertades de los ciudadanos que podría resultar inaceptables.

Por lo tanto, no es objeto de la consulta previa determinar, por ejemplo, cuál debería ser la base jurídica para legitimar el tratamiento o si dicha base jurídica está adecuadamente establecida. Tampoco es objeto de la consulta previa evaluar la posibilidad de obviar la aplicación de un derecho específico o cualquier otro aspecto que no esté directamente relacionado con el hecho de que el responsable presenta en la consulta un tratamiento legítimo, que cumple con los principios y derechos establecidos con el RGPD, pero que, a su vez, implica un elevado nivel de riesgo residual para los derechos y libertades.

Con anterioridad al marco temporal de esta Memoria, la AEPD hizo un esfuerzo para facilitar a los responsables la aplicación de estas obligaciones, por ejemplo, con la publicación de la *Guía práctica de análisis de riesgos para el tratamiento de datos personales*, la *Guía práctica para las evaluaciones de impacto en la protección de datos personales*, la *Listas de tipos de tratamientos de datos que requieren EIPD (art 35.4)*, la *Lista orientativa de tipos de tratamientos de datos que no requieren una evaluación de impacto relativa a la protección de datos (art 35.5)*, y el *Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para Administraciones Públicas* o el *Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para el Sector Privado*.

La AEPD es consciente de que es necesario realizar aún más acciones para hacer del cumplimiento de estas obligaciones una herramienta eficaz y eficiente para la protección de los derechos y libertades de los interesados. En este sentido, durante el año 2020 se han planificado nuevas iniciativas para dar respuesta a estos retos que se harán efectivas en sucesivos ejercicios.

#### ▲ 4.3.7. Colaboraciones con la Administración Pública, Universidad y otras entidades nacionales

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

- Autoridades Autonómicas de Protección de Datos en aspectos tecnológicos, en particular, con la cesión del código de la herramienta Comunica-Brecha al Consejo de Transparencia y Protección de Datos de Andalucía.
- Secretaría General de Administración Digital, (SGAD) en el desarrollo y revisión de guías para las AAPP.
- 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 Tecnológico 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-IMDEA Networks: con la que se ha realizado un contrato de colaboración sobre privacidad en móviles.

- Universidad de Alcalá de Henares: 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
- Fundación Éticas: Contrato para el desarrollo de guías de auditorías de aplicaciones de Inteligencia Artificial
- Grupo OdiselA, 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.

#### ▲ 4.3.8. Acciones y colaboraciones internacionales.

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 participando como co-revisores en la guía sobre notificación de brechas de seguridad, guía de Blockchain y la guía de anonimización (pendientes de publicar) así como ponentes en la carta del EDPB sobre “Posibilidad de establecer que todas las computadoras portátiles nuevas que ingresen al mercado de la UE necesitarían estar equipadas con una cubierta de cámara física”.

- Colaboración con el Supervisor Europeo de Protección de Datos, que se ha materializado en la publicación en común de una nota sobre equívocos en biometría y se está trabajando en una conjunta sobre equívocos en anonimización.
- Participación en el grupo de Inteligencia Artificial de la Conferencia Internacional.
- Colaboración con la Universidad de las Naciones Unidas en el campo de blockchain y con el Supervisor Europeo de Protección de Datos en temas tecnológicos.
- Colaboración con la Red Iberoamericana como revisores de los documentos publicados sobre Big Data e Inteligencia Artificial y el borrador de recomendaciones para el diseño de políticas de protección de datos en entornos de computación en la nube.
- 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”.
- Finalmente, colaboración con la División Internacional en la participación española en acciones puntuales internacionales, como cuestionarios con el GAFI, grupo FINMAT, ENISA.

#### ▲ 4.3.9. Otras acciones

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:

- En cuanto a formación interna, la DIT ha impartido:
  - Curso de Análisis de Riesgos y Evaluación de Impacto de la Privacidad, de 16 horas.
  - Curso de Cookies, de 4 horas.
  - Blockchain, de 3 horas para el Comité de Coordinación
- Desde la DIT se viene dando soporte al canal *INFORMA* 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.





## 5. Al servicio de los ciudadanos

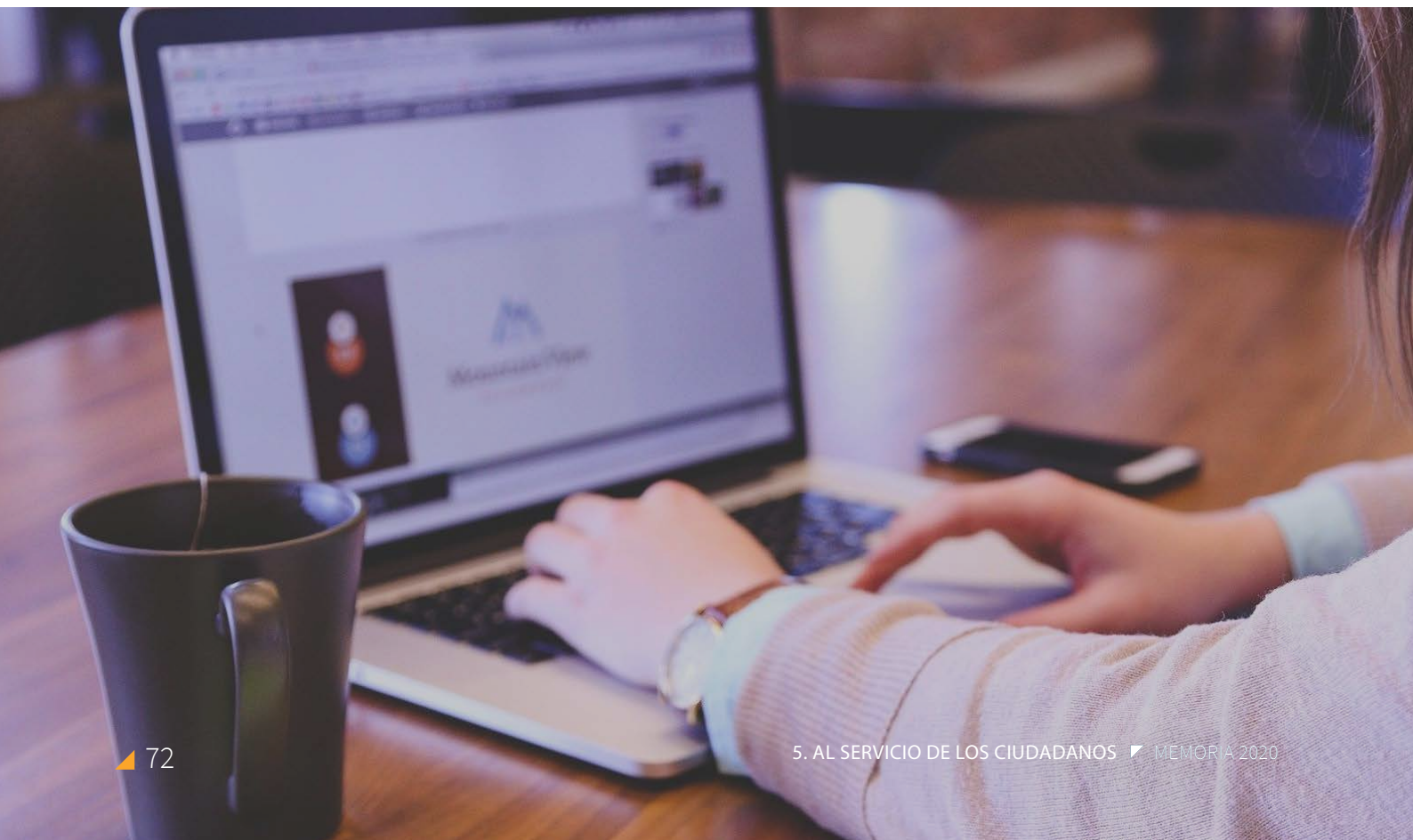
### 5.1. El Estado de Alarma – COVID-19 y la atención a los ciudadanos

La actividad de la Subdirección General del Registro General de Protección de Datos, como la de todas las áreas de la Agencia Española de Protección de Datos durante 2020, ha estado condicionada por la situación de emergencia de salud pública producida por la COVID-19, entre ellos el servicio tradicional de atención presencial al ciudadano, que dejó de prestarse el 13 de marzo para pasar a reforzar el servicio de atención telefónica.

La cancelación de la atención presencial se vio compensada con las demás vías de comunicación con los ciudadanos, telefónica, electrónica o a través de las consultas a las FAQs, que experimentaron un crecimiento respecto a las del año 2019, como se puede apreciar en el apartado final de esta Memoria, la Agencia en cifras.

El resto de las funciones y servicios de la Subdirección se han realizado y prestado en situación de teletrabajo sin que se haya resentido su eficacia o productividad, manteniéndose en términos similares a los de ejercicios anteriores.

Así mismo, la pandemia dio lugar al desarrollo de recursos específicos para atender las consultas que ha provocado la interrelación de las actuaciones para hacer frente a la COVID-19 y la protección de datos personales, como la creación de un espacio en la web dedicado a *Protección de datos y coronavirus*, o la publicación de FAQs temáticas elaboradas por la Agencia a partir de las preguntas recibidas y que se han demostrado de utilidad para los ciudadanos a la vista del número de consultas registradas.



## 13 de marzo de 2020

---

Se dio respuesta a cuestiones como:

- Que los empleadores, conforme a la normativa sanitaria, laboral, en particular de la de prevención de riesgos laborales y de acuerdo con las garantías que establecen, pueden conocer si las personas trabajadoras están infectadas de COVID-19 para garantizar su salud y evitar contagios al resto de trabajadores y adoptar las medidas previstas por las autoridades competentes.
- Que pueden comunicar esa información al resto del personal de la empresa, lo que debería realizarse sin identificar a la persona afectada a fin de mantener su privacidad, pero si así no fuera posible alcanzar la finalidad de proteger la salud, o se desaconseja por las autoridades sanitarias, podría proporcionarse su identidad.
- La obligación legal de los empleadores de proteger la salud de las personas trabajadoras y mantener el lugar de trabajo libre de riesgos sanitarios, lo que justifica que puedan recabar información a los empleados y visitantes externos sobre síntomas o factores de riesgo, como países visitados con alta prevalencia del virus y en el marco temporal de incubación de la enfermedad, fue antes de la declaración del estado de alarma, que responda al principio de proporcionalidad.
- La obligación del trabajador que está infectado por la COVID-19, o sometido a aislamiento preventivo, de informar a su empleador o, en su caso, a los delegados de prevención de riesgos de estas circunstancias, en situación en la que prima el derecho a la protección de la salud del resto de trabajadores y de la población en general.
- La toma de temperatura a los trabajadores por personal de seguridad para verificar si su estado de salud puede constituir un peligro para ellas mismas, para el resto del personal, o para otras personas relacionadas con la empresa, como salvaguarda de la salud de los trabajadores que debe limitarse a la finalidad específica de contener la propagación de la COVID-19.

## 16 de marzo

---

Ante la proliferación de páginas web y aplicaciones móviles que ofrecían ayuda y servicios para autoevaluar y aconsejar en relación con el Coronavirus, se advirtió al conjunto de la ciudadanía de los riesgos que implica el facilitar categorías de datos sensibles, como son los relativos a la salud, a estas webs y apps, incluso en aquellos casos en los que aparentemente esos datos no se asocian a la identidad del usuario que utiliza la aplicación, pues no proporcionaban la información exigible para identificar a los responsables, ni incluían las finalidades para las que podrían tratarse los datos (alguna de ellas incluso con los logos del Ministerio de Sanidad), y se informaba de que se iniciarían actuaciones de investigación para determinar la ilicitud de los tratamientos de datos personales, identificar a sus responsables e imponerles en tal caso importantes sanciones económicas.

## 6 de abril

---

Sobre el ejercicio de los derechos que la regulación del derecho fundamental a la protección de datos personales establece durante la vigencia del estado de alarma y en las que se explica:

- Que el estado de alarma no ha supuesto la suspensión del derecho fundamental a la protección de datos ni, en consecuencia, de los plazos para dar respuesta al ejercicio de los derechos que la normativa atribuye a las personas, ya se ejerzan ante el sector privado o público, pero que la misma normativa permite prorrogar el plazo establecido, de un mes, por otros dos más, siempre que el motivo sea consecuencia de cómo afecta el COVID-19.
- Que la obligación de notificar las brechas de seguridad de datos personales y de comunicarlas a los afectados, cuando entrañe un alto riesgo para sus derechos y libertades, en los plazos establecidos en la normativa de protección de datos se mantiene durante la vigencia del estado de alarma.



## 10 de junio

---

Se publicó un informe en relación con una consulta planteada sobre el acceso remoto con verificación de datos fuente por parte de los monitores de los ensayos clínicos como medida excepcional para garantizar la continuidad de la monitorización, crítica para la conducción de ensayos y tratamientos en investigación y cuya paralización puede tener impacto en la vida de los pacientes.

**En el ámbito educativo, el 19 de junio** se publicó una nueva FAQ, en relación con las cautelas que se deben adoptar en las clases y exámenes online.

**En el ámbito laboral, el 18 de junio se publicó el comunicado sobre la información acerca de tener anticuerpos de la COVID-19 para la oferta y búsqueda de empleo y el 23 de junio,** se realizó la publicación de nuevas FAQ, sobre si para solicitar y/o acceder a un puesto de trabajo se puede pedir como requisito que tenga anticuerpos de la COVID-19, así como si se puede incluir este dato en el CV.

Desde el área de atención al ciudadano se ha prestado una especial atención a resolver no sólo sus consultas y dudas, sino también las que albergan los sujetos obligados a través de las distintas vías de acceso a la Agencia y la celebración de jornadas, todas ellas en formato online, con aquellos sectores en los que la COVID-19 ha tenido un fuerte impacto en protección de datos:

## 14 de mayo

---

Con los DPD de las Consejerías de Educación de prácticamente la totalidad de las Comunidades Autónomas, así como de diversos representantes de las patronales del sector educativo para tratar y resolver las dudas y preocupaciones que la enseñanza online, en particular la realización de pruebas de evaluación ha generado en materia de protección de datos en la comunidad educativa.

## 29 de mayo

---

Con los DPD del sector de la salud de las CCAA y del sector privado, la Alianza de Sanidad Privada Española, que incluye los centros sanitarios de las grandes aseguradoras médicas, y Farmaindustria para tratar las dudas y cuestiones que plantea el tratamiento de datos de salud y el coronavirus.

## 23 de julio

---

Con CEOE para examinar el impacto en protección de datos de las medidas que todo el sector empresarial ha tenido que implantar con motivo de la COVID-19.

## 5.2. Educación y Menores

Como en años anteriores, el enfoque principal del Servicio de Educación y Menores de la Agencia se ha puesto en la prevención, principalmente dirigida a la sensibilización y formación de los menores para la utilización responsable y segura de sus datos personales en internet y en particular en las redes sociales, así como en la concienciación y formación de familias y docentes de la educación digital, ya que como siempre incidimos son los actores principales para conseguir trasladar a los menores el uso seguro y responsable de sus datos personales.

Conviene recordar que este Servicio se difunde como Canal Joven. Este Canal dispone desde sus inicios, en 2015, de varias vías de comunicación con los ciudadanos dirigidas a dar respuesta a las cuestiones o dudas que se planteen referentes a este ámbito. El Canal integra una dirección de correo electrónico ([canaljoven@aepd.es](mailto:canaljoven@aepd.es)) donde se reciben consultas relacionadas con la protección de datos, la educación y los menores, un teléfono específico también para consultas sobre estos temas (901 233 144), y un servicio de información de WhatsApp (616 172 204). A las consultas que llegan por estos medios se suman las recibidas a través de la Sede Electrónica de la Agencia, vía habitual de recepción de consultas y que desde el Área de Atención al Ciudadano se deriva al equipo del Canal Joven para su respuesta.

Por todas estas vías se ha dado respuesta, durante el año 2020, a 1.393 consultas, siendo las más frecuentes las recibidas telefónicamente, con 552 llamadas, lo que supone casi un 40% del total, además de 424 consultas a través de WhatsApp, que representa un 30%, 241 dirigidas a la dirección electrónica de Canal Joven, lo que supone un 17%, y 176 consultas que se han recibido a través de la Sede electrónica de la Agencia, lo que equivale casi a un 13% del total de consultas

Las consultas que más se han recibido en el Servicio de Educación y Menores durante 2020 han sido las planteadas por los progenitores y los centros educativos, tanto de primaria como de secundaria (CEIP e IES). Destaca que la mayoría de las cuestiones de estos colectivos se relacionan con los tratamientos de datos personales de los alumnos para el ejercicio de la función educativa que llevan a cabo los centros tanto en el curso 19-20 como con el inicio del curso 20-21.

Fundamentalmente, plantean la necesidad de continuar impartiendo clases online a los alumnos en un momento tan extraordinario como el originado por la pandemia de la COVID-19, utilizando para ello herramientas educativas que pueden llegar a generar dudas en cuanto a su utilización y las medidas de seguridad que debe tomar la comunidad educativa en general.

Así, al tener que desarrollar los centros docentes su función educativa en un nuevo escenario, se han visto abocados a utilizar aplicaciones educativas, en ocasiones nuevas para ellos, que ayudan a continuar con su labor de una manera adecuada, lo que ha llevado a plantear numerosas consultas, tanto de familias como de docentes y equipos directivos de centros, sobre si los tratamientos de datos personales que se realizaban se ajustaban a la normativa de protección de datos.

A la vista de la evolución de la línea telefónica de Menores durante 2020, se considera relevante hacer una distinción en relación con los períodos en los que se han recibido más llamadas ya que, al tratarse de un año en el que durante la mayoría del curso lectivo se ha impartido las clases utilizando medios digitales debido al estado de alarma y confinamiento, destacan claramente los meses

durante los que tanto docentes y responsables de centros educativos como padres y madres llamaban para informarse sobre el uso de las plataformas educativas que, aunque ya estuvieran en funcionamiento, planteaban dudas de utilización relacionadas con protección de datos, en especial el mes de junio, con la realización de los exámenes finales online y los meses de septiembre, octubre y noviembre con el inicio del curso escolar 20-21, y la decisión de las autoridades educativas de impartir las clases obligatoriamente en casa tanto a los alumnos de 2º y 3º de la ESO como a los alumnos de Bachiller y FP.

Con este escenario, se intentó ayudar a la comunidad educativa en las diferentes cuestiones que planteaban, así, al tratarse de preguntas recurrentes, se tomó la decisión de publicar unas FAQs sobre *realización de clases y exámenes online* utilizando herramientas de videollamada o plataformas educativas y su *implicación con relación a la protección de datos* tanto de alumnos como de profesores.

Por otra parte, y para ayudar también a este colectivo, se ha publicado en la *web de menores de la Agencia* un documento con el *correo de contacto de los Delegados de Protección de Datos de las Consejerías de Educación de las distintas CCAA*, para facilitar que los interesados o sus padres les puedan plantear consultas concretas sobre herramientas educativas o protocolos de actuación que llevan a cabo en el ámbito de sus competencias.

En cuanto al contenido de ayuda a las familias, se ha publicado una infografía que explica de manera resumida lo que supone *el consentimiento como causa que legitima alguno de los tratamientos que se llevan a cabo por los centros educativos*, en concreto en la publicación de fotos y vídeos de los menores, así como la diferencia que conlleva para los menores a la hora de otorgar dicho consentimiento haber cumplido 14 años.

También se ha participado en distintas acciones formativas dirigidas a los colectivos implicados en educación.

## NOOC “Menores y seguridad en la red” #MenorSeguroEnRed



Del 19 al 25 de mayo se realizó este NOOC, iniciativa que nace de la colaboración entre el Instituto Nacional de Tecnologías Educativas y de Formación del profesorado (INTEF), el Instituto Nacional de Ciberseguridad (INCIBE) y la Agencia Española de Protección de Datos (AEPD) con el objetivo de dar a conocer pautas, herramientas y estrategias que permitan evitar los riesgos de un uso inadecuado o poco seguro de la red, para orientar y acompañar a los menores en el entorno digital y salvaguardar su intimidad y bienestar personal...

Dirigido a la comunidad educativa, especialmente a los padres, a las familias y a los docentes, tutores y equipos directivos de centros educativos, que son responsables de la labor de acompañar a niños y adolescentes en la progresiva adquisición de competencias digitales que les permitan hacer un uso y navegación seguros en los entornos digitales. Contó con 7.211 alumnos, de ellos 2.847 docentes y 4.214 que no declararon serlo. Finalmente, 1.219 participantes superaron el plan de actividades del NOOC. Lo que supone un 16,91%, porcentaje dentro de la media de este tipo de actividades formativas masivas y abiertas.

Se presentaron y compartieron 1.177 retos o trabajos finales. Los seleccionados se encuentran accesibles en [este enlace](#) y en [la web del INTEF](#).

**Curso protección de datos, privacidad y derechos digitales**, celebrado del 15 de septiembre al 17 de noviembre 2020, con un total de 300 docentes y directores de centros educativos inscritos. La participación de la Agencia es fruto de la colaboración con el Instituto Nacional de Tecnologías Educativas y de Formación del profesorado (INTEF).

Centrado en el ámbito docente, los diversos profesionales que contribuyen a proporcionar educación y orientación a los alumnos están participando en esos procesos de tratamiento de datos personales y, por tanto, la privacidad de muchas personas depende en parte de cómo realizan su tarea diaria. Por estos motivos, resulta esencial el factor de responsabilidad que ello conlleva, sea cual sea la función del profesional en el ámbito educativo.

Así mismo, se mantienen reuniones periódicas con los distintos agentes implicados en la protección y seguridad de los menores, en especial del sector educativos.

Una de las últimas iniciativas que se han impulsado, a finales del año pasado, ha sido la creación de un Grupo de Trabajo dedicado a las Tecno-adicciones, o uso excesivo de los medios y servicios online, que integra a los principales agentes en esta materia, en la medida que, de entre las esferas de los jóvenes, afecta a su privacidad y se ve comprometida y en riesgo con la adicción a las TIC. Se plantea un desarrollo de los trabajos desde una perspectiva multidisciplinar que tenga en cuenta no sólo los menores afectados, sino aquellos directamente implicados en su prevención, detección, diagnóstico y en la adopción de medidas para estas conductas.

Adicionalmente, la actuación de la AEPD en este campo se ha centrado en la puesta en práctica del mandato contenido en la Ley Orgánica 3/2018, cuyo artículo 83 estableció, por primera vez, la obligación de que las Administraciones educativas incluyan en el diseño del bloque de asignaturas de libre configuración la competencia digital, así como los elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red.

En este sentido, la Agencia ha promovido junto con el Ministerio de Educación y Formación Profesional, a través del INTEF, el espacio web AseguraTIC destinado a educadores, familias, alumnos y administraciones educativas, cuyo objetivo es contribuir a la protección de los menores en su interacción con Internet canalizando más de 300 recursos aportados por las entidades participantes, principalmente con licencias Creative Commons que facilitan su uso, adaptación y distribución de forma gratuita. En él han participado entidades públicas (INTEF, INCIBE, CNIIE, etc.), y privadas (APEP, Google, Orange, Pantallas Amigas, Fundación ANAR, Facebook, Twitter y Fundación Telefónica).

Esta iniciativa ha sido promovida en 2020 en Iberoamérica a través del proyecto “Fortalecimiento de la estrategia de lucha contra la violencia de género en relación con las niñas, adolescentes y mujeres en internet”, impulsado por la RIPD en el marco del programa Eurososocial, en su eje preventivo.

**Finalmente, señalar que el número de visitas a AseguraTIC, desde su inicio, ha sido de 22.812.**

### 5.3. Comunicación

La Agencia ha puesto en marcha en 2020 numerosas iniciativas para dar visibilidad a las acciones realizadas. A continuación, se recogen las relacionadas con el departamento de prensa y comunicación, así como las acciones de divulgación publicadas en la página web de la Agencia y su agenda institucional.

#### 5.3.1. 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 2020, la cuenta de la AEPD contaba con más de 25.000 seguidores, con una media de 145 seguidores nuevos por semana. Durante 2020 se publicaron en el perfil más de 875 tuits, registrando más de 26.000 menciones y 7,3 millones de impresiones.

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



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

### ▲ 5.3.2. 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 2020 el blog de la Agencia ha recibido casi 223.000 visitas únicas. Entre los posts que han despertado un mayor interés se encuentran los relacionados con las *campañas de phishing sobre la COVID-19*; el *curso online gratuito de menores y seguridad en la Red organizado por la AEPD, el INTEF e INCIBE*; *cómo elaborar el registro de actividades de tratamiento*; el *top 5 de las medidas técnicas para tener en cuenta en materia de brechas de seguridad y la notificación de brechas de seguridad de los datos personales durante el estado de alarma*.

### ▲ 5.3.3. Canal de YouTube

El año 2019 se cerró superando los 2.500 suscriptores en el canal de YouTube de la Agencia. En 2020, esta cifra ha ascendido hasta los 3.500 suscriptores, obteniendo más de 124.000 visualizaciones, lo que representa casi 6.000 horas de visualización. Este canal engloba cuatro tipologías de vídeos: la grabación de conferencias, charlas o webinarios organizados por la Agencia; vídeos con consejos o recomendaciones (cómo evitar la publicidad

no deseada o utilización correcta de cámaras de videovigilancia, entre otros); 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.

### ▲ 5.3.4. 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 emite todos los miércoles, si bien todos los programas se encuentran disponibles de forma permanente en la *página web de Radio 5*.

La emisión comenzó el 4 de julio de 2018 y desde entonces se han emitido 114 piezas temáticas, en las que un experto de la Agencia o la propia conductora del programa ofrece consejos y recomendaciones. De ellas, más de 40 corresponden al año 2020.

### ▲ 5.3.5. Relaciones con los medios

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

A lo largo de 2019, la Agencia atendió más de 520 consultas de medios de comunicación relacionadas con este derecho fundamental. Las consultas más frecuentes han estado relacionadas con cuestiones relativas a la COVID-19 y el tratamiento de datos personales, aunque también hay que destacar el elevado número de peticiones relacionadas con las campañas puestas en marcha por la Agencia, como ‘Por todo lo que hay detrás’ para



difundir el uso del Canal Prioritario y ‘El control es tuyo, que no te controlen’, que se abordarán de forma más detallada con posterioridad. En paralelo, la Agencia registró consultas referidas a notificaciones de brechas de seguridad y relacionadas con sanciones impuestas por la AEPD en aplicación del Reglamento.

**FUE ACOSADO EN EL INSTITUTO PORQUE SU FOTO SE HIZO VIRAL**

Román le sacó una foto mientras le pegaban en el patio, se la pasó a Marina, ella la subió a stories y

No es por la foto, es por todo lo que hay detrás

Si te llega un contenido violento o sexual sin permiso de la víctima, denúncialo en Canal Prioritario. [aepd.es/canalprioritario](https://aepd.es/canalprioritario)

agencia española de protección de datos

Esta labor de atención personalizada a los medios se vio complementada con la difusión de más de 200 notas de prensa, convocatorias y notas de agenda informativa publicadas en la web. En relación con estas últimas, la Agencia publicó en 2020 más de un centenar de reuniones o actos públicos en los que participaron diferentes miembros de esta institución. En cuanto a las notas de prensa publicadas en la web durante 2020 recibieron más de 800.000 visitas. Esta actividad se vio complementada con la participación de la Agencia en la redacción de las notas de prensa de las reuniones plenarios que periódicamente celebra el Comité Europeo de Protección de Datos (CEPD).

## 5.4. Agenda institucional

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

Como viene siendo habitual en los últimos años, 2020 estuvo caracterizado por la organización y participación en reuniones, jornadas, foros, congresos, seminarios web, actos y presentaciones por parte de la Agencia, orientadas a analizar las implicaciones de la normativa de protección de datos en la actividad de distintos ámbitos, a fomentar la cultura de la protección de datos y a difundir iniciativas como el *Canal prioritario* de la AEPD para solicitar la retirada de contenidos de carácter sexual o violento que circulan por internet sin el consentimiento de las personas afectadas. Como consecuencia de la pandemia, gran parte de los actos y webinarios celebrados desde el periodo de confinamiento en adelante se desarrollaron en formato digital.

**Tú también #Puedes Pararlo con el #CanalPrioritario**

.Si tienes conocimiento de la publicación de fotografías, vídeos o audios de **contenido sexual o violento** en Internet sin el consentimiento de las personas afectadas (de nacionalidad española o residentes en España), solicita su retirada en el **Canal prioritario de la AEPD**

[Canal Prioritario >](#) [FAQ's >](#)

Dentro del ámbito del sector público, la AEPD ha participado diversas jornadas, seminarios y reuniones, como las II Jornadas de Igualdad y Justicia, organizadas por el Ministerio de Justicia; el X Congreso Nacional de Innovación y Servicios Públicos – CNIS 2020, organizado por el Club de Innovación y el Ayuntamiento de Madrid; el seminario virtual ‘Teletrabajo y respeto a la protección de datos, ¿es posible?’, organizada por la Universidad de Vigo; el taller digital sobre teletrabajo organizado por el Instituto Nacional de Administración Pública (INAP); la conferencia sobre ‘Protección de datos, privacidad y derechos digitales en los centros educativos’; el curso ‘Protección de datos, privacidad y derechos digitales’, organizado por el Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF); la Masterclass ‘Ley de Protección de Datos’, organizada por el Centro de Referencia Nacional en Administración, Seguros y Finanzas de la Consejería de Economía, Empleo y Competitividad de la Comunidad de Madrid; el Curso de formación de fiscales ‘El derecho fundamental a la protección de datos en el marco de la nueva normativa europea y nacional’, organizado por la Fiscalía General del Estado; la jornada digital centrada en la violencia digital ejercida sobre la mujer, organizada por Casa Mediterráneo y la Subdelegación del Gobierno en Alicante para conmemorar el Día Internacional de la Eliminación de la Violencia contra la Mujer y la reunión mantenida con representantes de la Agencia Española de Medicamentos y Productos Sanitarios (AEMPS), así como de comités de ética de la investigación.

En el plano del sector privado, la AEPD ha mantenido reuniones en 2020, como la reunión digital de trabajo con CEOE, CEPYME y ATA; la CECA y Telefónica. Además, ha participado en varias jornadas, foros y congresos, como del XVII Foro de Seguridad y Protección de Datos de Salud, organizado por la Sociedad Española de Informática de la Salud; la Jornada ‘La protección de informadores, alertadores o denunciantes no admite demora’, enmarcada en el Espacio Compliance de la Comisión Nacional de los Mercados y la Competencia; el XII Foro de Privacidad organizado por ISMS Forum Spain y el Data Privacy Institute; la Jornada ‘Mujer & Tecnología’, organizada por

IAB Spain; el XV Congreso de editores de prensa de la Asociación Española de Editoriales de Publicaciones Periódicas (AEEPP); la mesa redonda digital organizada por Servimedia, dedicada a ‘La influencia de los medios en la sociedad’ durante la pandemia y la 12ª Conferencia Internacional sobre Reutilización de la Información del Sector Público, organizada por la Asociación Multisectorial de la Información (ASEDIE), entre otros.

Por otra parte, la Agencia ha celebrado varias reuniones dirigidas a sectores específicos, como la celebrada con representantes de los principales operadores de telecomunicaciones, el Instituto Nacional de Ciberseguridad, el Ministerio del Interior y Fiscalía con el objetivo de explorar vías de colaboración orientadas a reforzar la privacidad y seguridad de los usuarios de dispositivos móviles; la reunión digital con delegados de protección de datos y las patronales del sector educativo con el objeto de tratar las cuestiones que en materia de privacidad y la protección de datos planteaba la celebración de exámenes online durante el cierre de los centros educativos a causa de la situación de crisis sanitaria motivada por la COVID-19; o la reunión digital con los delegados de protección de datos del sector de la sanidad pública y del sector privado al objeto de aclarar las dudas y cuestiones que plantea el tratamiento de datos de salud ante la situación provocada por la COVID-19.

Además, ha mantenido reuniones de carácter institucional con representantes de departamentos ministeriales o secretarías de Estado, como la celebrada con el ministro de Justicia, Juan Carlos Campo, y el secretario de Estado de Justicia, Pablo Zapatero, y la reunión digital con representantes de la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA). Asimismo, la Agencia ha celebrado una reunión digital con representantes de 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, dentro del marco de cooperación institucional entre la AEPD y las autoridades autonómicas de protección de datos.

La Agencia también ha participado en la reunión de constitución del Grupo de Expertos de Derechos Digitales, organizada por la Secretaría de Estado

de Digitalización e Inteligencia Artificial (SEDIA). Igualmente, ha mantenido reuniones con representantes de colegios, asociaciones, fundaciones, instituciones humanitarias y otros colectivos, como Forética; la Fundación Alicia Koplowitz y la Fundación Profesor Uría; la Fundación Carolina; la Fundación ProFuturo; la Asociación Española de Fundaciones (AEF); la plataforma Xnet; el Consejo General de Colegios Oficiales de Médicos de España; la Asociación Española de Fundaciones y la Fundación Éticas, entre otros.

En este ámbito, la Agencia ha participado en las Jornadas online de la Comisión de Menores de la Asociación Profesional Española de Privacidad (APEP) sobre 'Teleeducación y privacidad de los menores conectados'; la Jornada digital 'Nuevo paradigma: control de aforo, gestión de colas, en relación con la inteligencia de negocio y adecuación a una gestión empresarial segura', organizada por la Asociación Española de Empresas de Seguridad; el Foro 'Actualización de la Guía de cookies de la AEPD' de APEP; el taller teórico práctico online sobre Protección de datos dirigido a profesionales del Tercer Sector, organizado por la Red Europea de Lucha contra la Exclusión Social y la Pobreza en Castilla La-Mancha (EAPN-CLM); y el Digital Law World Congress, organizado por el Ilustre Colegio de Abogados de Barcelona (ICAB), entre otros.

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 reunión-coloquio del Centro Montañés de Investigación y Desarrollo Empresarial (CEMIDE) con una exposición sobre la versión 3.0 de Facilita, y los webinarios organizados por Cruz Roja dedicados al Canal Prioritario; Facilita 2.0, y a la aplicación y dudas en materia de protección de datos. Por otra parte, la Agencia ha organizado y celebrado un ciclo de seis 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 con posterioridad en esta Memoria.

Asimismo, la AEPD ha celebrado una videojornada con cerca de una veintena de representantes de distintos sectores, celebrada con el objetivo de reflexionar sobre el Marco de Responsabilidad Social y Sostenibilidad de la Agencia. Asimismo, ha organizado y celebrado las jornadas digitales 'Nuevos modelos de trabajo, nuevos liderazgos', con el objetivo de abordar cómo el teletrabajo contribuye a fomentar la conciliación y la productividad.

La Agencia ha mantenido reuniones de ámbito internacional, como la celebrada con representantes de la Comisión para la Protección de la Información Personal de Japón (PPC); el Grupo Permanente de Autoridades Nacionales de la Red Iberoamericana de Protección de Datos (RIPD); y el presidente del INAI de México, Francisco Javier Acuña, y la secretaria ejecutiva de la Comisión Interamericana de Mujeres de la Organización de Estados Americanos (OEA), Alejandra Mora, y ha celebrado videoconferencias, como la mantenida con representantes de las autoridades de protección de datos de Argentina, Colombia, México, Perú y Uruguay.

En este contexto, la AEPD ha seguido participando en las reuniones digitales plenarios y los Subgrupos del Comité Europeo de Protección de Datos (CEPD), y ha mantenido reuniones con comisionados de autoridades de dicho Comité para abordar los tratamientos de datos en la lucha contra la COVID-19 y su impacto en la actividad del CEPD. De igual manera, ha participado, entre otros, en el XVIII Encuentro Iberoamericano de Protección de Datos; el 5º Foro Internacional Infoem 'Protección de Datos y Acceso a la Información', organizado por el Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios; el seminario digital 'Pandemia mundial y enfermedad de Datos Personales', organizado por el Consejo para la Transparencia de Chile, y el evento digital 'El Canal Prioritario de la AEPD: una contribución de las Autoridades de Protección de Datos a la lucha contra la violencia digital en las mujeres, niñas y adolescentes', orientado principalmente a las Autoridades de Protección de Datos de México, Uruguay, Perú y Colombia.

Por otra parte, la AEPD ha continuado desarrollando una intensa actividad durante 2020 con la intención de presentar las herramientas e iniciativas desarrolladas en la lucha contra la violencia de género y el acoso a jóvenes, especialmente en relación con el *Canal Prioritario*. Buen ejemplo de ello fue la presentación en el Senado de la campaña ‘Por todo lo que hay detrás’ (que se detalla posteriormente), encaminada a promover la utilización del Canal prioritario de la Agencia.

Dentro de este apartado, la Agencia ha celebrado reuniones dirigidas a la búsqueda de vías de colaboración tanto con entidades del sector público como del privado con el objetivo de impulsar el Canal Prioritario de la Agencia. En este sentido, la Agencia ha mantenido reuniones con el secretario de Estado de Telecomunicaciones e Infraestructuras Digitales, Roberto Sánchez; la delegada del Gobierno contra la Violencia de Género, Victoria Rosell; la fiscal de sala delegada contra la Violencia sobre la mujer, Pilar Martín Nájera, y el fiscal de sala coordinador de Menores, Javier Huete; la presidenta del Observatorio contra la Violencia Doméstica y de Género del Consejo General del Poder Judicial, Ángeles Carmona; las direcciones generales para la Igualdad de Trato y Diversidad Étnico Racial, y de Diversidad Sexual y Derechos LGTBI; la Federación Española de Municipios y Provincias (FEMP); el Instituto de la Mujer y un conjunto de ONG de varios sectores; las direcciones generales de Discapacidad e INJUVE, así como con un conjunto de ONG del ámbito de la discapacidad y la juventud; la consejera de Educación, Formación Profesional y Turismo de Cantabria, Marina Lombó; la Dirección General de Telecomunicaciones y Transformación Digital de la Junta de Castilla y León; la Dirección General de Igualdad de Asturias; el secretario general técnico de la Consellería de Educación, Universidad y Formación Profesional de la Xunta de Galicia, Jesús Oitavén; la valedora do Pobo, María Dolores Fernández Galiño; la alcaldesa de Santander, Gema Igual; la Asociación de Medios de Información (AMI); la Asociación Española de Editoriales de Publicaciones Periódicas; Mediaset; Women in a Legal World, o la red social Facebook, entre otros.

**El Consejo Consultivo de la Agencia de Protección de Datos -órgano colegiado de asesoramiento a la dirección de la Agencia – mantuvo reuniones digitales el 8 de julio y el 17 de diciembre de 2020 para exponer y analizar la actividad de la institución.**

## 5.5. Infografías

La AEPD publicó en 2020 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 unas *recomendaciones en la contratación a distancia de servicios de comunicaciones y energía, consejos para evitar ser espiado o controlado por otras personas a través del dispositivo móvil, varias infografías para saber en qué casos se puede recurrir al Canal prioritario de la Agencia, medidas para minimizar el seguimiento en Internet, recomendaciones para madres, padres y tutores para proteger a los menores en Internet y un esquema con varios de los diferentes recursos gratuitos que pueden ser utilizados por los responsables para cumplir con la normativa de protección de datos.*

Asimismo, también se realizó una *infografía específica sobre Facilita\_Emprende*, una herramienta diseñada para abordar el cumplimiento de las obligaciones en materia de protección de datos para pequeñas empresas con modelos de negocio innovadores que pueden presentar una complejidad adicional a la hora de interpretar los riesgos.



## 5.6. Actividades de divulgación

### 5.6.1. Actividades de divulgación

La AEPD continuó en 2020 con su compromiso de fomentar la cultura de protección de datos entre los ciudadanos y organizaciones a través de diferentes acciones de divulgación con presencia de medios de comunicación.

#### ■ Presentación de la campaña 'Por todo lo que hay detrás' – Canal prioritario 28 de enero

Con motivo de la celebración del Día Internacional de Protección de Datos el 28 de enero, la Agencia presentó en el Senado la campaña 'Por todo lo que hay detrás', dirigida a promover la utilización del *Canal prioritario* de la Agencia, que fue declarada de servicio público por la CNMC. Para llevar a cabo la difusión de esta campaña se ha contado con el apoyo de las principales cadenas de televisión españolas, como Atresmedia, Mediaset y RTVE.

FUE CONDENADO A CINCO AÑOS DE CÁRCEL PORQUE GRABÓ a Sara sin permiso mientras mantenían relaciones sexuales, lo pasó por el grupo de amigos, que le animaron a subirlo a internet Y DIFUNDIÓ EL VÍDEO

No es por el vídeo, es por todo lo que hay detrás

Si te llega un contenido violento o sexual sin permiso de la víctima, denúncialo en Canal Prioritario.  
[aepd.es/canalprioritario](http://aepd.es/canalprioritario)

Logo de AEPD (Agencia Española de Protección de Datos) y CNMC (Comisión Nacional de los Mercados y la Competencia).

El Canal tiene como objetivo limitar la difusión y el acceso a contenidos sexuales o violentos publicados sin el permiso de las personas que aparecen en ellos, en particular, en casos de acoso a menores o violencia sexual contra las mujeres. El acto fue inaugurado por la presidenta del Senado, y se dirigió fundamentalmente a entidades que pudieran contribuir a la difusión de esta iniciativa,

como ONG de mujeres supervivientes a la violencia de género digital y menores; organismos públicos relevantes implicados en la protección de datos y la seguridad y organizaciones empresariales y sindicales, entre otros.

#### ■ Entrega de los Premios Protección de Datos 28 de enero

La Agencia entregó durante el acto en el Senado los 'Premios Protección de Datos 2019' en las categorías de Comunicación; Adaptación al Reglamento; Buenas prácticas en centros escolares; Investigación; Emprendimiento 'Ángela Ruiz Robles' y Buenas prácticas de protección en internet de la privacidad de las mujeres supervivientes a la violencia 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.

#### ■ Jornadas sobre Teletrabajo 24 y 26 de junio

La AEPD celebró dos jornadas en las que abordó desde una perspectiva práctica cómo el teletrabajo contribuye al fomento de la conciliación y la productividad, analizando también los retos que se presentan para su expansión en las administraciones y empresas españolas.

El día 24 de junio, las jornadas de debate contaron con representantes del Ministerio de Igualdad, el Ministerio de Política Territorial, la Organización para la Cooperación y el Desarrollo Económicos (OCDE), CEOE, CEPYME, Women in a Legal World, UGT, CCOO, CSIF y el Ministerio de Trabajo y Economía Social. La mesa del sector público estará moderada por la Agencia y la del sector empresarial por ADireLab.

El día 26 de junio estuvo dedicado a conocer experiencias prácticas de teletrabajo, ya en marcha, y los resultados obtenidos por parte de la AEPD, la Generalitat Valenciana, Zurich Seguros y Software del Sol. Los vídeos de la jornada de teletrabajo pueden *consultarse aquí*.



## ■ Seminario de la UIMP sobre la protección de datos personales en el marco de la epidemia COVID-19'

2, 3 y 4 de septiembre

La Agencia impartió del 2 al 4 de septiembre el seminario 'La protección de datos personales en el marco de la epidemia COVID-19', enmarcado en las Actividades de Verano 2020 de la Universidad Internacional Menéndez Pelayo (UIMP) de Santander, donde se analizó la incidencia de la COVID-19 desde la perspectiva de la protección de datos, tanto desde el punto de vista del marco jurídico de los tratamientos de datos personales asociados al contexto de la pandemia en lo que respecta a los criterios de necesidad y proporcionalidad, como la legitimación para realizarlos y la posición de los actores que intervienen en ellos, tanto públicos como privados.

### **Comunicación específica relacionada con la situación derivada de la expansión de la COVID-19**

La Agencia trabajó de forma intensa en las semanas posteriores a la aplicación del estado de alarma para establecer criterios prácticos que permitieran conciliar las necesidades sanitarias con el derecho fundamental a la protección de datos. El grueso de estos criterios se hizo público en la página web de la Agencia ([www.aepd.es](http://www.aepd.es)), creando una sección específica llamada *Protección de datos y coronavirus* para que tanto ciudadanos como responsables pudieran estar informados de los criterios y recomendaciones de esta Agencia.

El 12 de marzo se publicó *un informe* en el que la AEPD analizaba el tratamiento de datos personales en relación con la situación derivada de la extensión de la COVID-19. Ese mismo día se envió a todos los medios de comunicación *una nota de prensa* en la que se resumían y simplificaban los aspectos más destacados del mismo. Ese mismo día, la Agencia tuvo conocimiento a través de diversas informaciones de que estaban proliferando los ataques de phishing relacionados con el coronavirus, por lo que procedió a publicar con celeridad en su blog *un artículo en que alertaba a los ciudadanos de ataques de phishing* a través de servicios de mensajería instantánea, email y otros medios.

Tras constatar que estaban proliferando páginas web y aplicaciones móviles que ofrecían servicios para autoevaluar y aconsejar en relación con el Coronavirus por parte de entidades privadas, la Agencia lanzó un *comunicado en el que advertía al conjunto de la ciudadanía de los riesgos que implica facilitar categorías de datos sensibles*, como son los relativos a la salud, a estas webs y apps privadas que no aportaban en algunos casos la información exigible para identificar a los responsables, ni incluían las finalidades para las que podrían tratarse los datos.

Poco después, a modo de resumen de los diversos contactos y la colaboración desarrollada con las autoridades competentes, la Agencia hizo público *otro comunicado* en el que sintetizaba el contenido de los informes publicados sobre esta temática.

En abril, ante las consultas recibidas a través de diferentes vías sobre si el Real Decreto 463/2020 de declaración del estado de alarma (que interrumpía plazos para la tramitación de los procedimientos de las entidades del sector público) afectaba a la notificación obligatoria de las quiebras de seguridad ante la Agencia según lo que establece el RGPD, la Agencia *publicó y dio difusión a un post en su blog* aclarando este concepto. En él se clarificaba que los responsables y encargados de tratamiento debían seguir cumpliendo con sus obligaciones si sufrieran una brecha de seguridad de los datos personales que constituya un riesgo para los derechos y libertades de las personas físicas. Durante ese mismo mes, para apoyar al tejido empresarial español, la Agencia publicó *un documento con las cinco medidas técnicas de seguridad* que juegan un papel relevante en los tratamientos de datos personales para cumplir con las obligaciones de responsabilidad proactiva establecidas en el RGPD. Además, se publicó en el blog de la Agencia *un documento con recomendaciones generales* para el tratamiento de datos en situaciones de emergencia.

Posteriormente, a la vista de las iniciativas para la implantación de medidas encaminadas a prevenir contagios en las medidas de desescalada del confinamiento, la Agencia hizo público un *comunicado sobre la toma de temperatura* por parte de comercios, centros de trabajo y otros establecimientos.

Por otra parte, la Agencia Española de Protección de Datos, ante las consultas que venía recibiendo y dando respuesta a través de sus canales de atención al ciudadano y a las empresas y otros sujetos obligados al cumplimiento de la normativa de protección de datos, elaboró y publicó a través de su web una serie de Preguntas Frecuentes y sus respuestas (FAQ) con el objetivo de hacer más accesible la información sobre los criterios para el tratamiento de datos de salud en el ámbito laboral.

La Agencia también hizo público un *comunicado sobre la información acerca de tener anticuerpos de la COVID-19 para la oferta y búsqueda de empleo*, recogiendo información sobre que se estaba solicitando a los candidatos a un puesto de trabajo información de si han pasado la COVID-19 y desarrollado anticuerpos como requisito para acceder al puesto de trabajo ofertado y advirtiendo de que estas prácticas constituyen una vulneración de la normativa de protección de datos aplicable.

En cuanto a la *recogida de datos personales por parte de los establecimientos*, la Agencia también publicó un comunicado a finales de julio en el que destacaba que los ciudadanos deben recibir una información clara, sencilla y accesible sobre el tratamiento que se va a realizar antes de la recogida de los datos personales y que, en todo caso, la información se debe tratar con las medidas de seguridad adecuadas.

#### ▲ 5.6.2. Campañas de difusión

##### ■ ‘Por todo lo que hay detrás – Canal prioritario’

La campaña ‘Por todo lo que hay detrás’ se inició el 28 de enero, coincidiendo con la celebración del Día Internacional de la Protección de Datos. Compuesta por tres vídeos y tres carteles (“*Fue condenado a cinco años de cárcel porque...*”, “*Fue acosado en el instituto porque...*” y “*Se suicidó porque...*”), recoge situaciones extremas pero reales en las que se muestra en primer término el desenlace para detallar a continuación cómo se ha llegado a esa situación y las consecuencias que puede acarrear esa difusión.

A pesar de las ventajas que proporcionan las nuevas tecnologías y los servicios que estas ofrecen, en ocasiones se utilizan como vía para extender formas de violencia que fomentan la humillación pública de las personas, dañando de forma grave su privacidad. La campaña ‘Por todo lo que hay detrás’ trata de mostrar la historia que puede haber tras un simple reenvío para evidenciar las graves consecuencias de que se difundan imágenes, vídeos o audios sensibles en internet. Los destinatarios de la campaña, que promueve la denuncia de este tipo de contenidos, no son únicamente las personas que en algún momento puedan resultar afectadas por la difusión sino también a todos aquellos que son conocedores de la situación -y que también tienen la posibilidad de denunciarlo ante la Agencia- y a aquellos que, de manera irreflexiva o por desconocimiento, contribuyen a la difusión en Internet de estos contenidos, pudiendo incurrir en no sólo en responsabilidad *administrativa sino también disciplinaria, civil y penal*.

Para llevar a cabo la difusión de esta campaña se contó, entre otros, con el apoyo de entidades como Atresmedia, Mediaset y RTVE, Fundación Mutua Madrileña, Fundación ANAR, FAD, EMT y Metro de Madrid, Más móvil, Clear Channel o Google. Como ejemplos del importante impacto que ha tenido esta campaña se pueden citar los siguientes: la emisión del spot en televisión (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) por parte de las tres principales cadenas de televisión de ámbito nacional ha obtenido más de 50 millones de impactos. Asimismo, en cuanto a la difusión realizada en medios de transporte, la Empresa Municipal de Transportes (EMT Madrid) cedió gratuitamente durante 15 días el espacio de sus pantallas en 212 líneas, con un alcance potencial de un millón y medio de viajeros de media diaria. Asimismo, el Ayuntamiento de Santander también cedió gratuitamente el espacio digital de sus autobuses para la emisión de la campaña. En cuanto a Metro de Madrid, además de dos vídeos emitidos por el Canal Metro, se colocaron de forma gratuita en su circuito de transporte 258 carteles impresos en soportes de 70 x 100 cms.



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

Asimismo, desde el día 29 de enero la campaña en redes sociales fue muy intensa, poniéndose en marcha un reto en Instagram y Twitter en el que se animaba a actuar de manera directa contra la publicación sin consentimiento de contenido sensible -no compartiéndolo y denunciándolo en el Canal prioritario- bajo el hashtag #PuedesPararlo. Empresas, organismos, administraciones y personajes públicos se sumaron a la campaña retuiteando las publicaciones de la AEPD y en algunos casos realizando publicaciones propias que ayudaron a incrementar el impacto y difusión de la campaña en Twitter. Algunos de los organismos que realizaron difusión de la campaña fueron @desdelamoncloa, @GDTGuardiaCivil, @minecogob, @educaciongob, @educalNTEF, @InjuveSpain o @060gobes, entre otros.

La campaña también contó con la participación de colaboradores externos como RoEnLaRed, Rush Smith, Chris Pueyo, Marina Jade y Gominuke, que consiguieron más de un millón de impresiones de la campaña. La escritora Elvira Sastre, por su parte, realizó un hilo en Twitter en el que fomentaba la utilización del Canal prioritario, obteniendo más de un millón de impresiones adicionales.

## ■ Campaña de sensibilización para el sharenting responsable

La AEPD ha colaborado en 2020 con Pantallas Amigas en una campaña de sensibilización para el sharenting responsable. El objetivo de la campaña es concienciar sobre el uso de imágenes de menores de edad en internet, incidiendo sobre las cuestiones que los padres deben tener en cuenta antes de subir estos contenidos a la Red.

El término 'sharenting' se refiere a compartir imágenes online de hijos e hijas menores de edad por parte de sus padres. La campaña pone de relieve que en estos meses de reclusión debido a la pandemia ha proliferado la práctica de compartir imágenes familiares de menores de edad, acelerada por el contexto que ponía en las tecnologías ligadas a internet gran parte de las posibilidades para el ocio, el estudio, el trabajo o las relaciones personales.

Debido a esta situación, PantallasAmigas, con la colaboración de la Agencia Española de Protección de Datos, ha querido poner el foco en que se trata de una práctica no exenta de riesgos y que debe ser considerada y meditada con calma. El sharenting puede tener asociadas consecuencias negativas asociadas y por ello se debe realizar de manera responsable, valorando los pros y contras potenciales en cada ocasión.



## ■ Campaña ‘El control es tuyo, que no te controlen’

La campaña ‘*El control es tuyo, que no te controlen*’ es fruto de la colaboración entre la AEPD, el Ministerio de Educación y Formación Profesional, el Ministerio de Igualdad y PantallasAmigas, que pusieron en marcha esta campaña con el objetivo de ayudar a menores y adolescentes a detectar el acoso y la violencia de género digital. La campaña incluye mensajes que describen situaciones que los y las jóvenes pueden vivir en su centro de estudios, con su grupo de amistades o en sus relaciones personales. La petición de contraseñas a la pareja; el control del móvil de otra persona; el envío constante de mensajes con el propósito de herir a un compañero o una compañera de clase, o la difusión de imágenes sexuales, violentas o humillantes sin el permiso de quien aparece en ellas son algunas de estas situaciones.

EL CONTROL ES TUYO,  
QUE NO  
TE CONTROLLEN

#NOalAcosoDigital #ControlNoEsAmor

Logo de AEPD, España, Ministerio de Educación y Formación Profesional, Ministerio de Igualdad y PantallasAmigas.

‘*Tu vida está en tu móvil*’, ‘*Tu móvil hace cosas raras*’, ‘*Te están acosando, pide ayuda*’ y ‘*Han compartido imágenes comprometidas sin tu consentimiento*’ son los principales escenarios descritos, que se acompañan con recomendaciones y un código QR que enlaza a una página en la que se puede obtener más información sobre cómo identificar conductas violentas y actuar tanto si se es la persona a la que le está sucediendo como si se tiene conocimiento de ello. Los dispositivos móviles inteligentes, las redes sociales e internet

han transformado en gran medida la manera en que se relaciona la juventud. El 22% de los chicos y chicas de 10 años dispone de teléfono móvil, porcentaje que asciende exponencialmente hasta casi el 94% a los 15 años, según datos de 2019 del INE.

La Macroencuesta de Violencia contra la Mujer de 2019 del Ministerio de Igualdad revela, entre otras conclusiones, que un 18,5% de las mujeres de 16 o más años residentes en España han sufrido acoso sexual antes de cumplir los 15 años (conductas entre las que se incluye el envío de imágenes o fotos sexualmente explícitas que hayan hecho sentirse ofendida, humillada o intimidada a la mujer).

Entre los elementos gráficos de la campaña se encuentra un *cartel que reúne todas las situaciones descritas* y las recomendaciones enlazan a contenidos en los que pueden identificarse *formas de violencia de género digital* que no siempre son identificadas de ese modo por las y los jóvenes, *cómo detectar si el teléfono móvil puede estar siendo espiado* y recomendaciones a seguir, *indicios para detectar la violencia de género*, entre los que se encuentra que la pareja revisa el teléfono móvil y las redes sociales o *qué hacer si se están difundiendo imágenes de contenido sexual o violento sin el consentimiento de la persona que aparece en ellas*.

TU MÓVIL HACE  
COSAS RARAS

Disminuye la autonomía de forma repentina, se calienta cuando no lo utilizas, empeora la calidad del sonido en las llamadas...

**ALGUIEN PUEDE ESTAR ACCEDIENDO A TU TELÉFONO**

**Revisa la configuración de tus redes y aplicaciones**

#NOalAcosoDigital #ControlNoEsAmor

Logo de AEPD, España, Ministerio de Educación y Formación Profesional, Ministerio de Igualdad y PantallasAmigas.

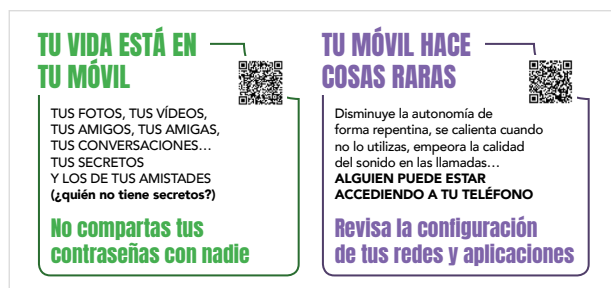


La campaña incluye los siguientes elementos offline y online:

- Un post en el blog de la Agencia a modo de *landing page de la campaña*



- Un cartel con 4 mensajes con códigos QR que enlazaban a información en diferentes páginas de las entidades participantes.



- Adaptación del cartel y sus mensajes para Twitter, Facebook e Instagram, en formato imagen, gif y vídeo.

Las entidades participantes realizaron diferentes acciones en sus redes sociales y páginas web, así como otras acciones con el material offline.

### 5.6.3. Premios

#### Premios concedidos por la AEPD

La Agencia entregó el 28 de enero de 2020 durante la presentación en el Senado de su campaña 'Por todo lo que hay detrás' los 'Premios Protección de Datos 2019' en las categorías de Comunicación; Adaptación al Reglamento; Buenas prácticas en centros escolares; Investigación; Emprendimiento 'Ángela Ruiz Robles' y Buenas prácticas de protección en internet de la privacidad de las mujeres supervivientes a la violencia 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.

En la categoría de Comunicación, la Agencia Española de Protección de Datos ha entregado el premio principal a la periodista Sofía Olmos, de la agencia de noticias Europa Press, por sus noticias publicadas sobre el uso responsable de las TIC y otras en las que se hace eco del incremento de la concienciación entre los ciudadanos, empresas y administraciones acerca de la importancia de la protección de los datos, entre otras.

Respecto al Premio a las 'Buenas prácticas en privacidad y protección de datos personales sobre iniciativas para adaptarse al Reglamento europeo de Protección de Datos', en la modalidad de empresas, asociaciones y fundaciones, el jurado ha concedido el premio, ex aequo, a la Asociación Proderechos Humanos de España, por su trabajo 'El Tribunal Constitucional subraya que la opinión es un dato especialmente protegido', sobre el recurso de inconstitucionalidad promovido por la Asociación contra la Disposición final tercera de la LOPDGDD, así como a Borja Adsuara, José Luis Piñar, Jorge García, Elena Gil, Víctor Domingo, Miguel Pérez Subías, Virginia Pérez Alonso, Rodolfo Tesone, por su trabajo 'Recurso de inconstitucionalidad contra la Disposición final tercera, apartado dos de la LOPDGDD', que comprende un conjunto de artículos en prensa y una campaña en redes sociales durante la tramitación del Proyecto de LOPDGDD en el Senado, así como el citado recurso de inconstitucionalidad, una vez aprobada la Ley.



En el apartado de entidades del sector público, se ha otorgado el premio al Ministerio de Trabajo, Migraciones y Seguridad Social, por 'ASSI-RGPD: aplicación web para el cumplimiento de los responsables de tratamiento de datos personales con el RGPD', una aplicación para salvaguardar los derechos y libertades de las personas y para que los responsables cumplan con el RGPD y la LOPDGDD.

En la categoría 'Premio a las 'Buenas prácticas educativas en privacidad y protección de datos personales para un uso seguro de internet', el jurado ha concedido el premio en la modalidad dirigida a centros de enseñanza de Educación Primaria, ESO, Bachillerato y Formación Profesional, al IES Rafael Alberti, de Cádiz, por 'El Ciberespacio: amenazas y oportunidades', un proyecto destinado al alumnado de edades comprendidas entre 12 y 18 años que combina medidas de prevención con un proceso educativo que implica a todos los agentes relacionados con el menor.

En la modalidad que reconoce el impulso y la difusión entre los menores de edad de buenas prácticas para un uso seguro de internet, el jurado ha otorgado el premio al Colexio Profesional de Enxeñaría en Informática de Galicia, por su trabajo 'Estrategia de sensibilización y formación del CPEIG para un uso seguro de Internet por parte de los/as menores de Galicia', una iniciativa encaminada a concienciar al alumnado desarrollando programas en los propios centros escolares y a través de progenitores y profesorado mediante formación impartida por personas colegiadas.

En la categoría de 'Investigación en protección de datos personales Emilio Aced' el jurado ha otorgado el premio principal a Julien Armand Pierre Gamba, Mohammed Rashed, Abbas Razaghpanah, Juan Tapiador y Narseo Vallina-Rodríguez (IMDEA Networks Institute, Universidad Carlos III de Madrid, Stony Brook University, ICSI) por su trabajo 'Un análisis de software de Android preinstalado'. Asimismo, ha concedido el accésit a Mikel Recuero (Subdirección General de Evaluación y el Fondo Europeo de Desarrollo Regional) por su trabajo 'La investigación científica con datos personales genéticos y datos relativos a la salud: perspectiva europea ante el desafío globalizado', que realiza un análisis del actual marco jurídico europeo de protección de datos en relación con la puesta en marcha de proyectos y consorcios paneuropeos e internacionales de investigación que requieran la recogida, explotación y reutilización de grandes cantidades de datos genéticos y datos de salud.

En relación con la nueva categoría de 'Emprendimiento en protección de datos personales Ángela Ruiz Robles', el jurado ha premiado el trabajo de Armando Molina (Molinapps SLU), 'Datos de salud en dispositivos móviles y seguridad jurídica: la solución DocToDoctor para médicos', destacando la incorporación de elementos innovadores desde el punto de vista de la privacidad desde el diseño y la alineación del proyecto con la Agenda 2030.

Finalmente, respecto a 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 supervivientes a la violencia de género, el jurado ha premiado a la Fundación Mutua Madrileña, por su 'Programa integral de prevención y protección de la privacidad de las mujeres víctimas de violencia de género', que contempla diversas iniciativas centradas en la sensibilización y protección de la intimidad de las personas en el entorno digital, que van desde la creación de campañas dirigidas a jóvenes a jornadas divulgativas con la ayuda de profesionales de la magistratura y expertos en protección de datos.

Además, ha otorgado un accésit al Ayuntamiento de Bigastro (Alicante), por su guía técnica 'El juego como recurso didáctico para prevenir situaciones de violencia por razón de género en la red'. El trabajo, elaborado desde la Concejalía de Servicios Sociales, Igualdad y Políticas Inclusivas, se centra en la sensibilización y prevención de las distintas formas de violencia por razón de género en el entorno de internet, y específicamente en la violencia de control tanto para población adolescente como de personas adultas.

### Premios recibidos por la AEPD

#### ■ Premio a la Mejor campaña institucional de la AUI – Por todo lo que hay detrás

La campaña 'Por todo lo que hay detrás' de la Agencia Española de Protección recibió el Premio de la Asociación de Usuarios de Internet (AUI) a la mejor campaña institucional de publicidad online. El objetivo de estos premios es reconocer aquellas iniciativas, personas u organizaciones que más se han destacado, durante el año previo a su entrega, en promover, innovar o facilitar los usos de internet y de las nuevas tecnologías en sus respectivas categorías. La campaña 'Por todo lo que hay detrás' está dirigida a *promover la utilización del Canal prioritario de la Agencia* para denunciar la difusión en internet de contenidos sexuales o violentos publicados sin el permiso de las personas que aparecen en ellos, en particular, en casos de acoso a menores o violencia sexual contra las mujeres.

#### ■ '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 mujeres supervivientes a la 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.

### 5.7. Acceso a la información pública y Transparencia

El número de solicitudes de acceso a información pública se ha incrementado respecto de los años anteriores, junto a la complejidad de las mismas. La mayor parte de las peticiones se refieren a expedientes y resoluciones sancionadores. Por ejemplo, una solicitud destacable ha sido la formulada por la Fundación CIVIO, que demandó toda la información relativa a actuaciones sancionadoras conjuntas, realizadas con otros miembros del Comité Europeo de Protección de Datos sobre los grandes gigantes de las telecomunicaciones y redes sociales (Google, Facebook, Twitter y WhatsApp). Se observa, igualmente, que muchas peticiones de resoluciones de procedimientos sancionadores proceden de los propios denunciantes. Los denunciantes no son considerados como parte interesada en el procedimiento y la resolución final no les es notificada directamente, por eso acceden a ella a través del procedimiento de acceso a información pública. Otras solicitudes se refieren a ficheros de tratamientos archivados y a contratos públicos celebrados por la AEPD.

## ➤ 6. Ayuda efectiva para las entidades

### 6.1. Transformación del canal Informa\_RGPD a Canal DPD

La Agencia Española de Protección de Datos rediseñó en noviembre de 2020 su canal INFORMA\_RGPD, cambiando su denominación a *Canal\_DPD* con el objetivo de canalizar las consultas que plantean los Delegados de Protección de Datos a la Agencia y de potenciar la figura creada por el RGPD en el marco del principio de responsabilidad proactiva.

El Canal\_DPD da un servicio específico a los Delegados de Protección de Datos del sector público y privado, de designación obligatoria y voluntaria, y previamente comunicados a la Agencia. El número total de entidades que han comunicado su DPD a la AEPD en este momento supera los 63.000.

La AEPD presentó INFORMA\_RGPD en febrero de 2018, tres meses antes de la aplicación del Reglamento General de Protección de Datos (RGPD), para ayudar a responsables, encargados y DPDs con la adaptación al nuevo marco normativo.

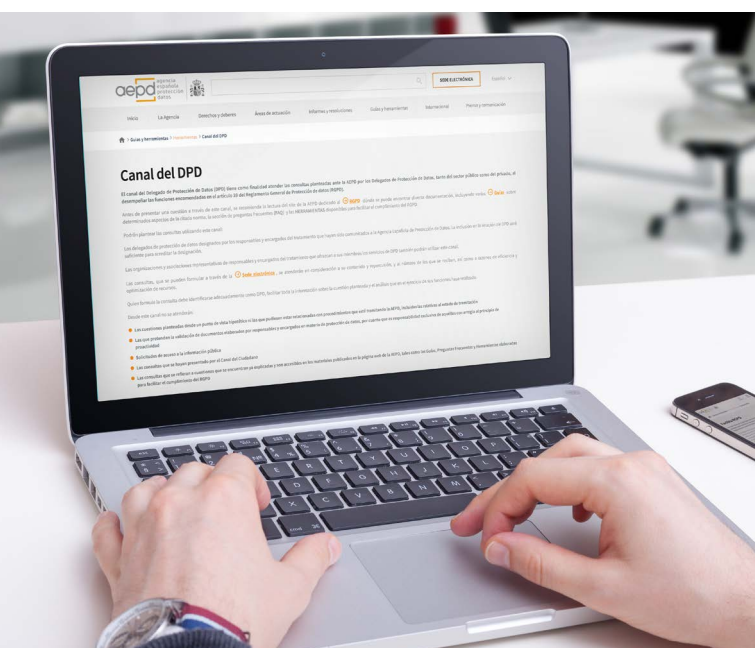
Tras más de dos años de la aplicación efectiva del Reglamento, el Canal INFORMA\_RGPD, con cerca de 7.000 consultas atendidas, dio por cumplido su objetivo de ayudar y facilitar las tareas de adaptación a la entonces novedosa regulación.

Durante este tiempo la Agencia ha ido presentando una amplia batería de servicios para facilitar la aplicación y el cumplimiento del RGPD. *Facilita\_RGPD*, *Facilita\_EMPRENDE*, *Gestiona\_EIPD*, *Comunica-Brecha*, además de *guías*, *directrices* y *orientaciones*, son algunas de las *herramientas* y *materiales* que están a disposición de responsables y encargados para dar soporte en aquellas dudas y cuestiones que puedan derivarse de la aplicación de la normativa.



#### Comunica-Brecha RGPD

Herramienta de ayuda a los responsables de tratamiento en la toma de decisiones ante la obligación de comunicar una brecha de seguridad de datos a los afectados



Asimismo, el artículo 39.1.e) del RGPD establece como funciones de los DPD el ser punto de contacto sobre tratamientos de datos con la autoridad de control y, a este efecto, faculta a los DPD para efectuar cualesquiera consultas a la autoridad de control. En consecuencia, el Canal DPD atiende exclusivamente las consultas que al amparo del artículo 39.1.e) pueden formular los DPD, así como para las cuestiones que plantee las asociaciones y organizaciones de categorías de responsables y encargados del tratamiento que ofrezcan a sus miembros servicios y asesoramiento propio de los DPD.

Los requisitos y condiciones de uso del Canal DPD se encuentran accesibles [en esta sección](#).

## 6.2. Inscripción de Delegados de Protección de Datos

La figura del DPD es una pieza clave del sistema que establece el RGPD, al que atribuye unas funciones y dota de una posición en la que se apoya su cumplimiento y a las que la LOPDGDD ha añadido una importante labor para la solución de reclamaciones.

Por ello se establece la obligación de su designación atendiendo a las cualidades profesionales, en particular los conocimientos especializados en el derecho y la práctica de la protección de datos, y de comunicar a las autoridades de control los DPD designados para darles publicidad por parte de éstas.

El número total de responsables que han comunicado la designación de DPD y sus datos de contacto a la Agencia Española de Protección de Datos en cumplimiento de lo estipulado en el artículo 37.7 del RGPD y 34.3 de la LOPDDGG es de 65.040 a 31 de diciembre de 2020, lo que supone un incremento de un 29% en el número total de entidades que han comunicado los datos de contacto de su DPD en relación con la misma fecha del año anterior.

El número total de DPD comunicados por la Administración General del Estado, las Comunidades Autónomas y la Administración Local es de 3.883 experimentando un incremento de un 25% con respecto a la misma fecha del año pasado.

Sigue preocupando el dato relativo a la Administración Local, donde solamente 3.334 Diputaciones, Ayuntamientos, así como entidades locales y los organismos asociados a todos ellos, han procedido a la comunicación de su DPD puesto que, aun suponiendo un incremento de un 25% con respecto a la misma fecha del año anterior, sigue estando muy lejos del total de responsables que componen la administración local en España y que deben contar con un DPD.

## 6.3. Certificación de DPD conforme al Esquema AEPD – DPD

El compromiso con la figura del DPD mediante la creación de un Canal de comunicación con la Agencia específico para ellos, a través de contactos con DPD sectoriales o para impulsar su formación tiene uno de sus componentes en el Esquema de la Agencia para certificar DPD. La voluntad de proporcionar seguridad a los responsables y encargados que han de designar un DPD impulsó la adopción del Esquema 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 última, y una de la de más envergadura, la llevada a cabo el 10 de enero, con la adopción de la versión 1.4 del Esquema, cuyas novedades más destacables fueron:

- ▶ La eliminación de la designación de entidades de certificación provisionales, posibilidad que obedecía a la necesidad de disponer de un marco que permitiera optar a la obtención de la certificación de DPD mientras se tramitaba el proceso de acreditación por ENAC. Al contarse ya con un número de entidades de certificación definitivamente acreditadas por ENAC carecía de fundamento mantener un sistema provisional, pues los candidatos ya podían acceder a entidades acreditadas y evitar las situaciones de provisionalidad e incertidumbre de si finalmente fuera acreditada la entidad provisional y se validarían los certificados obtenidos.
- ▶ La introducción de un código ético de aplicación a las entidades de certificación y de formación, que expresa los valores, principios y pautas de comportamiento responsable, basados en la normativa aplicable y en los requisitos del Esquema, que deben observar en el desarrollo de sus actividades con la finalidad de dotar al esquema de rigor y consistencia.



- Se modificó la Marca del Esquema y se introdujo un contrato para su uso, cuyo mantenimiento se hace depender, entre otros factores, de la observancia del código ético, pues en caso, contrario puede justificar su resolución y, en consecuencia, la imposibilidad de continuar prestando servicios como actor en el Esquema.

Para facilitar la adecuación a la nueva versión, tanto de entidades de certificación como de formación, se incluyó la correspondiente disposición transitoria.

En cuanto al desarrollo del Esquema, durante el año 2020 finalizó el proceso de acreditación de una nueva entidad de certificación Bureau Veritas Iberia S.L., con la que ya son siete las entidades de certificación, constatándose una cierta estabilización en cuanto a su número.

También la pandemia y sus consecuencias ha afectado a los procesos de certificación, suspendiéndose la celebración de varias pruebas que se reanudaron una vez que las condiciones lo permitieron, por lo que se está explorando la viabilidad de poderse realizar las pruebas online tanto para situaciones como la ocasionada por la pandemia como de cara al futuro. No obstante, es constante el seguimiento de las disposiciones y criterios que se adoptan en protección de datos y la revisión y actualización de las preguntas de las pruebas para obtener la certificación.

El número de exámenes que se prepararon durante 2020 fue de 61, que contaron con 536 candidatos, de los que se han certificado 200, con lo que a finales de año el número de DPD certificados con arreglo al esquema era de 614.

También se han llevado a cabo 9 procesos de auditoría de cumplimiento del Esquema, 7 de ellos de examen de adaptación a la nueva versión 1.4 del Esquema, y 2 auditorías de seguimiento. Auditorías que también se vieron afectadas por las restricciones que impuso la COVID-19.

## 6.4. Códigos de Conducta

En desarrollo de la regulación que de los códigos de conducta establece el RGPD, en concreto su artículo 43.1, el 27 de febrero se hicieron públicos los criterios de acreditación de los organismos de supervisión de los códigos de conducta que han de designar los promotores para poder ser acreditados por la Agencia Española de Protección de Datos. Publicación de la que se informó a los promotores de los códigos tipo inscritos el Registro General de Protección de Datos con la normativa anterior al Reglamento europeo, y de la necesidad de adecuar los organismos de supervisión previstos en sus proyectos de adaptación a la nueva normativa a dichos criterios.

A estos promotores también se les requirió para que aportaran nuevas versiones de sus proyectos de adaptación a los códigos de conducta que regula el RGPD ajustadas a estas condiciones. Las actuaciones realizadas durante 2020 en relación con los diferentes proyectos que de códigos de conducta que se fueron presentando determinaron:

- **a)** La cancelación de los antiguos códigos tipo que no optaron por adecuarlos al RGPD, conforme establece la Disposición transitoria segunda de la LOPDGDD:
  - Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF)
  - Consejo Gral. de Colegios de Odontólogos y Estomatólogos de España
  - Colegio de Farmacéuticos de la provincia de Barcelona
  - Federación Nacional de Clínicas Privadas
  - Asociación Empresarial de Gestión Inmobiliaria
- **b)** La inadmisión de los siguientes proyectos por no reunir los requisitos de admisibilidad que establecen las Directrices 1/2019
  - Business Adapter
  - Consejo Andaluz de Colegios de Administradores de Fincas



- c) La aprobación, el 9 de octubre, del “Código de conducta de tratamiento de datos en la actividad publicitaria”, cuyo promotor es la ASOCIACIÓN PARA LA AUTORREGULACIÓN DE LA COMUNICACIÓN COMERCIAL “AUTO-CONTROL”, y se acreditó como organismo de supervisión del código al Jurado de la Publicidad. La principal característica de este código es que incorpora un sistema de resolución extrajudicial de controversias en protección de datos que se susciten en el ámbito de la publicidad.

Para los códigos de conducta aprobados por la Agencia se procedió a crear un nuevo espacio, o registro de los códigos de conducta *en la web de la AEPD*.

Durante este año se han mantenido reuniones con los promotores de códigos de conducta cuyos proyectos se encuentra 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, que ha supuesto el estudio y valoración de los proyectos presentados y efectuar las recomendaciones y sugerencias de mejora.

La experiencia de los proyectos recibidos y de las reuniones mantenidas con los promotores es que hay que concienciarles de que los requisitos de los códigos de conducta no responden a los de los antiguos códigos tipo. El RGPD aporta una mayor flexibilidad en cuanto a su contenido, pero éste ha de satisfacer una necesidad específica del sector o actividad de tratamiento y debe aportar un valor añadido a la regulación de obligado cumplimiento.

En el marco europeo se ha colaborado en la revisión de los Criterios de Acreditación de los Organismos de Supervisión de los Códigos de Conductas elaborados por Alemania, Irlanda y Finlandia, para la emisión del correspondiente dictamen por el CEPD; y en la valoración de los códigos de conducta de carácter transnacional por afectar a tratamientos de datos en diversos Estados miembros de CISPE y EUCLLOUD.

## 6.5. Promoción de la formación y sensibilización. Sesiones formativas

Se ha continuado con la labor de formación y sensibilización a través de sesiones y jornadas online, pues la COVID-19 supuso la anulación de las actividades formativas presenciales. Los organismos e instituciones que fueron destinatarias de estas acciones fueron:

- Ministerio de Educación y Formación Profesional
- Ministerio de Transportes, Movilidad y Agenda Urbana
- Ministerio de Justicia
- Ministerio de Política Territorial y Función Pública
- Ministerio de Derechos Sociales y Agenda 2030
- Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática
- Dirección General de Seguros y Fondos de Pensiones
- Delegación del Gobierno en Extremadura
- Agencia Española del Medicamento y Productos Sanitarios
- Diputación Provincial de Huesca
- INAP
- Jornada sobre “La transparencia y la protección de datos: una perspectiva local”, organizada por el INAP

En este ámbito destaca el esfuerzo que ha supuesto adaptar los cursos que se estaban impartiendo al importante cambio que se ha producido en el INAP durante el año 2020 en cuanto a la gestión y reorganización de los cursos que se programan e imparten anualmente para el personal al servicio de la Administración Pública. Por una parte, se diseñó un nuevo programa y se elaboró su contenido para el curso básico dirigido con carácter general a los empleados públicos

que se imparte de manera abierta con un mayor número de alumnos, e impartida la primera edición, y, por otra, se presentó el modelo de curso dirigido a los empleados públicos que fueran DPD en el sector público o formaran parte de sus equipos, o aspiraran a serlo, integrando en una sola acción formativa los dos cursos que se ofertaban en ediciones anteriores. Finalmente, la primera convocatoria de este último curso se programó para el 2021.

Así mismo, en la esfera interna de la Agencia se han celebrado sesiones formativas prácticas sobre determinadas materias e impulsado la organización de un curso de formación entre los empleados de la AEPD, cuya dirección y seguimiento está a cargo del DPD de la Agencia en desarrollo de sus funciones, y elaborado un paquete de contenidos para formar a los nuevos empleados que se incorporen a la Agencia.

## 6.6. Protocolos de actuación e instrumentos de colaboración

En otros ámbitos se ha trabajado en forjar alianzas y reforzar la colaboración con algunas de las instituciones y entidades con las que se comparten objetivos:

- Protocolo General de Actuación con Unión Española de Entidades Aseguradoras y Reaseguradoras (UNESPA) firmado el 22 de enero.
- Protocolo General de Actuación con la Fundación ANAR firmado el 21 de febrero.
- Protocolo General de Actuación con la Fundación Mutua Madrileña firmado el 21 de febrero.
- Protocolo General de Actuación con la Asociación Española de Fundaciones firmado el 14 de julio.
- Protocolo General de Actuación con el Instituto Andaluz de la Mujer, en materia de atención a las personas cuyos datos se

hayan obtenido y difundido ilegítimamente, especialmente en caso de imágenes, vídeos, o audios con datos sensibles, firmado el 7 de septiembre.

## 6.7. Transferencias internacionales

En el ámbito de las transferencias internacionales de datos, la sentencia de 16 de julio del Tribunal de Justicia de la Unión Europea (Schrems II), que invalidó la Decisión de la Comisión Europea 2016/1250 sobre el “Escudo de la privacidad” (Privacy Shield), para los flujos de datos con destino a los Estados Unidos, y mantuvo la validez de la Decisión 2010/87 sobre las cláusulas contractuales estándar (SCC por sus siglas en inglés) para las transferencias de datos a encargados del tratamiento establecidos en terceros países, ha constituido uno de los acontecimientos más relevantes del año en materia de protección de datos, pues a partir de dicha fecha las transferencias de datos a Estados Unidos no se pueden realizar al amparo de la Decisión de Adecuación que suponía el Escudo de la Privacidad.

El planteamiento inicial de la cuestión prejudicial planteada por el Tribunal Superior de Irlanda preguntaba por la validez de las SCC de la Decisión 2010/87, sobre las que el Tribunal sostiene su validez, que no queda puesta en entredicho por el mero hecho de que, debido a su carácter contractual, las SCC no vinculen a las autoridades del país tercero al que se transfieran los datos, pues la referida Decisión incluye mecanismos efectivos que permiten garantizar en la práctica que el nivel de protección exigido por el Derecho de la UE sea respetado y que las transferencias de datos personales basadas en las SCC sean suspendidas o prohibidas en caso de que se incumplan o de que resulte imposible cumplirlas.

El TJUE examinó asimismo la validez de la Decisión Escudo de la privacidad para las transferencias de datos a Estados Unidos, dado que el litigio nacional que dio lugar a la cuestión prejudicial obedeció al flujo de datos entre la UE y los Estados Unidos.

La Corte determinó que el Escudo de la Privacidad es incompatible con el artículo 45 del RGPD a la luz de los artículos 7, 8 y 47 de la Carta Europea de Derechos Fundamentales por cuanto:

- En primer lugar, reconoce, al igual que su precedente del Puerto Seguro, la primacía de las exigencias relativas a la seguridad nacional, el interés público y el cumplimiento de la ley estadounidense. Las limitaciones de la protección de datos personales que se derivan de la normativa interna de los Estados Unidos relativa al acceso y la utilización por sus autoridades de los datos transferidos desde la UE no están reguladas conforme a exigencias sustancialmente equivalentes a las requeridas por el principio de proporcionalidad en la UE, dado que los programas de vigilancia basados en la mencionada normativa no se limitan a lo estrictamente necesario.

Los programas de vigilancia, acceso a la información y a los datos personales por motivos de seguridad nacional de manera masiva sin determinar prescriptores o criterios, ni limitaciones, al que por Ley están obligados los destinatarios de los datos por vía electrónica, no incluyen limitaciones a la habilitación que otorga para la ejecución de esos programas lo que posibilita las injerencias en los derechos fundamentales de las personas cuyos datos personales se transfieren a ese país tercero.

- Y, en segundo lugar, por la falta de garantías para las personas no nacionales de los Estados Unidos que sean potencialmente objeto de esos programas, sin que el mecanismo del Defensor del Pueblo contemplado en el Escudo de la Privacidad proporcione a esas personas ninguna vía de recurso ante un órgano que ofrezca garantías sustancialmente equivalentes a las exigidas en el Derecho de la Unión, que puedan asegurar tanto la independencia del Defensor del Pueblo como la existencia de normas que le faculten para adoptar decisiones vinculantes con respecto a los servicios de inteligencia estadounidenses. Carece de poderes ejecutivos para servir como vía de reparación.

Si bien las SCC continúan siendo válidas, el Tribunal subrayó la necesidad de que éstas proporcionen en la práctica un nivel de protección esencialmente equivalente al garantizado por el RGPD y destacó que corresponde al exportador, en colaboración en su caso con el importador, evaluar si el nivel de protección exigido por la legislación de la UE se respeta en el país tercero de que se trate para determinar si las garantías proporcionadas por las SCC pueden cumplirse en la práctica, y, en su caso, aportar garantías adicionales. Obligación que cabe extender al resto de instrumentos de transferencia recogidos en el artículo 46 del RGPD, como las normas corporativas vinculantes (BCR por sus siglas en inglés).

La sentencia ha ocasionado un intenso trabajo llevado a cabo el Comité Europeo de Protección de Datos con la finalidad de facilitar su aplicación y proporcionar a los responsables y encargados recomendaciones para atender lo establecido en la sentencia, que se recoge en el apartado correspondiente a la actividad internacional de la Agencia.

En cuanto a la actividad de la Agencia Española de Protección de Datos en esta materia, el 11 de marzo, la Agencia aprobó las primeras normas corporativas vinculantes (BCR, por sus siglas en inglés) al GRUPO FUJIKURA AUTOMOTIVE EUROPE (GRUPO FAE) en el marco del Reglamento general de protección de datos (RGPD), y unas de las primeras en el ámbito europeo. En la tramitación de estas BCR la Agencia actuó como autoridad líder y contó con el informe favorable del Comité Europeo de Protección de Datos.

El 15 de diciembre se aprobaron las normas corporativas vinculantes del GRUPO IBERDROLA en las que la Agencia también fue la autoridad líder para su tramitación e igualmente fueron favorablemente informadas por del Comité Europeo de Protección de Datos.

Al margen de estas dos aprobaciones, la Agencia está tramitando otras 12 BCR, de ellas 8 como autoridad líder y 4 como co-revisora.

## 7. La potestad de supervisión

### 7.1. Resultados

El año 2020 ha sido un año condicionado por la pandemia causada por el virus SARS-CoV-2. Por ello, resulta obligado hacer una mención a los cambios organizativos que hubo que implantar para responder a la crisis ocasionada por la COVID-19.

Por una parte, con el inicio del confinamiento generalizado se extendió el programa de teletrabajo, que existía con anterioridad, a la totalidad del personal de la Subdirección General de Inspección y a todos los días de la semana. En esto, hay una excepción que es la del personal que debía acudir a realizar tareas que exigían presencialidad -tales como el envío de notificaciones en papel o la descarga de archivos recibidos en soporte físico-, en las condiciones menos comprometidas, dentro de lo posible. Para la realización de estas tareas se establecieron turnos, de tal modo que acudía a la sede de la Agencia únicamente el personal imprescindible. La frecuencia de esos turnos fue variando a lo largo de los meses. Así, por ejemplo, a partir de junio, debido a la reanudación de los plazos en los procedimientos administrativos que habían quedado suspendidos durante los meses anteriores, fue necesario ampliar la frecuencia. Una vez se recobró el ritmo habitual, los turnos se acomodaron a la situación.

El análisis del volumen de la entrada, sin tener en cuenta las reclamaciones que llegan a través de otros países europeos, viene marcado por dos factores. En primer lugar, se ha producido una disminución en el número de reclamaciones recibidas -un 11% menos respecto al año anterior-, lo cual puede ponerse en relación con la situación de confinamiento que se ha vivido durante 2020, y con la suspensión generalizada de actividades de toda índole. Sin embargo, se han incrementado notablemente -en un 73%- las actuaciones realizadas por propia iniciativa de la Agencia. Este hecho es indicativo de la labor de supervisión permanente que se efectúa.

En otro orden de cosas, el RGPD extiende la obligación de notificar las brechas de seguridad de datos personales sufridas por las distintas entidades. Estas notificaciones, como se ha mencionado anteriormente en esta Memoria, son inicialmente recibidas por la División de Innovación Tecnológica. Tras un primer análisis, sólo algunas se remiten a la Subdirección General de la Inspección para que estudie si resulta pertinente iniciar actuaciones previas de investigación y continuar con los procedimientos establecidos o si por el contrario se pueden archivar.

También en este apartado se observa que la tónica respecto al año precedente se mantiene estable, puesto que si en 2019 fueron 79 las comunicaciones de brecha de seguridad de datos personales que se remitieron a la Subdirección para su estudio, en 2020 han sido 81.

Por otra parte, en el escenario europeo han continuado en funcionamiento los mecanismos de cooperación entre las autoridades de control de los Estados para la gestión de los casos transfronterizos. Con la aplicación efectiva del RGPD, los ciudadanos pueden presentar reclamaciones ante cualquier autoridad del Espacio Económico Europeo y las autoridades intercambiarán las reclamaciones recibidas para que sean atendidas adecuadamente. El sistema de información que soporta este intercambio es el IMI (Información del Mercado Interior).

Pues bien, a pesar de que la pandemia obligó a suspender las reuniones presenciales, se recurrió en mayor medida a los medios telemáticos y con ello pudo continuar el trabajo coordinado entre las autoridades de control. En suma, en el transcurso del tiempo desde el inicio de la aplicación del RGPD se ha adquirido mayor fluidez en los trámites que se realizan a través del sistema IMI.

En cuanto a las cifras de estas reclamaciones transfronterizas, se observa estabilidad, pues que en 2020 se ha recibido prácticamente el mismo número de reclamaciones procedentes de otras autoridades de control del EEE (tan sólo un 1%

menos respecto al año anterior). No obstante, debe destacarse que la complejidad de estas reclamaciones ha sido bastante más elevada que las que tenían las de ejercicios anteriores y el tiempo que ha llevado su resolución también.

Hay que señalar que durante el año 2020 se han gestionado casos que incluyen cuestiones novedosas en las que intervienen varias autoridades y presentan una gran variedad de interpretaciones, sobre todo teniendo en cuenta la diferente normativa local existente en los países del EEE.

Más allá de la temática de la reclamación, y volviendo otra vez a las reclamaciones presentadas ante la Agencia, se observa una tónica de estabilidad, con levísimo decrecimiento, en los porcentajes resultantes del análisis previo de las reclamaciones. Así, tras el análisis inicial se dictó resolución de inadmisión en el 56% de los casos (de conformidad con el artículo 65.2 de la LOPDGDD o por ser competencia de otras autoridades de control), frente al 52% de 2019. El 44% restante, por tanto, pasaron al trámite de traslado al responsable o, en su caso, a la apertura de actuaciones de investigación o de procedimiento.

Otro aspecto positivo del año 2020 fue la constatación de que el trámite de traslados se encuentra ya plenamente implantado. Su objeto es facilitar la resolución rápida de reclamaciones, de acuerdo con las previsiones del RGPD, según lo dispuesto en la LOPDGDD y con independencia de la actividad inspectora que siempre puede realizar la Agencia. Implica una ampliación de los días de tramitación de las reclamaciones asociada a la necesidad de remitirlas, con el fin de solicitar información al responsable del tratamiento de datos personales o a su DPD, esperar respuesta y evaluarla. Pero tiene como ventaja que, con esta fase de traslado, las reclamaciones pueden resolverse más rápidamente -en 2020, se resolvió el 77% de las reclamaciones después de haber procedido al traslado -, dato ligeramente inferior al obtenido durante 2019. Con esta fase se consiguen unos resultados satisfactorios para los reclamantes al ver solucionada su caso en un tiempo mucho más corto, sin menoscabo de la actividad de supervisión que siempre se puede realizar.

En la fase de traslado de la reclamación, prevista en el artículo 65.4 de la LOPDGDD, se han resuelto 2.157 reclamaciones como consecuencia de haberse obtenido, tras el traslado, una respuesta satisfactoria del responsable o del encargado del tratamiento, o de los Delegados de Protección de Datos designados por aquellos.

Cabe señalar que, de estas reclamaciones, 1.055 estaban relacionadas con el ejercicio de los derechos de protección de datos que quedaron atendidos tras el traslado de la reclamación, siendo en la mayoría de los casos subsanada la falta de respuesta inicial del responsable o del encargado ocasionada por un hecho puntual. En este punto procede destacar, por su novedad, que en 4 ocasiones se había ejercido el derecho a la limitación del tratamiento, reconocido en el artículo 18 del RGPD, y en otras 4, el derecho de portabilidad de los datos regulado en el artículo 20 del RGPD. Asimismo, merece ser mencionado que 130 reclamaciones se referían a la falta de atención del ejercicio del derecho al olvido proclamado en los artículos 93 y 94 de la LOPDGDD.

En las reclamaciones presentadas por otros asuntos, la adopción por el responsable de medidas adecuadas, tanto para corregir el incidente objeto de la reclamación como para evitar situaciones similares en el futuro fue la causa de que la reclamación se entendiera resuelta. Así, a modo de ejemplo, de las 184 reclamaciones relacionadas con violaciones de la seguridad de los datos personales que se resolvieron en 2020 tras el traslado de la reclamación, 130 lo fueron como consecuencia del establecimiento por parte del responsable de tales medidas adecuadas.

En lo relativo al procedimiento sancionador, interesa recordar que, a raíz de las novedades introducidas por el RGPD y la LOPDGDD, se unificó el procedimiento sancionador, sin distinguir en función de la naturaleza pública o privada del infractor. No obstante, sí existen diferencias en las sanciones que pueden imponerse. En caso de que el infractor tenga naturaleza privada, se puede resolver con una sanción económica o con un apercibimiento. En caso de que se constate la infracción, si el infractor tiene naturaleza pública, se sanciona con apercibimiento. Tanto la multa



administrativa como el apercibimiento pueden ir acompañados de medidas correctoras de las infracciones.

También 2020 ha sido el año de la consolidación del Canal Prioritario, cuyo objetivo es la atención urgente en caso de difusión ilegítima de contenidos sensibles, cuando afecten gravemente a sus derechos y libertades o puedan producir perjuicios de muy difícil reparación.

Gracias a la intervención de la Agencia se ha logrado, en unos plazos muy reducidos, la retirada de fotografías y vídeos de contenido sexual o violento que se visualizan a través de internet sin consentimiento de los afectados, muchas veces pertenecientes a colectivos vulnerables. Con ello se ha intentado que no se viralizaran, consiguiendo una efectividad muy alta.

Durante 2020 se han recibido 358 peticiones a través del *Canal Prioritario*, de las cuales 174 han entrado a través del canal de menores. Tras el análisis por parte de la Agencia, finalmente se han tramitado como urgentes 49 de estas peticiones por encontrarse dentro de los objetivos perseguidos por este Canal. Este número se ha triplicado respecto a 2019, año en el que se tramitaron 14 peticiones urgentes. De las 49, se han solicitado 29 retiradas urgentes de los contenidos a proveedores de servicios consiguiendo la retirada en más de un 86% de los casos. En los 20 casos restantes que no requerían la retirada de contenidos también se les ha dado un tratamiento prioritario sin adoptar dichas medidas. Por otro lado, el resto de peticiones recibidas a través del Canal Prioritario también puede haber continuado su tramitación, aunque ya sin el carácter de urgencia, debido a que, tras el análisis de las mismas, se ha observado que no tienen relación con contenidos especialmente sensibles.

Pese a la eficacia que ha demostrado la adopción de medidas a través del Canal Prioritario, el número de reclamaciones presentadas ha sido reducido, por lo que resulta necesario insistir en la difusión de dicho Canal para promover su utilización con el fin de dar una respuesta eficaz frente a la difusión de imágenes sobre violencia digital.

Por otro lado, se han remitido determinadas reclamaciones a las autoridades autonómicas de protección de datos por referirse a materias de su competencia.

El detalle del conjunto de reclamaciones tramitadas por la Subdirección General de Inspección de Datos y su valoración figura en el apartado correspondiente de la Agencia en cifras.

Con independencia de las cifras indicadas, y a la vista de la entrada recibida en la Subdirección, se advierte que a lo largo de 2020 se ha registrado un importante número de reclamaciones referidas a tratamientos de datos personales en ámbitos directamente relacionados con la pandemia.

**La tasa de reclamaciones resueltas frente a las presentadas ha sido de un 101%, produciéndose una mejora de un 5% frente a los resultados del año anterior.**

También se ha reducido el número de reclamaciones pendientes de resolver a final del año en un 3%. A pesar de que estos datos numéricos no tienen en cuenta la complejidad de las reclamaciones y de los asuntos tratados, que han exigido un mayor nivel de dedicación comparándolo con el ejercicio 2019, se puede observar la mejora producida.

Esto permite obtener como conclusión que el teletrabajo de manera continuada ha permitido obtener unos resultados mejores que los del año anterior.

Se han estudiado los casos urgentes recibidos a través del Canal Prioritario, se han investigado las presuntas vulneraciones de la normativa referentes a tratamientos que guardan relación con la COVID19, al tiempo que se continuaban gestionando y resolviendo los expedientes abiertos durante 2019 y durante el 2020. Esto constituye un logro muy relevante y demuestra que la capacidad de adaptación de la Agencia para responder a los retos y continuar velando por el derecho a la protección de datos personales ha sido muy grande y que los resultados del

teletrabajo han sido tan eficaces o más que los del trabajo presencial, como lo demuestra el aumento de la productividad.

Relacionado con este aspecto hay que destacar que el teletrabajo no solo ha permitido mantener el capital humano que tiene la subdirección, que valora en gran medida la posibilidad de conciliar que ofrece esta modalidad de trabajo, sino que también ha facilitado la incorporación de nuevas personas a la plantilla.

## 7.2. Procedimientos más relevantes

### Ámbito nacional

Durante el año 2020, se puede destacar que se han analizado 165 reclamaciones relacionadas con la captación y/o difusión de la imagen de miembros de las fuerzas y cuerpos de seguridad, en redes sociales y aplicaciones de mensajería; estas actuaciones han sido realizadas por particulares, generalmente en el marco de operaciones policiales realizadas para la verificación del efectivo cumplimiento de las restricciones gubernativas adoptadas durante el estado de alarma. Prácticamente en su totalidad estas reclamaciones han sido archivadas tras su análisis, al no apreciarse que los tratamientos concretos afectados pudieran vulnerar la normativa de protección de datos.

Debe recordarse que, al margen del régimen sancionador previsto en esta normativa, el artículo 36.23 de la Ley Orgánica 4/2015, de Protección de la Seguridad Ciudadana, prevé que, cuando pueda poner en peligro la seguridad personal o familiar de los agentes, de las instalaciones protegidas o en riesgo el éxito de una operación, puede ser constitutivo de infracción de esa ley orgánica el uso de imágenes o datos personales o profesionales de los citados miembros. A este respecto, resulta significativa la Sentencia TC (Pleno) 172/2020, que el 19 noviembre de 2020 declaró inconstitucional y anuló el inciso "no autorizado" que, referido a ese uso, había sido aprobado por el legislador.

Fueron también numerosas las reclamaciones presentadas por particulares contra vecinos (que se dieron en denominar "policías de balcón") por la difusión en redes sociales de fotografías y vídeos con el objetivo de dar publicidad a supuestos incumplimientos de las mencionadas restricciones, generalmente en la vía pública. En estos casos, la Agencia informó a los afectados sobre los instrumentos disponibles en las correspondientes redes para limitar la difusión de los datos, ejercitando el derecho previsto en el artículo 94.2 de la LOPDGDD.

Las reclamaciones referidas a incumplimientos legales en el tratamiento de datos sanitarios asociados a la pandemia por la COVID-19 también merecen ser destacadas particularmente contra un sitio web que, con garantías no suficientemente acreditadas, ofrecía contacto con profesionales médicos para la asistencia sanitaria online. Tras las actuaciones practicadas, los responsables del sitio web, que permaneció en servicio dos meses, aportaron a la Agencia las garantías que habían adoptado para cumplir cada uno de los requisitos previstos en la normativa de protección de datos, particularmente las orientadas a asegurar la confidencialidad de los datos sanitarios.

Se recibieron también reclamaciones relacionadas con la toma de temperatura por personal que habitualmente realiza labores de vigilancia en la entrada, en el entorno laboral, en establecimientos comerciales y en lugares de culto religioso. La Agencia requirió información a los respectivos responsables sobre las citadas actividades.

Otras reclamaciones se referían a supuestas vulneraciones del principio de minimización de datos, generalmente relacionadas con la solicitud de informes acreditativos de la prueba de diagnóstico del coronavirus o de los informes sanitarios que, en su caso, eximían de portar mascarilla. A este respecto, se verificó el cumplimiento estricto de las medidas preventivas decretadas por las distintas Administraciones públicas sanitarias, que las fuerzas de seguridad debían garantizar y que los establecimientos comerciales debían implementar.

Han sido también significativas las reclamaciones analizadas que se referían a la vulneración del principio de confidencialidad asociado al dato de contagio por el coronavirus en distintos ámbitos, particularmente en el entorno laboral y en redes sociales y medios de comunicación, si bien en este último caso la publicación del dato estaba generalmente amparada por la libertad de información. En el ámbito laboral, en particular, la Agencia solicitó al empleador que justificara, en cada caso, la ponderación realizada, entre el derecho a la privacidad del trabajador contagiado y la necesidad de evitar el contagio del resto de trabajadores.

También se recibieron reclamaciones contra centros educativos que, atendiendo a las restricciones de movimiento asociadas al estado de alarma y en ejercicio de la función educativa que tienen encomendada, se habían visto impulsados a emplear herramientas de teleeducación, en video clases o exámenes online, expresamente previstas en el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por la COVID-19.

Cabe destacar el procedimiento PS/00052/2020, instruido contra la Consejería de Educación e Innovación de la Comunidad de Madrid, en relación con el uso de una aplicación informática por parte de algunos profesores de un centro educativo de la Comunidad de Madrid como recurso metodológico para el alumnado. El procedimiento concluye con una sanción de apercibimiento por incumplimiento del artículo 5.1.a del RGPD.

También merece la pena destacar el PS/00245/2019 que finalizó con un apercibimiento a la Dirección General de Educación del Gobierno de Navarra por infringir el artículo 5.1.a) del RGPD relación con el artículo 9.1 del RGPD y 9.1 de la LOPDGDD, y por el artículo 13 del RGPD. En este caso, el departamento de Educación hacía cuestionarios a los alumnos de 4º de Primaria en los que incluía el sexo del alumno dando tres alternativas (chico, chica, u "otras opciones").

Algunas reclamaciones se referían a la recepción de comunicaciones electrónicas comerciales en las que se promocionaban productos sanitarios y actividades formativas relacionados con la pandemia y que en numerosos casos vulneraban la normativa específica que regula su emisión, el artículo 21 de la LSSI. En el ámbito publicitario debe señalarse que la actividad promocional telefónica, regulada en el artículo 48 de la LGT, ocasionó, como otros años, numerosas reclamaciones (más del 6% del total de reclamaciones presentadas), fundamentalmente contra operadores de telecomunicaciones, que fueron objeto de un exhaustivo análisis por parte de la Subdirección General de la Inspección de Datos. Por lo que respecta al comercio online, son particularmente destacables las deficiencias detectadas en el cumplimiento del derecho de información previsto en el artículo 13 del RGPD y en la forma de obtener el consentimiento para la finalidad publicitaria.

Otras reclamaciones se referían a acciones agresivas con carácter presuntamente delictivo que pretendían la obtención de beneficios económicos a partir de la excepcionalidad de la situación vivida por los ciudadanos que, como consecuencia del confinamiento, estaban haciendo un mayor uso de los servicios telemáticos. Estas reclamaciones, que en su práctica totalidad se referían a conductas extorsionadoras ("sextorsión online") fueron trasladadas a la Fiscalía General del Estado, en aplicación del Protocolo General de Actuación suscrito en 2019, para la colaboración en materia de atención a las personas cuyos datos se hayan obtenido y difundido ilegítimamente. Por lo general, estas reclamaciones se presentaron a través del Canal Prioritario, que desde el mes de septiembre de 2019 está disponible en el sitio web de la Agencia y que se consolidó a lo largo de 2020.

En relación con las brechas de seguridad de datos personales que se notificaron a la Agencia y fueron remitidas a la Subdirección General de la Inspección de Datos para su estudio, se ha detectado un aumento de ataques por ransomware relacionados con la pandemia.

En 2020 se ha consolidado un descenso en los procedimientos de ejercicio de derechos y un aumento de procedimientos sancionadores. Probablemente su razón se encuentre en que se han recibido muchas denuncias por la deficiente implantación de las obligaciones establecidas en el RGPD, particularmente de la obligación de informar acerca del tratamiento de datos personales con anterioridad al mismo.

Hay que destacar las investigaciones efectuadas acerca de esas cláusulas informativas y los consentimientos solicitados por parte de entidades del sector bancario, y que han dado lugar a la incoación y resolución, en un caso, de expedientes sancionadores mucho más complejos y extensos que los que se resolvían con la anterior normativa de protección de datos. Se ha profundizado en el estudio pormenorizado de las cláusulas informativas que se facilitan a los clientes, poco comprensibles y que en muchos casos incorporan solicitudes de consentimientos para comunicaciones a empresas del Grupo que exceden de los supuestos recogidos en el RGPD.

Este análisis de los protocolos de adecuación al RGPD ha determinado la imposición de multas de carácter disuasorio -previstas en dicha norma en cuantías superiores a las de la normativa anterior-, junto con requerimientos de adecuación a la normativa vigente en un plazo de tiempo concreto.

En este sentido, debe señalarse que el RGPD ha modificado sustancialmente el modelo de supervisión frente al de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Esta modificación afecta tanto a las acciones correctivas como a las multas económicas para hacer frente a las infracciones del Reglamento. El RGPD ha incorporado un amplio abanico de acciones correctivas, como las siguientes:

- Sancionar con una advertencia cuando las operaciones de tratamiento previstas puedan infringir RGPD
- Sancionar con apercibimiento cuando las operaciones de tratamiento hayan infringido RGPD

- Ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos
- Ordenar que las operaciones de tratamiento se ajusten a las disposiciones del RGPD, de una determinada manera y dentro de un plazo especificado
- Ordenar al responsable que comunique al interesado las violaciones de la seguridad de los datos personales
- Imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición

Medidas correctivas que se añaden a las de resolución extrajudicial o amistosa de reclamaciones a través del procedimiento de traslado a responsables y delegados de protección de datos que se comenta en esta Memoria.

En cuanto a las multas económicas, el Reglamento establece que deberán ser efectivas, proporcionadas y disuasorias, incluyendo sanciones económicas que pueden llegar hasta los 20 millones de euros o el 4% del volumen de negocio a nivel mundial del responsable de la infracción.

Esta última previsión ha determinado un cambio sustancial en la cuantía de las sanciones económicas en caso de determinadas infracciones del Reglamento, del que son una muestra las importantes sanciones económicas con cuantías de millones de euros impuestas por autoridades de protección de datos de los Estados miembro de la UE, entre las que se encuentra la Agencia Española de Protección de Datos.

A este respecto, cabe citar el procedimiento PS/00070/2019 en el que se sanciona a la entidad Banco Bilbao Vizcaya Argentaria (BBVA) porque el documento facilitado a los clientes para informarles del tratamiento de sus datos personales no cumple con los requisitos exigidos en el RGPD: es inadecuada o insuficiente la terminología, no informa de las finalidades del tratamiento ni de las bases legales para el mismo, principalmente para aquellos tratamientos basados en el interés

legítimo. También se sanciona a la entidad porque los consentimientos no eran específicos, e informados, ni estaban legitimados por el interés legítimo. Además de las sanciones económicas impuestas, que suman en conjunto un importe de 5 millones de euros, se ha requerido a la entidad para que realice las modificaciones necesarias para el cumplimiento de lo establecido en los artículos 6, 13, y 14 del RGPD.

También se ha continuado tramitando el procedimiento PS/00477/2019 contra la entidad Caixabank, por la cláusula informativa facilitada a los clientes y los tratamientos realizados basados en el interés legítimo. Este procedimiento finalizaría en los primeros días de 2021. Además de las sanciones económicas, que en conjunto sumarían un importe de 6 millones de euros, se requería a la entidad la realización de las modificaciones necesarias para el cumplimiento de lo establecido en los artículos 6, 13, y 14 del RGPD.

Asimismo, se han resuelto reclamaciones referidas al tratamiento de los datos de la huella dactilar para el control horario y laboral de los trabajadores que han sido muy novedosos por la temática que conlleva y porque se empiezan a utilizar datos biométricos.

Así, por ejemplo, en el E/05310/2020 se han llevado a cabo actuaciones previas de investigación ante la Asociación del Colegio Alemán de Bilbao por la implantación de un sistema de gestión para el registro de jornada laboral de sus trabajadores mediante huella dactilar. Finalmente se acredita que la actuación de la reclamada, como entidad responsable del tratamiento, ha sido acorde con la normativa sobre protección de datos personales y se procede al archivo de las actuaciones.

Se puede encontrar otro ejemplo relevante en el PS/00418/2019. Se trata de reclamaciones contra el sistema de identificación y reconocimiento electrónico mediante la huella digital y rasgos faciales creado por Izenpe -prestador de Servicios de Confianza- para la identificación de los trabajadores y usuarios del servicio Vasco de Empleo -Lanbide-. Para la emisión de los medios de identificación se recaban huellas dactilares de los diez dedos de las manos, lo que se considera

desproporcionado y se resuelve con una sanción de apercibimiento impuesta a Izenpe. También se requiere a la entidad que adecúe sus operaciones de tratamiento a la normativa de protección de datos y, en concreto, que mantenga el registro de una sola huella dactilar, a su elección, y que proceda a la eliminación del resto de huellas -las correspondientes a nueve dedos de las manos-.

Los procedimientos sancionadores originados por reclamaciones motivadas por sistemas de video-vigilancia que graban vía pública y carecen de cartel informativo siguen siendo muy numerosos, reflejando la preocupación de los ciudadanos por la vulneración de su privacidad por grabaciones desproporcionadas a la finalidad perseguida.

Otro asunto para destacar es la ausencia de DPD en la organización. Durante el año 2020, se han finalizado 8 procedimientos sancionadores por este motivo. Dos de ellos se refieren a la infracción cometida por empresas privadas (PS/00417/2019 a Glovoapp23, S.L. y PS/00251/2020 cuyo responsable es una empresa de seguridad). Los otros seis procedimientos sancionadores se han realizado como consecuencia de las reclamaciones presentadas contra seis ayuntamientos que carecían de Delegado de Protección de Datos. Tres de estos ayuntamientos fueron sancionados y se requirió su nombramiento (PS/00314/2020 Ay. De Fuente del Saz, PS/00325/2020 Ay. De San Fernando de Henares y PS/00326/2020 Ay. De Mejorada del Campo). Los tres restantes habían iniciado la tramitación del nombramiento del DPD en el transcurso del expediente (PS/00226/2019 Ay. De Sevilla, PS/00001/2020 Ay. De Huerca y PS/00257/2020 Ay. De Arroyomolinos).

También hay que destacar la importancia que tienen los expedientes relacionados con los servicios de Internet que suponen un 16% del total, con un incremento del 5% respecto del año anterior. Este tipo de expedientes está marcando una tendencia creciente y a su vez requieren para su resolución de unos conocimientos tecnológicos avanzados y en continua formación.



Se puede destacar el procedimiento PS/00416/2019, instruido contra la entidad Miraclia, en relación con una reclamación por la utilización de los datos personales del reclamante para hacerle una broma mediante una llamada telefónica a su línea móvil, sirviéndose para ello de una app. La llamada se graba y se difunde a terceros sin el consentimiento del afectado. Tras el estudio del caso, se imponen dos sanciones a Miraclia, por infracción del principio de transparencia y por ausencia de base legitimadora, por un importe de 20.000 euros cada una, y se requiere a la entidad la adecuación de sus tratamientos a la normativa de protección de datos.

También hay que destacar que durante el estado de alarma se abrieron varias investigaciones por iniciativa propia relacionadas con tratamientos de datos personales en ámbitos directamente relacionados con la pandemia, en especial, por posibles incumplimientos legales en el tratamiento de datos sanitarios asociados a la COVID-19, como webs, chats y apps de información, así como apps de rastreo de contactos COVID-19 por bluetooth, registro de datos relacionados con la pandemia, toma de temperatura en sistemas de transporte a los usuarios, en los establecimientos a los clientes, registro de datos del acceso de los clientes a establecimientos bajo el amparo de algunas normativas autonómicas, tratamientos de reconocimiento facial a la entrada de establecimientos, estudios de movilidad durante el estado de alarma.

Algunas de las investigaciones relativas al uso de webs, chats y apps de información terminaron en archivo al no acreditarse incumplimientos.

Este es el caso del expediente E/03832/2020 relacionado con la creación de una web-app de la Generalitat Valenciana cuyo objetivo era la petición de cita médica y el autodiagnóstico o del expediente E/03771/2020 basado en el desarrollo de una aplicación web y una app para dispositivos móviles web y app del Gobierno de Navarra. En el ámbito privado y también relacionado con el desarrollo de aplicaciones destaca el expediente E/2729/2020 en el que se realizó un análisis a la aplicación Coronastop desarrollada por Hocelot technologies Spain S.L.

También asociado a las actuaciones realizadas como consecuencia de la COVID-19 se puede mencionar el expediente de investigación realizado a RENFE Viajeros Sociedad Mercantil Estatal, S.A., E/03689/2020, por la implantación del billete personalizado, en todos sus canales de venta y para todos los servicios comerciales que precisaran reserva de plaza, solicitando a los viajeros datos personales como nombre, DNI y un número de teléfono móvil para contactar por motivos de salud.

La mayoría de estas investigaciones relacionadas con la COVID-19 siguen en curso por ser tratamientos complejos y estar algunos aún en desarrollo.

Por último, cabe mencionar el procedimiento PS/00070/2020 en el que el reclamante denuncia al alcalde de un municipio por la difusión, a través de su perfil de Facebook, de una sentencia judicial de la que se desprenden datos de salud sobre su persona. En dicha sentencia, el reclamante es demandante contra el Ayuntamiento y el reclamado, en calidad de alcalde del municipio.

Aunque el perfil de Facebook del reclamado es su perfil privado, los hechos tienen relación con su condición de alcalde. Finalmente, se sanciona con apercibimiento por infracción del artículo 5.1.a) del RGPD a la persona física, que secundariamente es alcalde, por usar Facebook, con su cuenta personal y a título particular para exponer una sentencia de una persona que litigaba contra el Ayuntamiento y el alcalde.

### **Ámbito transfronterizo**

Especial interés suscita, por su contenido novedoso, el asunto tramitado por la vía del procedimiento de cooperación, previsto en el artículo 60 del RGPD para los tratamientos transfronterizos, y relacionado con una violación de seguridad de los datos que afectó a la red social Twitter. En este asunto, la Agencia actuó en calidad de Autoridad interesada y, en su desarrollo, intervino el Comité Europeo de Protección de Datos para resolver la controversia surgida entre el proyecto de decisión de la Autoridad Principal y las objeciones pertinentes y motivadas presentadas por las Autoridades interesadas, siendo adoptada la Decisión 01/2020.

Entre otros asuntos de interés tramitados por el procedimiento de cooperación, pueden citarse, asimismo, la violación de seguridad de los datos personales padecida por una cadena hotelera de Reino Unido, Marriot Hotels, en la que pudieron verse afectados alrededor de 339 millones de registros, y la sufrida por una empresa con establecimiento principal en Reino Unido, Ticketmaster, en la que más de 9 millones de clientes pudieron ser potencialmente afectados y resultar comprometidos detalles de sus tarjetas bancarias.

También merece destacar, el primer procedimiento sancionador de ámbito transfronterizo que se ha resuelto siendo autoridad líder la AEPD respecto de los tratamientos realizados por la empresa Miraclia. Fue tramitado como consecuencia de una reclamación presentada en la autoridad de control de un país miembro de la UE contra una empresa cuyo responsable del tratamiento en Europa tiene su sede en España. Hay que indicar que estos procedimientos tienen un tratamiento complejo y una duración mayor que la de los procedimientos nacionales.

La Agencia, después de postularse para colaborar en operaciones conjuntas con las autoridades de Irlanda y Luxemburgo en 2019, tras un año de negociaciones, en marzo de 2020 firmó un Memorando de Entendimiento o MOU con la autoridad irlandesa para colaborar en una operación conjunta bajo el artículo 62 del RGPD, que concluyó con la entrega en plazo de las actividades solicitadas. Bajo un artículo 61 se estableció en septiembre de 2019 una colaboración con la autoridad italiana para la investigación de un tratamiento en España y otro en Italia de una compañía española con implantación internacional, también en Italia; esta colaboración ha continuado en 2020 con la entrega de la documentación solicitada y recopilada en la investigación de los tratamientos.

Por último, cabría subrayar que en 2020 la Subdirección ha participado en un estudio sobre el uso del Big Data en el sector europeo de los seguros y sobre prácticas de los databrokers en el subgrupo de Social Media del EDPB -Comité Europeo de Protección de Datos-.

### 7.3. Planes sectoriales o de auditoría

Durante el año 2020 se presentaron los resultados de dos planes de oficio: el Plan de Inspección de Oficio de la Atención Sociosanitaria y Plan de Inspección de Oficio sobre Contratación a Distancia en Operadores de Telecomunicaciones y Comercializadores de Energía.

El ‘Plan de Inspección de oficio de la atención sociosanitaria’, analiza por primera vez los tratamientos que se llevan a cabo en este ámbito e investiga su adecuación a la normativa de protección de datos.

Entre las conclusiones más relevantes se encuentran las referidas a la información que se debe ofrecer al usuario de estos servicios, que preferiblemente será por capas, concisa y con un lenguaje claro, de acuerdo con la capacidad de comprensión del destinatario de la información.

Durante las auditorías se detectaron problemas relacionados con la identificación por parte de los responsables de las bases jurídicas que amparan los tratamientos.

En el desarrollo de la inspección se apreciaron dudas sobre si los centros podían facilitar información sobre la estancia, ubicación o estado de salud de un usuario a solicitud de los familiares. En este sentido, la AEPD observa que debe recabarse el consentimiento del usuario.

No obstante, en casos de urgencia vital o si la presencia de personas vinculadas al usuario por razones familiares o de hecho pudiera ser esencial para la debida atención del usuario, siempre que el paciente no se haya opuesto a que dicha información sea facilitada, el centro puede informar si la persona se encuentra ingresada y su ubicación, sin indicar datos de categorías especiales o sobre la atención prestada.

El apartado de preguntas frecuentes da respuesta a otras dudas surgidas en el contexto de la actividad de la atención sociosanitaria, por ejemplo, si es posible cancelar determinados datos de un

usuario a petición suya, llevar a cabo tratamientos con fines de investigación médica en un centro, o si es obligatorio facilitar datos personales de los usuarios del centro si lo solicitan las fuerzas de seguridad.

El Plan incluye recomendaciones relativas a la seguridad de los datos debido a que se trata de categorías especiales, como minimizar la compartición de datos personales entre profesionales a lo estrictamente necesario; elaborar perfiles de acceso que consideren las necesidades de información de cada profesional; realizar auditorías de los accesos; que los empleados que traten datos personales de los usuarios suscriban un compromiso de confidencialidad, o evitar la utilización de usuarios genéricos cuya utilización se comparte entre varios empleados, entre otras.

El 'Plan de inspección de oficio sobre contratación a distancia en operadores de telecomunicaciones y comercializadores de energía' analiza los tratamientos de datos en estos sectores y su adecuación a la normativa de protección de datos desde la perspectiva de la acreditación de la identidad del contratante y de los servicios contratados.

El Plan hace hincapié en la verificación de los procedimientos que se utilizan en los sectores de telecomunicaciones y energía para identificar a los interesados con el objetivo de evitar la suplantación de identidad y el consiguiente fraude.

Asimismo, la Agencia, consciente de la necesidad de que las empresas estén en condiciones de acreditar los servicios contratados cuando estos se realizan a distancia y por tanto sin presencia de los contratantes, ha prestado especial atención a este aspecto, analizando proyectos innovadores implantados por las entidades. Entre ellos, se encuentran la firma manuscrita biométrica, el reconocimiento facial, los productos de análisis de riesgos online, la notificación electrónica certificada y la prueba acreditativa de los sucesos digitales.

El Plan se complementa con un decálogo dirigido a los usuarios para asegurarse de que se está accediendo a la página web de la empresa con la que se desea contratar; leer la política de privacidad; utilizar contraseñas seguras e informarse sobre la posible comunicación de sus datos a terceras

empresas o cómo ejercer sus derechos, son algunas de las recomendaciones.

A raíz de las incidencias detectadas en materia de transparencia e información, la Agencia recomienda que, en los medios telemáticos donde no es posible facilitar una información completa al usuario, se adopte un modelo de información por capas o niveles. Asimismo, recuerda que los datos personales deben recopilarse para fines específicos, explícitos y legítimos y no para fines distintos de los establecidos originalmente.

Entre las recomendaciones relacionadas con los tratamientos basados en el consentimiento destaca la necesidad de que el responsable se asegure de que el consentimiento obtenido sea libre, específico, informado e inequívoco.

Respecto a la acreditación de la identidad del interesado, se destaca la necesidad de extremar las garantías de identificación del contratante antes de llevar a cabo el contrato y recuerda la importancia de utilizar sistemas con garantías adicionales, como la autenticación reforzada del cliente, basada en la utilización de dos o más elementos independientes que proceden de algo que sólo conoce, posee o es el usuario, de forma que la vulneración de uno no comprometa la fiabilidad de los demás.

Para la acreditación de la contratación a distancia, se subraya que es recomendable que las empresas utilicen sistemas que permitan acreditar los contratos efectuados telemáticamente mediante la obtención de prueba de los sucesos digitales. También recuerda que los datos recabados para captar clientes y que finalmente no llegan a materializarse en una relación comercial deben ser suprimidos salvo que se basen en otro fundamento jurídico.

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

También se ha continuado con los trabajos de Evaluación Schengen a España, si bien condicionado por las limitaciones impuestas por la pandemia.

## 8. Una estructura en permanente evolución

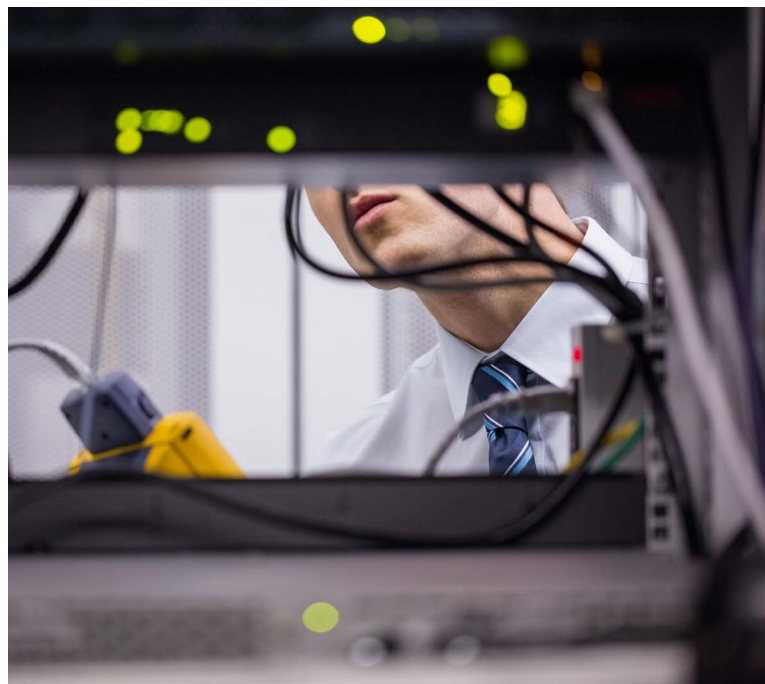
### 8.1. Avance en digitalización

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, durante el pasado año 2020 la Agencia ha completado diversas iniciativas relevantes tanto en el área de las infraestructuras y la seguridad como de los servicios y aplicaciones.

En primer lugar, cabe destacar la puesta en marcha del **servicio compartido GEISER** que proporciona la Secretaría General de Administración Digital, como solución de registro electrónico. GEISER ha permitido reemplazar una aplicación específica de desarrollo propio, en una clara apuesta de la Agencia por la reutilización y la racionalización en el uso de sus recursos.

Adicionalmente, ahondando en este compromiso con la utilización de los medios comunes, la Agencia ha abordado las tareas tecnológicas necesarias para la actualización a **Cl@ve 2.0**: la sede electrónica incorpora ahora esta versión que permite la conexión con el nodo eIDAS español, y habilita el reconocimiento de los sistemas de identidad electrónica de otros países europeos. De igual modo, el pasado año se ha iniciado la **emisión y gestión de las notificaciones en papel** mediante el servicio **Notific@**, que hasta el momento se venía empleando de forma exclusiva para las de carácter electrónico.

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 2020, se ha llevado a término la renovación en su totalidad de la sede electrónica anteriormente referida. Sobre una plataforma tecnológica actualizada, la *nueva sede electrónica* ofrece un diseño más usable y responsive, así como múltiples funcionalidades mejoradas.



Internamente, la Agencia ha concluido un proceso de migración y reordenación esencial para la modernización de sus infraestructuras y la mejora de la seguridad, disponiendo su CPD en un servicio de Virtual Data Center en Nube que garantiza el nivel medio del ENS. Este servicio comprende un Centro de Ciberoperaciones de Seguridad (SCC) 24 x 7, en contacto directo con el responsable de operaciones.

Por último, otra iniciativa destacable, orientada en este caso a la mejora de la protección de la información, ha sido la puesta en marcha de un servicio de impresión centralizada, que incluye la característica Follow-Me. Esta función crea un entorno virtual que permite al usuario imprimir sus documentos mediante cualquiera de las impresoras disponibles, según momento y lugar con el valor añadido en seguridad, debido a que la petición de impresión no se procesa hasta que la persona que la ha realizado acude y se identifica debidamente en la impresora.

## 8.2. El teletrabajo como herramienta de Prevención de Riesgos Laborales (PRL)

Desde marzo de 2020, el teletrabajo se ha convertido en la principal herramienta de la AEPD a efectos de minimizar el riesgo de contagio de la plantilla durante la pandemia. Si bien el impulso del teletrabajo ya estaba recogido en la política de RSC de la Agencia y en los primeros dos meses se había impulsado esta forma de prestación laboral hasta el 80 % de la plantilla, ha sido a raíz de la situación de emergencia sanitaria cuando el teletrabajo se ha implantado para la práctica totalidad de la plantilla y de forma continuada (el 100% de la jornada).

Para garantizar la compatibilidad de esta situación con la prestación del servicio en condiciones de calidad, se ha establecido un sistema de turnos en aquellas unidades en las que, tras un análisis de las funciones, se ha advertido tal necesidad. Esto ha afectado fundamentalmente a la SGID y a la Oficina de registro, dependiente de Secretaría General. En consonancia con las medidas aconsejadas por las autoridades competentes, en la Oficina de registro se ha establecido un sistema de cita previa para la atención al ciudadano.

De esta forma, por medio de este teletrabajo continuado, que se ha imbricado en la modalidad de teletrabajo extraordinario por razones de salud pública, prevista en las distintas Resoluciones que han regulado sucesivamente el Programa de teletrabajo de la entidad, se ha conseguido minimizar los desplazamientos y el contacto social de los empleados de la Agencia, con la reducción de riesgos que ello conlleva en la situación de la pandemia.

Las encuestas de evaluación del teletrabajo han reflejado lo acertado de la decisión anterior, que cuenta con el máximo respaldo de la plantilla. De esta forma, la valoración de empleados y supervisores del teletrabajo continuado ha sido globalmente positiva – los empleados lo puntúan con un 8.92 y los supervisores del teletrabajo con un 9.34, destacando que éstos descartan que el teletrabajo suponga cargas en la planificación

del trabajo de las unidades-. Asimismo, de las encuestas se deduce que el teletrabajo continuado no ha afectado al clima laboral, y del análisis de las tecnologías de la información empleadas para el desarrollo de la prestación de servicios se ha comprobado empíricamente que la actividad ofrece indicadores de participación y actividad de los trabajadores sostenidos a lo largo del año. Esto, junto al cumplimiento de los objetivos generales de la Agencia permite afirmar que el teletrabajo continuado ha coadyuvado al mantenimiento del nivel de actividad.

De esta forma, el teletrabajo se sigue considerando una herramienta indispensable en la política de recursos humanos del ente, tanto para captar talento como para retenerlo, y para impulsar la conciliación de los empleados y su satisfacción e identificación con la organización.

En consonancia con la situación, tanto la realización de reuniones de trabajo y de órganos colegiados como la realización de las actividades formativas se han realizado de forma completamente telemática (sin perjuicio de que algunas puedan haberse seguido desde la Agencia por algunos empleados, de forma mixta). Este cambio ha impactado de forma positiva especialmente en materia de Formación, apreciándose una mayor participación de la plantilla en las actividades formativas.

## 8.3. Otras actuaciones en materia de PRL

A lo anterior hay que sumarle otras actuaciones en materia de PRL, recogidas en el documento *Protocolo para la reincorporación al centro de trabajo tras el fin del estado de alarma, realizado en abril de 2020*. Por medio de este documento se recogen diversas medidas que se adoptarán cuando se produzca la vuelta a un sistema mixto de teletrabajo y, por consiguiente, la vuelta a la presencialidad de la prestación laboral. Entre otras actuaciones, se ha adaptado el edificio para garantizar la seguridad de aquellos empleados que participan en el sistema de turnos y aquellos que decidan asistir con regularidad a la sede de la Agencia: se ha dotado de gel hidroalcohólico, pantallas protectoras, mascarillas, pañuelos,



papeleras con tapa y demás elementos recomendados por las autoridades sanitarias y laborales.

Asimismo, se ha realizado un estudio de los espacios y la distribución de las personas y se ha diseñado un sistema de turnos a efectos de garantizar que se mantengan las distancias de seguridad incrementando, en el caso de despachos compartidos, un día de teletrabajo a efectos de que no se compartan espacios. A todo ello se le ha unido las labores de información y comunicación al personal, incluyendo la colocación de señales y la señalización de distancias.

#### 8.4. Provisión de puestos

Además de todo lo anterior, a lo largo del año se ha producido un importante esfuerzo para garantizar la dotación de puestos:

- Concursos: dos concursos específicos y dos concursos generales, afectando a un total de 18 puestos de trabajo.
- Libres designaciones: tres convocatorias, afectando a un total de 8 puestos de trabajo.
- Publicaciones en Funciona de 13 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.

#### 8.5. Ejecución presupuestaria

##### Ejecución presupuestaria del presupuesto de gastos

El Presupuesto de la Agencia Española de Protección de Datos en el ejercicio 2020 ha seguido siendo, como en 2019, el presupuesto prorrogado del año 2018 por importe de 14.228.680 euros. Sin embargo, en 2019 el presupuesto se vio incrementado en más de un 5,5 % tras una generación de crédito a partir de unos fondos FEDER obtenidos ese mismo año.

A lo largo del ejercicio económico 2020 se han aprobado varias modificaciones presupuestarias internas que no han incrementado la cuantía inicial del presupuesto de gastos. Principalmente se han transferido créditos desde el capítulo 6 para financiar el acondicionamiento de la sede de la Agencia a la Inspección Técnica de Edificios y para la cobertura de los gastos financieros generados como consecuencia de las liquidaciones negativas de la cuenta que la Agencia tiene en el Banco de España, y desde el capítulo 2 para financiar la inclusión de la Agencia Española de Protección de Datos en el contrato centralizado para la prestación de los servicios consolidados de telecomunicaciones a la Administración General del Estado y las necesidades del capítulo primero de gastos de personal.

Por Orden de la Ministra de Hacienda y en cumplimiento del Real Decreto Ley 11/2020, de 31 de marzo, por el que se adoptan medidas urgentes complementarias en el ámbito social y económico para hacer frente a la COVID-19, la AEPD tuvo que realizar un ingreso en el Tesoro Público de 21 millones de euros para contribuir a las necesidades económicas derivadas de la COVID-19, lo que supuso una merma de alrededor de un 40% del remanente de tesorería de la AEPD.

En cuanto al nivel de ejecución, se ha producido un incremento significativo respecto al año anterior, llegándose a un porcentaje de ejecución superior al 99%, 11,5 puntos más que en 2019.

## Presupuesto 2019 - 2020 Presupuesto, obligaciones reconocidas y porcentaje de ejecución

2019	Cap	Descripción	Presupuesto	Obligaciones reconocidas	Porcentaje de ejecución
	I	Gastos de personal	8.625.050,03 €	7.437.996,30 €	86,24%
	II	Gastos corrientes en bienes y servicios	5.082.028,20 €	4.616.681,36 €	90,84%
	III	Gastos financieros	180.950,00 €	151.398,12 €	83,67%
	IV	Transferencias corrientes	338.992,00	294.930,67 €	87,00%
	VI	Inversiones reales	937.860,00 €	809.867,86 €	86,35%
	VIII	Activos financieros	22.800,00 €	3.890,98 €	17,07%
	<b>TOTAL</b>		<b>15.187.680,23 €</b>	<b>13.314.765,29 €</b>	<b>87,67%</b>

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%
	<b>TOTAL</b>		<b>35.228.680 €</b>	<b>34.933.219,32 €</b>	<b>99,16%</b>

DIFERENCIAS 2019 - 2020	Cap	Descripción	Presupuesto	Obligaciones reconocidas	Porcentaje de ejecución
	I	Gastos de personal	598.752,75 €	492.073,73 €	12,56%
	II	Gastos corrientes en bienes y servicios	178.355,58 €	156.535,88 €	6,50%
	III	Gastos financieros	81.222,47 €	70.697,31 €	1,04%
	IV	Transferencias corrientes	21.089.885,63 €	21.127.937,63 €	12,97%
	VI	Inversiones reales	353.000 €	226.572,90 €	13,38%
	VIII	Activos financieros	0	2.217,62 €	-9,73%
	<b>TOTAL</b>		<b>20.040.999,77 €</b>	<b>21.618.454,03 €</b>	<b>11,49%</b>

## Ejecución presupuestaria del presupuesto de ingresos

El presupuesto aprobado para la Agencia en el ejercicio 2020 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 9.127.610 euros y con un remanente de tesorería por un importe de 5.051.270 euros. El resto se cubre igualmente con las previsiones de transferencias corrientes (transferencias de la UE) por un importe de 20.000 euros, de ingresos patrimoniales (intereses de cuentas bancarias) por importe de 7.000 euros y con las previsiones de préstamos por un importe de 22.800 euros.

Durante el año 2020, el importe de los derechos reconocidos brutos asciende 8.950.381,99 euros, correspondiendo el 99,52% (8.907.017,59 €) 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 25% respecto a los datos de 2019. Los derechos reconocidos netos ascienden a 8.184.599,75 euros, una vez contabilizadas las insolvencias o anulaciones producidas durante este año.

La recaudación total en el ejercicio corriente 2020 asciende a 7.498.621,14 euros, de los que 7.455.256,74 euros corresponden a sanciones (un 99,42%). Esta recaudación ha supuesto un incremento de 322,08% respecto a la recaudación total de 2019.

La recaudación neta en el ejercicio corriente 2020 ha sido de 6.770.920,24 euros, una vez contabilizadas las devoluciones de sanciones, así como la devolución de los fondos del proyecto europeo SMOOTH.

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 2020 asciende a 8.826.753,47 euros, y la recaudación neta total ha sido de 8.167.337,22 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 2020 asciende a 659.416,25 euros y la devolución de intereses de demora a la cantidad de 42.904,16 euros, como consecuencia de la estimación total o parcial de recursos potestativos de reposición o contencioso-administrativos. En este campo hay que resaltar que las devoluciones en comparación con 2019 han disminuido en más del 50%.

## 9. La necesaria cooperación institucional

### 9.1. 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 2020, la secretaria del Consejo, por orden de la dirección, convocó 2 reuniones que se celebraron el 8 de julio y el 17 de diciembre de 2020, reuniones en las que se expuso y analizó la actividad del organismo.

En la reunión del 8 de julio destacó la presentación del Plan de Responsabilidad Social de la AEPD y toda la actividad de la Agencia en relación con la COVID-19.

En la reunión del 17 de diciembre, además de exponer la actividad de las distintas subdirecciones, se eligieron los trabajos premiados en la convocatoria de los premios de la AEPD de 2020. 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.

Señalar que el Consejo Consultivo se compone actualmente de 10 vocales, 4 de los cuales se hallan vacantes. También está pendiente la designación del director del Consejo de Transparencia

y Protección de Datos de Andalucía que asumió las competencias en la materia a inicios de 2020. Como quiera que los miembros del Consejo Consultivo son nombrados por el Gobierno a propuesta del Ministerio de Justicia y en representación de las entidades e instituciones previstas en el Estatuto de 1993, la directora de la Agencia dirigió a comienzos de 2020 una carta al Ministro de Justicia para informarle de las vacantes del Consejo y la necesidad de su cobertura.

### 9.2. 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 2020 dichas actividades se hayan focalizado en el denominado “Grupo internacional con autoridades autonómicas”.

En este sentido, en 2020 la División de Relaciones Internacionales de la Agencia y representantes de las autoridades autonómicas han celebrado una reunión del “grupo internacional”.

El principal objeto de esta reunión fue la puesta en marcha del nuevo mecanismo de cooperación e intercambio de información en relación con la actividad del Comité Europeo de Protección de Datos.

Este nuevo sistema responde a las previsiones de la Ley Orgánica 3/2018, según la cual la Agencia Española y las autoridades autonómicas podrán solicitar y deberán compartir la información necesaria para el cumplimiento de sus funciones y, en particular, la relativa a la actividad del Comité Europeo, en el que la Agencia es la representante común.

El sistema está basado en una plataforma colaborativa proporcionada por el INAP y permite

tanto que las autoridades autonómicas reciban información y documentación sobre las actividades del CEPD, que hagan aportaciones a los temas objeto de discusión en el Comité y que se pueden intercambiar opiniones entre todos los participantes en la plataforma.

Está previsto que el sistema se complemente con reuniones regulares, cuya periodicidad aún no está determinada, pero que se prevé tengan carácter trimestral, si bien en los primeros meses de implantación del sistema es previsible que sean más frecuentes. De hecho, en enero de 2021 ha tenido lugar ya la primera de estas reuniones, estando prevista la siguiente para el mes de abril.

### 9.3. Relaciones con el Defensor del Pueblo

#### Asuntos o materias objeto de queja

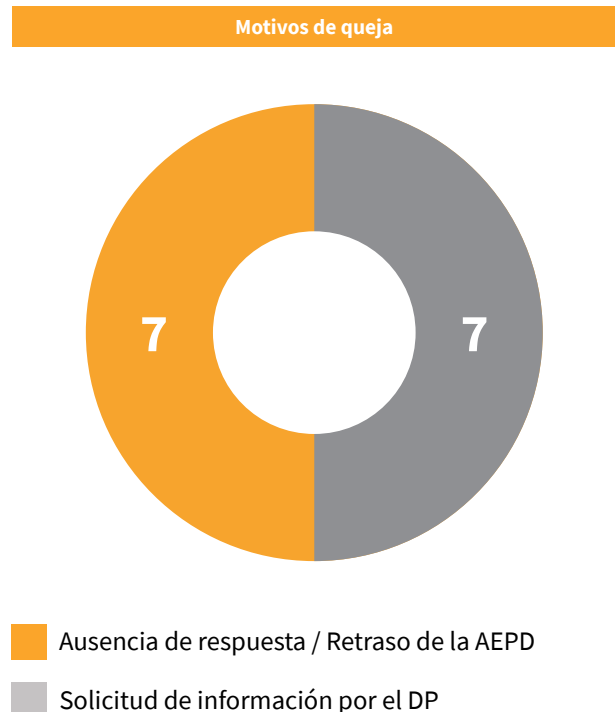
Durante el presente año 2020 se han tramitado un total de 14 asuntos, frente a los 23 del pasado año.



En cuanto a las materias o asuntos objeto de queja, no hay una cuestión prevalente. Así, las quejas promovidas ante esta Agencia hacen referencia a temas tan diversos como la inclusión en ficheros de morosos, la videovigilancia en el ámbito de las comunidades de vecinos, el ejercicio de los derechos de acceso (a la historia clínica) y de cancelación, o la recogida y tratamiento de la información de los datos de localización de terminales telefónicas móviles (geolocalización) o de tráfico de las comunicaciones.

#### Motivos de queja

Respecto a los motivos que han llevado a los ciudadanos a dirigirse a la AEPD mediante este cauce, el principal de ello, con diferencia, en siete ocasiones, ha sido el relativo a la queja por la falta de respuesta en plazo de la resolución de las correspondientes reclamaciones y recursos formulados ante la Agencia. En los siete restantes, el Defensor del Pueblo solicita información a esta Agencia sobre algún informe emitido por ella (así ocurrió en relación con el estudio del INE sobre geolocalización), sobre expedientes en curso (caso La Manada o de la Mancomunidad de Navarra sobre tarjetas para el uso de contenedores), o bien para conocer el criterio de la Agencia sobre algún tema para realizar un estudio más profundo del mismo, como el cobro de tarificación adicional del número de teléfono para conocer situación en los ficheros de morosos o el plazo de conservación de los datos relativos a la actividad de los abonados por parte de los operadores de telecomunicaciones.





## ➤ 10. Una autoridad activa en el panorama internacional

### 10.1. Unión Europea

Como se ha señalado en otro lugar de esta Memoria, la actividad del Comité Europeo de Protección de Datos se ha intensificado de forma significativa a lo largo del año 2020.

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 2020. Buena parte de la actividad del Comité en 2020 ha girado en torno a dos grandes temas: las implicaciones desde la perspectiva de la protección de datos de las medidas adoptadas por las autoridades para la lucha contra la COVID-19 y las transferencias internacionales de datos, en particular tras la Sentencia del Tribunal de Justicia de la UE conocida como Schrems II.

Respecto al primero de estos temas, desde el comienzo de la pandemia se hizo patente que la lucha contra la enfermedad implicaba el uso de datos personales, en particular, de datos de salud. Por ello, el Comité Europeo de Protección de Datos consideró necesario adoptar diversos documentos en los que se establecieran límites, criterios y garantías para esos usos de los datos personales.

Cuatro de estos documentos son otras tantas **Declaraciones** relacionadas con diversos aspectos de la COVID-19. La primera, aprobada a mediados de marzo, aclara las bases para la licitud del tratamiento de los datos personales en el contexto de la pandemia y tiene un formato de pregunta y respuesta.

El principal mensaje que contiene esta Declaración es que, aunque el derecho a la protección de datos no puede convertirse en un obstáculo para la adopción de las medidas de salud pública necesarias para evitar la expansión de la enfermedad, el contenido esencial del derecho deber ser respetado y el RGPD contiene previsiones lo suficientemente flexibles como para poderlo conciliar con los objetivos de salud pública perseguidos. Es interesante señalar que esta Declaración refleja de forma muy directa algunos de los criterios contenidos en el primer informe sobre protección de datos y COVID-19 publicado por la Agencia Española en marzo de 2020.

Una segunda **Declaración** se refiere a la restricción de los derechos de los interesados en conexión con el estado de emergencia de salud pública y se elaboró a petición de la autoridad de protección de datos de Hungría, con motivo de la suspensión de las garantías establecidas en el RGPD realizada por el Gobierno de Hungría, aprovechando la declaración del estado de emergencia.

Otras dos **Declaraciones**, aprobadas en el mes de junio, se centran en la interoperabilidad de las aplicaciones de seguimiento de contactos y en el tratamiento de los datos personales en el contexto de la reapertura de fronteras. La AEPD participó como co-ponente de esta última.

Junto con estas declaraciones, el Comité adoptó dos Directrices también relacionadas con la lucha contra la pandemia.

Las primeras de ellas fueron las *Directrices sobre el tratamiento de datos de salud para la investigación científica en el contexto de la pandemia de COVID-19*. Debido a la pandemia se pusieron en marcha con gran rapidez numerosos proyectos de investigación con el fin de obtener resultados lo más rápidamente posible tanto en el terreno de la prevención como en el del tratamiento de la enfermedad.

Las Directrices reiteran, una vez más, que las normas de protección de datos no entorpecen las medidas adoptadas para luchar contra la pandemia de COVID-19. El RGPD incluye distintas disposiciones que permiten gestionar el tratamiento de datos personales con fines de investigación científica relacionados con la pandemia de COVID-19 sin menoscabo de los derechos fundamentales a la privacidad y a la protección de los datos personales. El RGPD prevé una excepción específica a la prohibición del tratamiento de determinadas categorías especiales de datos personales, como los datos sanitarios, cuando sea necesario a esos fines de investigación científica. Asimismo, contiene previsiones suficientes como para atender a aspectos tales como la base jurídica para estos tratamientos, la aplicación de las garantías adecuadas, el ejercicio de los derechos de los interesados o las transferencias internacionales exigidas por los proyectos de investigación.

Las segundas de estas *Directrices se referían al uso de datos de localización y herramientas de seguimiento de contactos en el contexto de la COVID-19*. En el momento en que esas Directrices se adoptaron, los gobiernos y el sector privado estaban dirigiendo su mirada hacia el uso de soluciones tecnológicas basadas en los datos como parte de la respuesta a la pandemia de COVID-19, lo que planteaba muchos interrogantes desde el punto de vista de la privacidad.

En estas Directrices el CEPD manifiesta su convicción de que, en la medida en que el tratamiento de datos personales resulte necesario para la gestión de la pandemia de COVID-19, la protección de datos es imprescindible para generar confianza y sentar las condiciones para la aceptación social de cualquier solución y, así, garantizar la eficacia de las medidas adoptadas.

Las Directrices precisan las condiciones y los principios que deben guiar el uso proporcionado de datos de localización y de herramientas de rastreo de contactos. El CEPD es de la opinión de que el uso de aplicaciones de rastreo de contactos debe ser voluntario y no puede basarse en el rastreo de movimientos individuales, sino más bien en información sobre la proximidad de los usuarios. Asimismo, el Comité señaló la importancia de que

estas herramientas formen parte de un esquema más amplio de prevención y subrayó que su implantación, por sí misma, no puede constituir la solución a la pandemia.

Estas Directrices fueron una ampliación de la contribución que hizo el Comité a un documento de guía sobre uso de apps en la lucha contra la pandemia que la Comisión Europea publicó en abril de 2020. La Agencia Española participó como correectora en esa contribución.

En relación con el otro gran tema objeto de la atención del Comité durante 2020, las transferencias internacionales, en febrero de 2020 el Comité adoptó unas *Directrices sobre las transferencias de datos personales entre autoridades y organismos del Espacio Económico Europeo a los no pertenecientes a este Espacio*.

Las directrices se refieren a las transferencias internacionales de datos efectuadas con diversos fines de cooperación administrativa entre organismos públicos comprendidos en el ámbito del RGPD. En consecuencia, no cubren las transferencias en el ámbito de la seguridad pública, la defensa o la seguridad del Estado. Además, no se ocupan del tratamiento y las transferencias de datos por parte de las autoridades competentes con fines de aplicación de la ley penal, ya que éstas se rigen por su instrumento específico, la Directiva de Ámbito Penal 680/2016. Por último, las directrices se centran únicamente en las transferencias entre organismos públicos y no abarcan las transferencias de datos personales de un organismo público a una entidad privada o de una entidad privada a un organismo público.

Las Directrices tienen por objeto dar una indicación de las expectativas del Comité en cuanto a las garantías para las transferencias internacionales de datos entre organismos públicos. Estas garantías pueden ofrecerse mediante un instrumento jurídicamente vinculante y exigible entre organismos públicos o, previa autorización de la autoridad de supervisión competente, mediante disposiciones que deben insertarse en los acuerdos administrativos no jurídicamente vinculantes entre organismos públicos.

Sin embargo, fue la Sentencia Schrems II del Tribunal de Justicia la que motivó una más intensa actividad por parte del Comité.

Aunque el contenido de la Sentencia se detalla en el apartado de Transferencias internacionales de esta Memoria, cabe repetir aquí que en ella el Tribunal analiza las obligaciones de importadores y exportadores en el marco de las CCT y destaca que es responsabilidad del exportador valorar la posible presencia de esas disposiciones de la legislación del país de destino que impidan al importador cumplir con sus obligaciones en el marco de las cláusulas y, en caso de que existan, aplicar medidas complementarias que permitan asegurar el nivel de protección. Si no pueden encontrarse medidas suplementarias que permitan alcanzar ese fin, el exportador debe suspender la transferencia o, si pretende seguir realizándola, notificarlo a la autoridad de supervisión, que tomará las medidas que considere oportunas.

El Comité emitió una Declaración sobre la Sentencia Schrems II muy poco después de su adopción y, posteriormente, publicó unas Preguntas Frecuentes (FAQ, por sus siglas en inglés) sobre la misma. En esas FAQ se ofrecía la interpretación del Comité sobre el contenido de la Sentencia y sus implicaciones para las transferencias internacionales, tanto a EEUU como a otros países terceros. Al mismo tiempo, el Comité se comprometía a apoyar a los exportadores de datos en la identificación de las posibles medidas suplementarias para esos casos en que la legislación del país de destino impida al importador cumplir con sus obligaciones con arreglo a las cláusulas contractuales y, con las variaciones apropiadas, en el marco de otros instrumentos de transferencia.

Con este objetivo se aprobaron en el mes de noviembre las *Recomendaciones sobre medidas*

*que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE*.<sup>4</sup>

Las Recomendaciones indican a los exportadores una serie de pasos a seguir, posibles fuentes de información y algunos ejemplos de medidas complementarias que podrían implementarse. Como primer paso, el CEPD aconseja a los exportadores que mapeen e identifiquen adecuadamente todas sus transferencias. Un segundo paso es verificar el instrumento de transferencia que utiliza. En ausencia de una decisión de adecuación, debe confiar en una de las herramientas de transferencia enumeradas en los artículos 46 del RGPD para las transferencias que son regulares y repetitivas. Un tercer paso es evaluar si hay algo en la legislación o la práctica del tercer país que pueda afectar la eficacia de las salvaguardias adecuadas de las herramientas de transferencia en el contexto de su transferencia específica. El cuarto paso es identificar y adoptar las medidas complementarias que son necesarias para llevar el nivel de protección de los datos transferidos al estándar de la UE de equivalencia esencial.

Las Recomendaciones contienen ejemplos (la lista no es exhaustiva) de medidas complementarias con algunas de las condiciones que necesitarían para ser eficaces. Estas medidas son de carácter tecnológico, organizativo o legales. En las propias recomendaciones se indica que es posible que el exportador concluya que ninguna medida complementaria, o que ninguna combinación de ellas, puede garantizar un nivel de protección esencialmente equivalente para su transferencia específica. En esos casos, se insta al exportador a dar cumplimiento a las previsiones del RGPD y de las propias CCT y suspender o dar por terminada la transferencia para no comprometer el nivel de protección de los datos personales.

También en relación con la Sentencia Schrems II, y en la misma fecha que las anteriores *Recomendaciones*, el Comité adoptó las *Recomendaciones sobre Garantías Esenciales Europeas para medidas de vigilancia*. Estas Recomendaciones son una actualización de otras ya aprobadas por el Comité (entonces GT29) después de la primera Sentencia Schrems.

---

<sup>4</sup> Esta versión es la adoptada en el mes de noviembre, que fue objeto de un periodo de consulta pública. La adopción definitiva, teniendo en cuenta las más de 200 contribuciones recibidas, se espera para el segundo trimestre de 2021

En aquella Sentencia el TJUE invalidó el esquema del “Puerto Seguro” para transferencias a EEUU y el GT29 elaboró su documento, basado en la jurisprudencia de los Tribunales europeos, para identificar las “Garantías Esenciales Europeas” que deben respetarse para asegurar que las injerencias sobre los derechos a la privacidad y la protección de los datos personales transferidos a un país tercero a través de medidas de vigilancia no vayan más allá de lo necesario y proporcionado en una sociedad democrática.

A raíz de la Sentencia Schrems II, el CEPD decidió que sería adecuado actualizar esas Garantías Esenciales Europeas para reflejar nuevos contenidos de la Sentencia, así como los de otras decisiones tanto del TJUE como del Tribunal Europeo de Derechos Humanos aparecidas después de la publicación del primer documento.

El objetivo de las Recomendaciones actualizadas es proporcionar una lista de elementos para examinar si las medidas de vigilancia que permiten el acceso a datos personales por parte de autoridades públicas en un tercer país pueden considerarse una interferencia justificable o no. De hecho, las Garantías Esenciales Europeas forman parte de la evaluación a realizar para determinar si un tercer país proporciona un nivel de protección esencialmente equivalente al garantizado dentro de la UE, aunque no son, por sí solas, suficientes para definir todos los elementos que es necesario considerar para concluir que un tercer país ofrece ese nivel de protección.

En este mismo terreno de las transferencias internacionales el Comité ha emitido diversos

**documentos en preparación del Brexit.** Como se recordará, el periodo transitorio en el que el derecho de la Unión en materia de protección de datos se seguía aplicando en Reino Unido finalizó el 31 de diciembre de 2020.

La definitiva salida del Reino Unido tiene una consecuencia obvia, como es que las comunicaciones de datos desde la Unión Europea al Reino Unido pasan a ser transferencias internacionales y han de atenerse a las reglas que al efecto establece el RGPD. No obstante, esa cuestión quedó momentáneamente resuelta a partir de la extensión del periodo transitorio hasta junio de 2021 en el ámbito de la protección de datos a la espera de que la Comisión adopte decisiones de adecuación (en el ámbito del RGPD y de la Directiva de Ámbito Penal) que permitan mantener los flujos de datos hacia el Reino Unido.

Sin embargo, hay otras cuestiones prácticas, como son la gestión de las Normas Corporativas Vinculantes en que la sede principal de la corporación se encuentra en Reino Unido, por lo que la autoridad de supervisión británica juega el papel de autoridad de contacto y tiene unas obligaciones específicas como tal, o la resolución de procedimientos sancionadores en el marco del mecanismo de cooperación en que la autoridad británica es autoridad principal.

Es sobre estas cuestiones sobre las que se ha pronunciado el Comité a través de varias declaraciones y notas informativas en que ha establecido las condiciones para resolver los problemas derivados de la salida de la Unión del Reino Unido<sup>5</sup>.

---

<sup>5</sup> “Information note on BCRs for Groups of undertakings / enterprises which have ICO as BCR Lead SA”, accesible, solo en versión inglesa, en [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_informationnoteforgroupswithicoasbcrleadsa\\_20200722\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_informationnoteforgroupswithicoasbcrleadsa_20200722_en.pdf); “Information note on data transfers under the GDPR to the United Kingdom after the transition period”, accesible, solo en versión inglesa, en [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_informationnote\\_20201215\\_transferstoukaftertransitionperiod\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_informationnote_20201215_transferstoukaftertransitionperiod_en.pdf); “Statement on the end of the Brexit transition period”, accesible, solo en versión inglesa, en [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_statement\\_20201215\\_brexit\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_20201215_brexit_en.pdf). Estos dos últimos documentos han sido reemplazados por otros adoptados en enero de 2021 en los que se tiene en cuenta el acuerdo alcanzado entre la UE y el Reino Unido para la prolongación del periodo transitorio. En todo caso, todos estos documentos son continuación de otros anteriores, adoptados a lo largo de 2018 y 2019, tanto ante la eventualidad de que se produjera un Brexit sin acuerdo como para aclarar la situación durante el periodo transitorio.

Aparte de estos dos grandes temas en los que se ha centrado buena parte de la actividad del Comité en 2020, se han adoptado también otros documentos de interés.

El primero de ellos, atendiendo al orden de aprobación, fueron las *Directrices sobre el tratamiento de datos personales en el contexto de vehículos conectados y aplicaciones relacionadas con la movilidad*.

Hoy en día, los vehículos se están convirtiendo en centros de datos masivos. Y no son sólo los vehículos, sino también los conductores y los pasajeros quienes están cada vez más conectados. Las directrices del CEPD se centran en particular en el tratamiento que el uso no profesional de los vehículos conectados puede implicar para una variedad de interesados: conductores, pasajeros, propietarios de vehículos, arrendatarios, etc. Más concretamente, se trata de los datos personales **i)** tratados dentro del vehículo, **ii)** intercambiados entre el vehículo y los dispositivos personales conectados a él (por ejemplo, el teléfono inteligente del usuario) o **iii)** recogidos dentro del vehículo y exportados a entidades externas (por ejemplo, fabricantes de vehículos, administradores de infraestructuras, compañías de seguros, talleres de reparación de automóviles) para su posterior tratamiento.

Las Directrices analizan cuestiones tales como la legislación aplicable (teniendo en cuenta que en ocasiones el vehículo puede actuar como un dispositivo en el que se almacena y del que se obtiene información, estando sujeto, por tanto, a la Directiva 2002/58) y los riesgos en términos de protección de datos que el uso de estos vehículos, en las distintas facetas que se han señalado más arriba, pueden tener para las personas, ofreciendo recomendaciones para hacer frente a esos riesgos.

El Comité ha actualizado también las *Directrices sobre consentimiento* en el ámbito del RGPD que, en su momento, adoptó el GT29. El CEPD decidió modificar estas directrices, inicialmente aprobadas por el GT29, debido a la publicación de varias guías sobre consentimiento y cookies por parte de diversas autoridades, entre ellas la AEPD.

El objetivo perseguido con esta modificación era armonizar la interpretación sobre las condiciones en las que se debía prestar el consentimiento para el tratamiento de las cookies, en cumplimiento de la Directiva sobre la privacidad y las comunicaciones electrónicas (Directiva e-privacy) y el RGPD.

La modificación se limitó a dos partes diferenciadas, una relativa a los conocidos como muros de cookies, que impiden el acceso al contenido de una web con el único fin de conseguir la aceptación del tratamiento de cookies. La segunda modificación afecta a uno de los ejemplos del texto. En la nueva redacción se deja claro que, en ninguna circunstancia, la opción “seguir navegando” puede considerarse una forma válida de obtener el consentimiento. Este segundo cambio afectó directamente a la guía de cookies aprobada por la AEPD, que fue revisada en línea con el contenido de las Directrices.

El pasado año fue también publicada una actualización de las *Directrices sobre los conceptos de responsable y encargado*, que adapta al marco del RGPD el dictamen aprobado en 2010 por el GT29.

Dado el carácter central que las nociones de responsable, encargado y corresponsables tienen en el sistema de protección del RGPD, la aprobación de estas nuevas Directrices era esperada con gran interés y ha sido el resultado de un trabajo de casi dos años en el seno del Comité.

Cabe decir que en lo relativo a las nociones de responsable y encargado las Directrices no se separan de la posición del GT29 en su dictamen original, si bien, y dado que el RGPD establece obligaciones específicas para encargados, así como disposiciones sobre el contenido de los contratos que deben regir las relaciones entre responsables y encargados, se han añadido nuevos contenidos relacionados con esas materias.

Donde sí hay diferencias significativas es en el apartado relativo a corresponsables, dado que, aunque esta posición legal sí estaba recogida en la Directiva 95/46, su desarrollo en la práctica había sido mucho más limitado que el que ha venido determinado tanto por el RGPD como por la jurisprudencia del Tribunal de Justicia de la UE (TJUE).



Algunas conclusiones destacadas que pueden encontrarse en las Directrices serían las siguientes:

- La corresponsabilidad requiere la participación conjunta de dos o más entidades en la determinación de los fines y medios. La participación conjunta puede tomar la forma de una decisión común tomada por dos o más entidades o resultar de decisiones convergentes de dos o más entidades en relación con los propósitos y medios esenciales.
- Los corresponsables pueden tratar datos con el mismo fin o con fines estrechamente vinculados o complementarios.
- El uso de un sistema técnico ya existente no excluye el control conjunto cuando las entidades que utilizan el sistema pueden decidir sobre los fines y los medios de tratamiento de datos personales que se realizarán en este contexto.
- Si un encargado ofrece un servicio definido previamente (por ejemplo, un importante proveedor de servicios en la nube), el responsable debe tomar la decisión final para aprobar activamente la forma en que se lleva a cabo el tratamiento y / o poder solicitar cambios si es necesario.

Las Directrices se han sometido a un periodo de consulta pública, ya finalizado, y su adopción definitiva, una vez valoradas las contribuciones recibidas, se espera para el primer trimestre de 2021.

Junto con las anteriores, el Comité aprobó también *Directrices sobre la interacción entre la Segunda Directiva sobre Servicios de Pago (PSD2) y el RGPD*, en las que se pretende proporcionar orientación y asistencia interpretativa en relación con la aplicación del RGPD en el contexto de la prestación de los nuevos servicios de pago previstos en la Directiva. En este sentido, hay que tener en cuenta que una característica importante de la PSD2 es que introduce un marco jurídico para los nuevos servicios de iniciación de pagos y también de información de cuentas, permitiendo a los nuevos proveedores de servicios de pago obtener

acceso a las cuentas de pago de los interesados y, consecuentemente, participara en tratamientos de los datos asociados tanto a las cuentas como a los servicios que se ofrecen.

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

En este ejercicio se ha dado continuidad al desarrollo del marco normativo de supervisión de la protección de datos en la Unión Europea en el ámbito de los sistemas IT de Cooperación Policial y judicial del Espacio de libertad Seguridad y Justicia. Este marco se había abordado hasta fechas recientes desde la perspectiva de la cooperación entre los Estados Miembros mediante un enfoque de peer review o revisión entre pares.

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

Esas agencias o grandes sistemas integran intercambios de datos personales entre las autoridades nacionales participantes, usando una infraestructura europea e.g Europol, o entre esas autoridades entre sí y con una instancia central europea, como es el caso de la agencia europea (Eu-LISA) Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia. Cada uno de

estos sistemas tiene su propio marco normativo, que designa una autoridad común o conjunta de control de protección de datos encargada de la supervisión del sistema IT.

Estas autoridades conjuntas tienen distintos formatos, denominaciones y reglas de procedimiento. Tradicionalmente, el modelo era el de “autoridades conjuntas de control”, que ha ido evolucionando paulatinamente a la figura de los “grupos de supervisión coordinada”.

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

En 2018 se aprobó el Reglamento UE/2018/1725, que regula la protección de datos en el ámbito de las instituciones, agencias y organismos de la Unión, reemplazando al anterior Reglamento UE/45/2001. El nuevo Reglamento establece que la supervisión de los distintos sistemas IT se habrá de llevar a cabo “en el marco” del Comité europeo de Protección de Datos. Para dar paso a este sistema al amparo de comité se ha creado el nuevo “Comité de la Supervisión de la Coordinación” que debería sustituir a las distintas autoridades conjuntas en un futuro próximo.

Un nuevo hito en la evolución y desarrollo del nuevo sistema de supervisión ha tenido lugar en Eurojust, donde el pasado diciembre de 2019 se produjo del traspaso de poderes de la supervisión del sistema por parte del Grupo de Supervisión Conjunta de Eurojust al Supervisor Europeo de Protección de Datos. La supervisión de la protección de datos se ha incorporado en 2020 al nuevo Comité de Coordinación de la Supervisión.

En diciembre de 2019, fueron aprobadas las normas de procedimiento del nuevo Comité de Coordinación Supervisión que habrá de sustituir a los diferentes grupos de supervisión de la coordinación de los sistemas IT del SIS de visados, del SIS II (Sistema Schengen II) y del JAS y CIS de Aduanas (Sistemas de Información Conjunta y Sistema de Información de Aduanas) y del extinto Órgano de Supervisión Conjunta de Eurojust y del Comité de Supervisión de Europol. Hasta la fecha se han producido dos reuniones del nuevo Comité para tratar la supervisión de dos de los Sistemas IT pertenecientes al sistema, el sistema de Información del Mercado Interior (IMI) y el sistema IT Eurojust.

Por otra parte, el ejercicio 2020 ha continuado del desarrollo del nuevo modelo de interoperabilidad de los sistemas con la continuación de la implantación del Portal de Europeo Búsquedas. El modelo ha visto la incorporación de instrumentos normativos que modifican las autoridades conjuntas y los marcos normativos del ámbito de Cooperación Policial y Judicial y que se enmarcan en una nueva iniciativa de la Comisión Europea: el llamado Pacto por la Inmigración y Asilo.

Esta iniciativa introduce un nuevo instrumento legislativo, el Reglamento Europeo de Screening. Queda por definir el modelo de participación del Comité en esta futura supervisión conjunta del resto de los sistemas del conjunto que está suponiendo la reforma de los actuales Reglamentos sectoriales que gobiernan cada uno de los sistemas de información de cooperación policial y judicial por el colegislador europeo, así como la creación de nuevos instrumentos jurídicos, como el ya mencionado Reglamento UE de Screening, cuyos conjuntos de datos se incorporan al sistema SIS II. Este modelo de supervisión supone la reforma de los distintos Reglamentos EU de cada uno de los antiguos sistemas ya mencionados y la aprobación de los distintos marcos legislativos para nuevos sistemas como el “Entry, Exit System” o “Sistema de Entrada y Salida” y el ETIAS.

Este conjunto de instrumentos informáticos integrados en una nueva plataforma de tres capas integra un identificador de identidades múltiples, un programa de emparejamiento biométrico y un repositorio común de identidades. Este sistema, que incorpora datos biométricos alfanuméricos, permitirá la detección e identificación de las personas que se presentan varias identidades bajo unos mismos datos biométricos, por ejemplo, huellas dactilares. Además, se encuentran en desarrollo los Sistemas de Entrada Salida Europeo (EES) y ETIAS (para los viajeros exentos de visado con destino a la UE), que se prevé sean integrados también en el nuevo sistema de interoperabilidad.

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

Por último, el sistema de interoperabilidad se ha visto afectado por la agregación del mencionado Pacto sobre Inmigración y Asilo. Este marco pretende “aumentar la confianza y crear un nuevo equilibrio entre responsabilidad y solidaridad en el ámbito de la Migración y Asilo”.

Se desarrolla en 6 ejes:

- Procedimientos rápidos y eficaces.
- Espacio Schengen y fronteras exteriores bien gestionados.
- Solidaridad efectiva.
- Capacidades y talentos.
- Profundizar en las asociaciones internacionales.
- Flexibilidad y resiliencia.

El nuevo sistema de inmigración y asilo pretende “responsabilidades más claras gracias a procedimientos mejores y modernizados” en cada uno de sus ejes. Se pretende restablecer la confianza entre los Estados miembros y aportar claridad a los solicitantes de asilo y mejorar los procedimientos de asilo y retorno. Se incorpora un “nuevo y más rápido procedimiento fronterizo de asilo y, en su caso, seguido de un procedimiento de retorno rápido, para acelerar la toma de decisiones y aumentar la eficiencia de los procedimientos de asilo”. Ello supone un nuevo control obligatorio previo y se incorporan novedades que afectarán a los distintos sistemas IT de Cooperación Policial y judicial.

La Agencia Española ha participado en todas las reuniones de los grupos coordinados de supervisión celebradas en 2020, así como en las del Comité de Supervisión Coordinada establecido en el marco del CEPD. En este contexto, realiza el seguimiento del desarrollo tanto de las actividades de las agencias europeas y grandes sistemas de información mencionados anteriormente como de la evolución normativa que se ha descrito anteriormente.

Debe señalarse también que la Agencia ha participado en tres evaluaciones Schengen durante 2020. 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 Bélgica, Lituania y Alemania.

## 10.3. Participación de la AEPD en otros foros internacionales

### 10.3.1. Comité Consultivo de la Convención 108 del Consejo de Europa

La AEPD 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 la nueva 108+ Convención para la protección de datos personales del Consejo de Europa.

La Agencia desarrolla en el marco del Comité Consultivo entre otros los trabajos para la redacción del nuevo Referencial de adecuación para la validación de los candidatos a miembros de la Convención y para los procesos de reevaluación de Estados miembros y Observadores que se lleva a cabo cada seis años. En colaboración con los expertos del Comité Consultivo y de la Universidad de Notre Dame de Namur, la AEPD ha venido participando en este ejercicio como miembro del equipo de redacción del nuevo Referencial.

En este marco la AEPD ha participado además en los trabajos sobre las recomendaciones del Consejo relativas a los tratamientos de reconocimiento facial, sobre tratamientos de datos de datos para perfilados y decisiones automatizadas y sobre tratamientos de datos relativos a los niños en los sistemas educativos.

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).



## 11. La cooperación con Iberoamérica

Además de las actividades que se describen en otros apartados de la Memoria 2020, la red Iberoamericana de Protección de Datos (RIPD), en la que la Agencia Española de Protección de Datos ostenta la Secretaría Permanente, ha desarrollado las que se describen a continuación.

### 28 enero

---

Día Internacional de la Protección de Datos. *“La revolución digital de nuestra era ¿una oportunidad para la economía global?”*. Taller *“La Interdependencia Digital y la Protección de Datos Personales”*. Eventos organizados por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales de México (INAI) y el Instituto de Acceso a la Información Pública y Protección de Datos Personales de la Ciudad de México (INFOCDMX). Lugar de celebración: Ciudad de México.

La AEPD, a través de la División Internacional, asistió presencialmente como ponente en ambos eventos, junto con representantes de la Comisión Europea, de otras Autoridades iberoamericanas, del INAI e INFOCDMX y expertos y especialistas de México.

### 29 abril

---

Seminario virtual “Pandemia mundial y enfermedad de datos personales”. Organiza: Consejo para la Transparencia de Chile.

La AEPD, a través del Coordinador de la Unidad de Apoyo y Relaciones Institucionales, participó como ponente, junto con los presidentes del INAI de México, de la CNIL de Francia y del Consejo para la Transparencia de Chile. En dicho debate se expusieron las actuaciones realizadas por la AEPD con ocasión de la pandemia COVID-19.

### 1 junio

---

Charla virtual (Webinario). “Protección de datos Personales: innovación y gestión durante y después de la pandemia”. Organiza: Organización de Estados Americanos.

La AEPD, a través del Director de la División de Innovación y Tecnología, intervino como ponente en el Panel “Protección de Datos Personales y COVID-19: ¿en dónde estamos?”.

### 2 junio

---

Reunión (virtual) del Grupo Permanente de Autoridades Nacionales de Protección de Datos (GPAN), sobre actuaciones de las Autoridades iberoamericanas de Protección de Datos en relación con la COVID-19.

Asistieron a dicho foro las Autoridades nacionales de Argentina (AAIP), Chile (CpT), Colombia (SIC), Costa Rica (PRODHAB), España (AEPD), México (INAI), Perú (ANPD), Portugal (CNPD) y Uruguay (URCDP). El objetivo principal era intercambiar información sobre las actuaciones llevadas a cabo por cada una de las nueve Autoridades en relación con la pandemia, especialmente las actuaciones de investigación.

Por parte de la AEPD, asistieron la Directora, el Coordinador de la Unidad de Apoyo y Relaciones Institucionales, el Director de la División Internacional, el Director de la División de Innovación y Tecnología, el Abogado del Estado-Jefe del Gabinete Jurídico y el Vocal Asesor responsable de la Secretaría Permanente de la RIPD.



## 18 junio

---

Webinario “Privacidad: perspectivas de América Latina y la UE en tiempos de COVID-19”. Organiza: Centro para la Evaluación de Políticas basada en la Evidencia (CEPE) de la Escuela de Gobierno de la Universidad Torcuato Di Tella, Argentina, dentro del Ciclo de charlas: "Pensando la pospandemia". Por parte de la AEPD, intervino como ponente el Coordinador de la Unidad de Apoyo y Relaciones Institucionales.

## 24 junio

---

Taller (virtual) sobre la Ley de Protección de Datos de Jamaica. Organiza: Banco Interamericano de Desarrollo.

En el Taller participan, por parte de Jamaica, la Ministra de Energía, Ciencia y Tecnología, y su equipo directivo, y, por parte de la Red Iberoamericana de Protección de Datos, el Director de la División Internacional de la AEPD, junto con representantes del área de relaciones internacionales del INAI de México y de la CNPD de Portugal.

## 11 julio

---

Acto de clausura (virtual) del Diplomado de Datos Personales. Universidad Libre de Derecho (México).

En el evento participó, por parte de la AEPD, el coordinador de la Unidad de Apoyo y Relaciones Institucionales, junto con las Autoridades de Protección de Datos de Colombia, Uruguay, México y Argentina y la FTC norteamericana.

## 24 julio

---

Webinario sobre el anteproyecto de ley de protección de datos personales, organizado por la Coalición de Datos Personales de Paraguay.

Por parte de la AEPD, en calidad de Secretaría Permanente de la RIPD, participó el Vocal Asesor de la Unidad de Apoyo, junto con el Superintendente Delegado de Protección de Datos Personales de la SIC de Colombia.

## 26 agosto

---

Evento 2020 sobre Protección de Datos y Salud, organizado por la Unidad Reguladora y de Control de Datos Personales de Uruguay.

Por parte de la AEPD, participó como ponente el Coordinador de la Unidad de Apoyo y Relaciones Institucionales, con una ponencia que llevaba por título “La reutilización de datos sensibles”.

## 3 septiembre

---

Webinario “Extraterritorialidad y la cooperación internacional en Iberoamérica: situación actual y perspectiva futura”, organizado por la Asociación Latinoamericana de Privacidad (ALAP).

Por parte de la AEPD, en calidad de Secretaría Permanente de la RIPD, asistió el Vocal Asesor de la Unidad de Apoyo, junto con el Director de la Agencia de Acceso a la Información Pública de Argentina, el Secretario de Protección de Datos del INAI de México, y el Coordinador de Protección de Datos de la Unidad Reguladora y de Control de Datos de Uruguay.

## 26 octubre

---

Reunión con la Secretaria Ejecutiva de la Comisión Interamericana de la Mujer de la Organización de Estados Americanos.

Se celebró dicha reunión en el marco del proyecto sobre “Fortalecimiento de la Estrategia de lucha contra la violencia de género contra niñas, adolescentes y mujeres en internet”, financiado por el programa Eurosocial+ de la Unión Europea, en el que participan el INAI y la AEPD, como socios líderes, las Autoridades de Protección de Datos de Colombia (SIC), Perú (ANPD), Uruguay (URCDP), Costa Rica (PRODHAB) y Portugal (CNPD), y los Institutos de Transparencia y Protección de Datos del Estado de México (INFOEM) y de la Ciudad de México (INFOCDMX). Por parte de la AEPD, participó la Directora y el Vocal Asesor de la Unidad de Apoyo.

## 28 octubre

---

Foro (virtual) organizado por la Asociación Latinoamericana de Privacidad (ALAP). Ciclo “Privacy Café”. La importancia de la formación profesional: la experiencia española.

Por parte de la AEPD, intervinieron el Vocal Asesor de la Unidad de Apoyo y responsable de la Secretaría Permanente de la RIPD; la Jefa del Área de Certificación, y un miembro de la División de Innovación y Tecnología.

## 10 noviembre

---

Ciclo de Webinarios “La gobernanza de los flujos de datos y el comercio”, organizado por la Organización Mundial del Comercio.

Por parte de la AEPD y en representación de la RIPD, intervino el Director de la División Internacional en el Panel titulado “Diferentes modelos para facilitar el intercambio transfronterizo de datos personales”.

## 10 noviembre

---

Webinario “La protección de datos personales y su formación especializada”, organizado por la Asociación Iberoamericana de Protección de Datos y Ciberseguridad (AIPyC).

Por parte de la AEPD, intervinieron el Vocal Asesor de la Unidad de Apoyo y responsable de la Secretaría Permanente de la RIPD; la Jefa del Área de Certificación, y un miembro de la División de Innovación y Tecnología.

## 11 noviembre

---

Taller (virtual) de apoyo a la aplicación de la Ley 81, de 2019 (entrada en vigor, el 29/3/2021) sobre Protección de Datos Personales de Panamá, organizado por la RIPD, la Autoridad Nacional de Transparencia y Acceso a la Información Pública de Panamá (ANTAI), y el Banco Interamericano de Desarrollo (BID).

Por parte de la AEPD, intervino el Vocal Asesor de la Unidad de Apoyo, junto con la Directora de la ANTAI, el Director de la Autoridad Nacional de Protección de Datos de Perú, la Directora de la Agencia de Protección de Datos de Costa Rica (PRODHAB), y el Superintendente Delegado de Protección de Datos de Colombia.

## 19 noviembre

---

Taller (virtual) sobre aplicación práctica del derecho al olvido, organizado por la AEPD, en calidad de Secretaría Permanente de la RIPD.

Dicho Taller fue impartido por el Coordinador de la Unidad de Apoyo y Relaciones Institucionales de la AEPD, para 60 empleados y empleadas de las Autoridades Iberoamericanas miembros de la RIPD.

## 26 noviembre

---

Webinario “El Canal Prioritario de la AEPD: una contribución de las Autoridades de Protección de Datos a la lucha contra la violencia digital en las mujeres, niñas y adolescentes”, organizado por el Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales de México (INAI).

Dicho evento se enmarca dentro de las actividades del proyecto sobre “Fortalecimiento de la Estrategia de lucha contra la violencia de género contra niñas, adolescentes y mujeres en internet”, financiado por el programa Eurosocial+ de la Unión Europea. El acto, que fue presentado por la Comisionada del INAI, Josefina Román, tuvo como ponentes a la Directora de la Agencia y a la Subdirectora General de Inspección de Datos.

El evento contó con una amplia participación, especialmente de las Autoridades socios del proyecto, del resto de Autoridades de la RIPD y de autoridades de México.

## 4 diciembre

---

XVIII Encuentro Iberoamericano de Protección de Datos (Sesión Cerrada). Organización: Unidad Reguladora y de Control de Datos Personales de Uruguay. Plataforma: Zoom.

Participaron en dicho Encuentro las entidades que integran la RIPD, que en la actualidad son treinta y cuatro, desglosadas en 16 Miembros (Autoridades) y 18 Observadores, nacionales e internacionales.

Intervinieron también como invitados, entre otros, una representación de la Autoridad Nacional de Protección de Datos de Brasil, del Banco Interamericano de Desarrollo (BID), de la Unidad de Protección de Datos y Flujos Internacionales de la Comisión Europea, del Foro de la Sociedad Civil de la RIPD, del programa Eurosocial+, de la Secretaría General Iberoamericana (SEGIB) y la relatora de Protección de Datos Personales del Comité Jurídico Interamericano de la OEA.

El programa se estructuró en tres partes: una primera, de carácter fundamentalmente informativo, abierta a invitados, para exponer las actuaciones más significativas de la RIPD durante el último año (estado de los desarrollos legislativos, estado de las relaciones con la OEA, información sobre el borrador de orientaciones RIPD sobre computación en la nube, y sobre el proyecto de lucha contra la violencia digital en mujeres, niñas y adolescentes). Terminada esta primera parte de la sesión cerrada, impartió una conferencia la Doctora Carmela Troncoso, sobre las apps de seguimiento y rastreo de contactos en el contexto de la pandemia, presentada por la Directora de la AEPD. En la segunda parte de la sesión cerrada, ya sólo para Miembros y Observadores, como puntos más destacados, se aprobó el nuevo Plan Estratégico de la RIPD 2021-2025, se comunicó la acreditación del Consejo de Transparencia y Protección de Datos de Andalucía y la Autoridad Nacional de Transparencia y Acceso a la Información de Panamá como nuevos Miembros de la RIPD, así como de la Comisión Estatal de Garantía de Acceso a la Información Pública de San Luis Potosí (CEGAIP) en calidad de Observador. Finalmente, se designó la nueva Presidencia de la RIPD para el período 2021-2022, que recayó por unanimidad en la Superintendencia de Industria y Comercio de Colombia (SIC), y, como consecuencia de la crisis de COVID-19, se acordó prorrogar el mandato del Comité Ejecutivo y aplazar la designación de la sede del XIX Encuentro hasta que cambien las circunstancias actuales derivadas de la pandemia.

En representación de la AEPD, como Secretaría Permanente de la RIPD, asistieron al Encuentro la Directora, el coordinador de la Unidad de Apoyo y Relaciones Institucionales y el Vocal Asesor de la Unidad de Apoyo.

## 15 diciembre

---

5º Foro Internacional (online) “Protección de Datos y Acceso a la Información”. Organizado por el INFOEM (Estado de México).

La Directora de la Agencia clausuró dicho evento, que tenía por objeto debatir y analizar los desafíos y oportunidades en materia de protección de datos personales en tiempos post COVID-19.



# **LA AGENCIA EN CIFRAS**

## 1. Marco de Responsabilidad Social y Sostenibilidad

### Grado de cumplimiento del plan RSC (2019-2020)

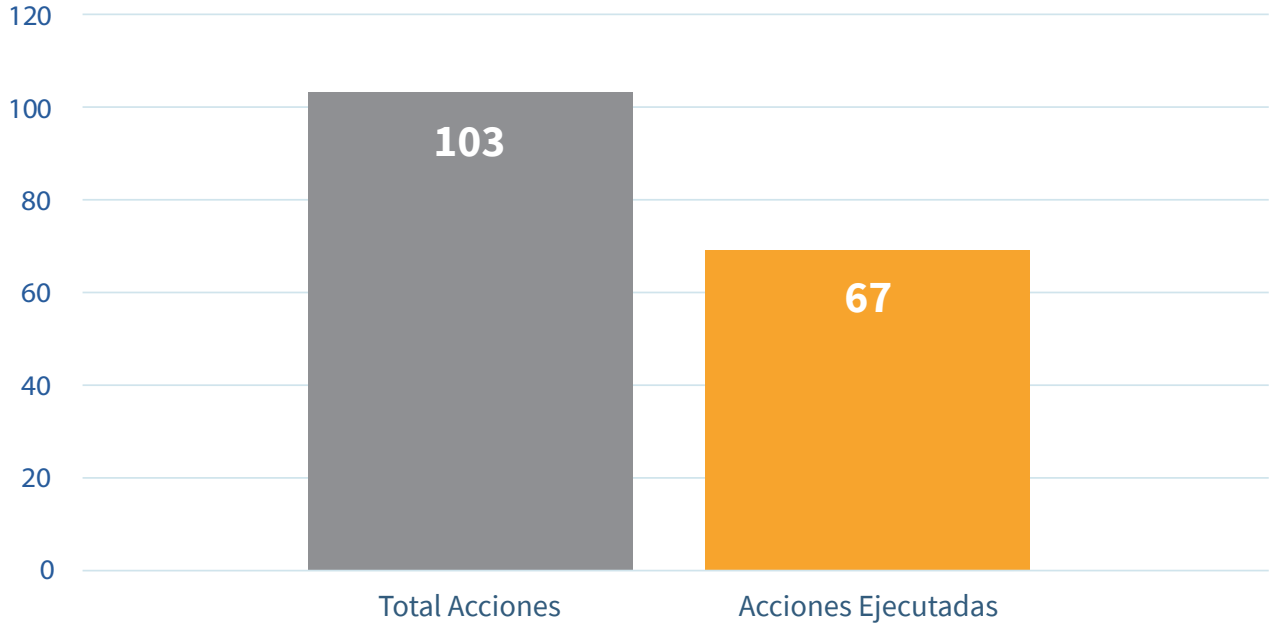
Acciones totales del plan	103
Acciones cumplidas, total o parcialmente, durante el periodo 2019-2020	67
Nivel de cumplimiento (Periodo 2019-2020) sobre el total del plan (Periodo 2019-2024)	65%

### Grado de cumplimiento del plan RSC por ejes (Periodo 2019-2020)

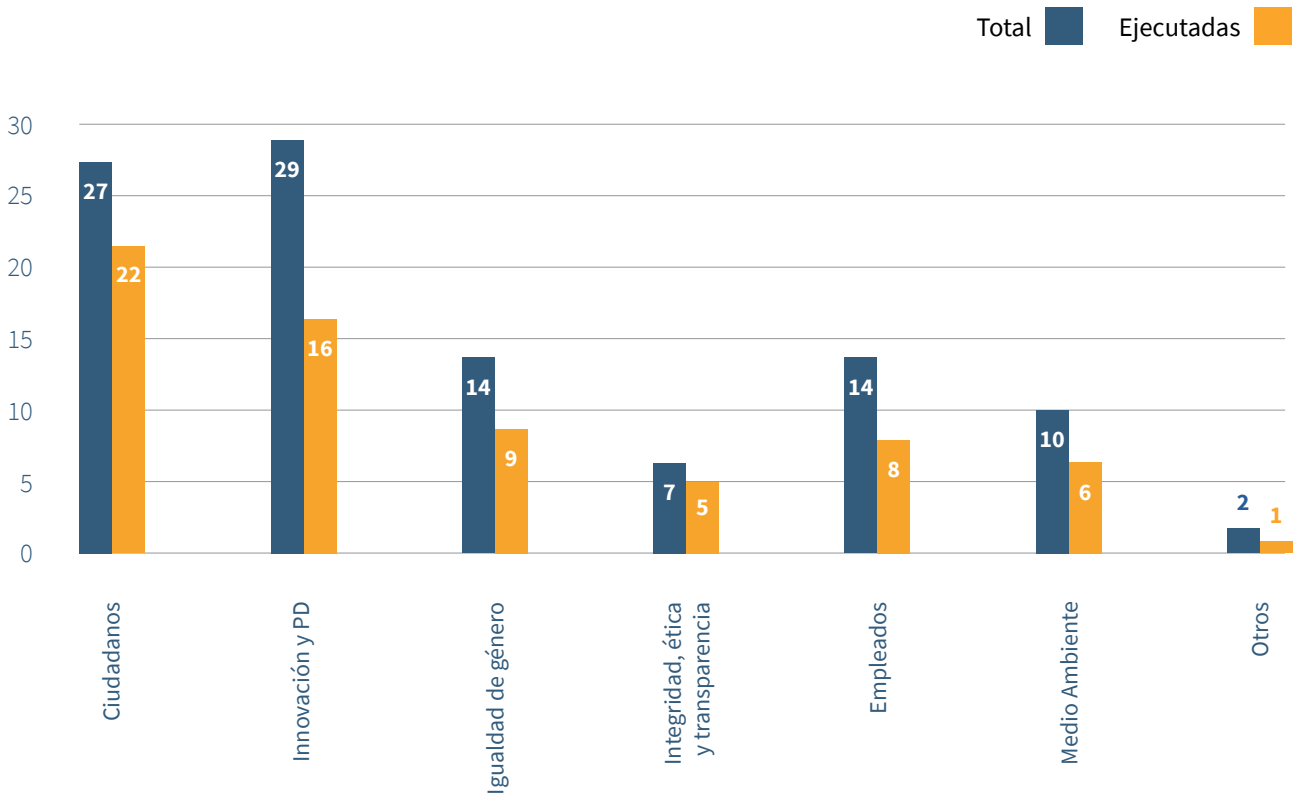
	Total acciones (2019-2024)	Acciones ejecutadas	%
Compromisos con los ciudadanos	27	22	82%
Innovación y protección de datos	29	16	55%
Igualdad de género	14	9	65%
Ética, integridad pública y transparencia	7	5	70%
Empleado	14	8	57%
Medio ambiente y cambio climático	10	6	60%
Otros	2	1	50%
<b>TOTAL</b>	<b>103</b>	<b>67</b>	<b>65%</b>



### Grado de cumplimiento Global (Periodo 2019-2020)



### Grado de cumplimiento Ejes (Periodo 2019-2020)



## 2. Inspección de datos

### 1. El inicio de la potestad de supervisión. Reclamaciones, comunicaciones y actuaciones por iniciativa propia

La Subdirección General de Inspección de Datos (SGID, en adelante), es el órgano dependiente de la Directora de la Agencia, que, en caso de posible vulneración de la normativa o de no atención al ejercicio de derechos, analiza los indicios, realiza las actuaciones de tutela o 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 plantearse directamente ante la Agencia, que es la situación más frecuente, aunque también pueden llegar a través de alguna Autoridad de Control 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 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 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 planes sectoriales y auditorías preventivas previstas en la normativa, cuyo objetivo es dictar directrices que sirvan de guía en el cumplimiento de lo establecido reglamentariamente.

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, en los casos en los que resulta 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 únicamente aquellas en las que la DIT determina que procede su evaluación y posible investigación por parte de la Subdirección General de Inspección de Datos.

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

Tipo de entrada	2019	2020	% relativo	Δ% anual
Reclamaciones presentadas en la AEPD	11.590	10.324	91%	-11%
Casos transfronterizos procedentes de otras AC del EEE	790	784	7%	-1%
Propia iniciativa de la AEPD (excl. brechas)	15	26	0%	73%
Notificaciones de brechas de seguridad trasladadas a la SGID	79	81	1%	3%
<b>TOTAL</b>	<b>12.474</b>	<b>11.215</b>	<b>100%</b>	<b>-9%</b>

En 2020 la tasa de reclamaciones resueltas frente a reclamaciones recibidas ha aumentado un 5% respecto al año anterior. Cabe destacar esta mejora de la productividad en la resolución de reclamaciones, sobre todo si se tiene en cuenta la situación de emergencia sanitaria y de confinamiento y el empleo del teletrabajo como modo habitual de prestación de servicios. Este indicador consolida la mejora de productividad que se ha venido observando con la implantación de la política de teletrabajo de la Agencia en los últimos años. En la siguiente tabla se pueden consultar las cifras relacionadas con la tasa de resolución de reclamaciones:

Tasa de resolución de reclamaciones	2019	2020	Δ% anual
Reclamaciones resueltas en el año*	11.182	10.443	-7%
Reclamaciones pendientes de resolver al finalizar el año	3.826	3.709	-3%
Tasa de reclamaciones resueltas vs. recibidas en el año**	96%	101%	5%

\* La bajada en número de reclamaciones resueltas está relacionada con la bajada en el número de reclamaciones presentadas ante la AEPD, que se ha reducido un 11%. Como se puede apreciar, se han resuelto porcentualmente un 4% más que las reclamaciones presentadas.

\*\* A la vista de los datos obtenidos, se puede comprobar que se ha mejorado un 5% respecto al mismo dato del año anterior, a pesar de la situación de confinamiento y pandemia.

## 2. Resoluciones

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

### Resoluciones en fase de Análisis de la Reclamación

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

Esta fase, previa a la tramitación de cualquier procedimiento, finaliza con la inadmisión de la reclamación presentada, por no cumplir con los requisitos establecidos en el artículo 65 de la LOPDGDD. El valor de inadmisiones en esta fase se encuentra en torno al 50% de los casos, en línea con la cifra del año anterior, como muestra la siguiente tabla:

Tipo de resultado	2019	2020	% relativo	Δ% 2018/19
Resoluciones tras la fase de Análisis de la reclamación	5.897	5.671	56%	-4%
Inadmisiones a trámite*	5.820	5.522	55%	-5%
Competencia de otras AC nacionales (CGPJ, AC auton.)*	77	149	1%	94%
Resoluciones en otras fases	5.300	4.396	44%	-17%
<b>TOTAL</b>	<b>11.197</b>	<b>10.067</b>	<b>100%</b>	<b>-10%</b>

\* 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. 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 manera se consiguen solucionar un número elevado de reclamaciones en un tiempo reducido, con independencia de la actuación inspectora que siempre se puede realizar e de acuerdo con las competencias que tiene atribuidas la SGID.

En línea con los resultados observados en el ejercicio anterior, la inclusión de esta nueva fase de traslado ha supuesto una gran mejora con relación a los procedimientos de trabajo anteriores. Así, en 2020, después de haber procedido al traslado de la reclamación, se dictó resolución finalizando su tramitación prácticamente en el 80% de los casos. Por tanto, dando respuesta a los reclamantes de manera más rápida que la que se conseguía con la normativa anterior.

Tipo de resultado	2019	2020	% relativo	Δ% 2018/19
<b>Resoluciones tras Traslado*</b>	<b>4.197</b>	<b>3.405</b>	<b>77%</b>	<b>-19%</b>
Respuesta satisfactoria tras traslado al responsable o enc.	2.598	2.157	49%	-17%
Archivo por ser plena competencia de otra AC del EEE	384	414	9%	8%
Archivo provisional actuando como AC interesada en el EEE	571	451	10%	-21%
Archivo por otros motivos tras traslado	644	383	9%	-41%
<b>Resoluciones tras Actuaciones previas de Investigación</b>	<b>428</b>	<b>347</b>	<b>8%</b>	<b>-19%</b>
Archivo de actuaciones previas de investigación	428	347	8%	-19%
<b>Resoluciones tras procedimiento de Ejercicio de derechos</b>	<b>337</b>	<b>251</b>	<b>6%</b>	<b>-26%</b>
Resuelto en el procedimiento de ejercicio de derechos	337	251	6%	-26%
<b>Resoluciones tras procedimiento Sancionador</b>	<b>338</b>	<b>393</b>	<b>9%</b>	<b>16%</b>

\* Incluyen reclamaciones relacionadas con el ejercicio de derechos



Tipo de resultado	2019	2020	% relativo	Δ% 2018/19
Resuelto en procedimiento sancionador - Multa	112	172	4%	54%
Resuelto en procedimiento sancionador - Apercibimiento	139	163	4%	17%
Resuelto en procedimiento sancionador - Archivo	87	58	1%	-33%
<b>TOTAL</b>	<b>5.300</b>	<b>4.396</b>	<b>100%</b>	<b>-17%</b>

### Tiempos medios de resolución

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

En fase de Análisis de la reclamación, el tiempo medio responde al tiempo desde que tiene entrada la reclamación hasta que se resuelve su inadmisión. Debe tenerse en cuenta que el artículo 65.5 de la LOPDGDD establece un plazo de 3 meses para este concepto.

Tiempos medios de resolución en fase de Análisis (en días)	2019	2020	Δ% anual
Resoluciones tras el Análisis de la reclamación*	25	25	0%
<b>TOTAL</b>	<b>25</b>	<b>25</b>	<b>0%</b>

\* Incluyen reclamaciones relacionadas con el ejercicio de derechos

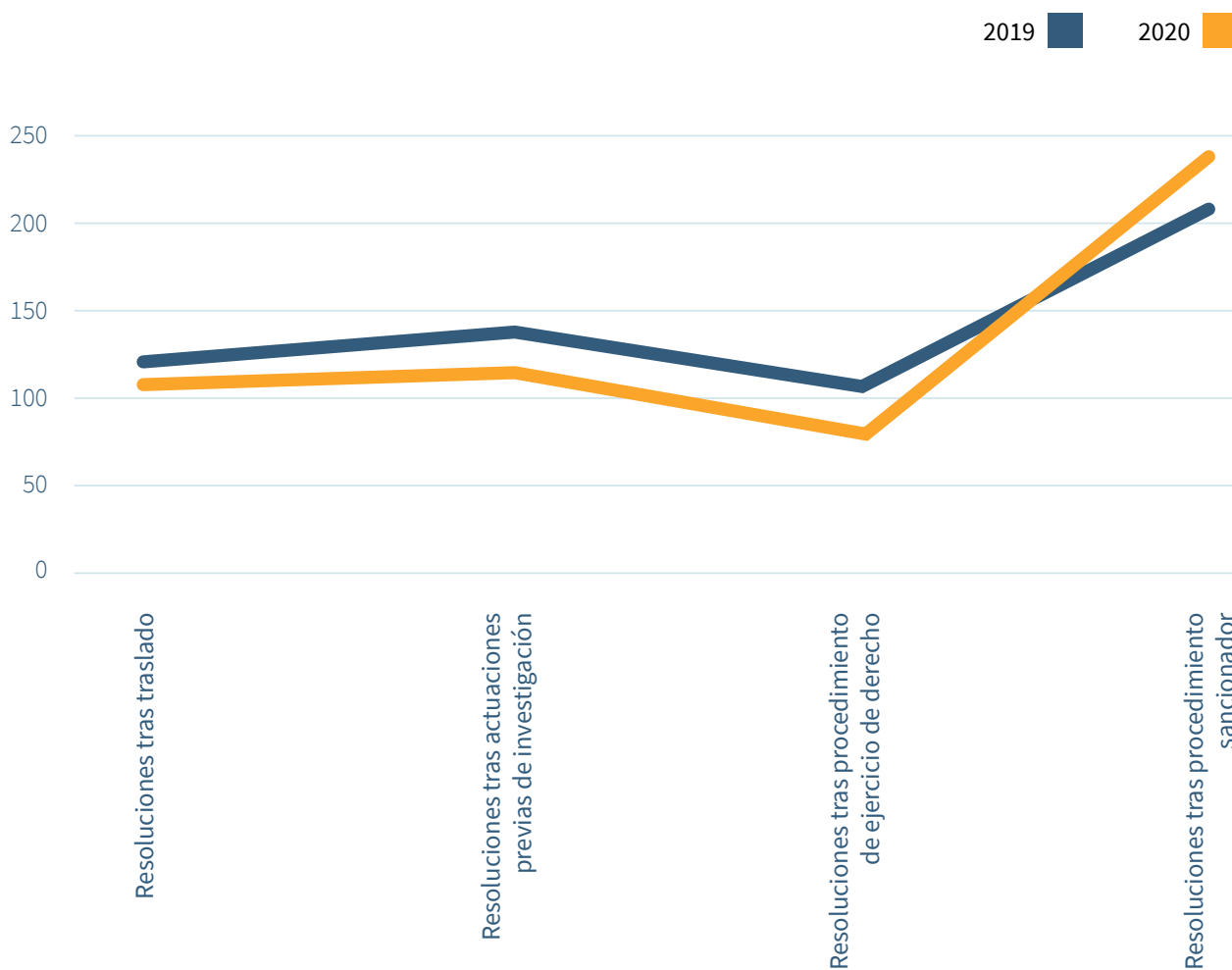
En la fase de traslado, el tiempo medio responde al tiempo desde que tiene entrada la reclamación hasta que se firma la resolución.

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.

Tiempos medios de resolución según la fase del procedimiento (en días)	2019	2020	Δ% anual
Resoluciones tras traslado*	126	110	-13%
Resoluciones tras actuaciones previas de investigación**	138	228	65%
Resoluciones tras procedimiento de ejercicio de derechos	109	79	-27%
Resoluciones tras procedimiento sancionador	212	233	10%
<b>TIEMPO MEDIO</b>	<b>132</b>	<b>129</b>	<b>-2%</b>

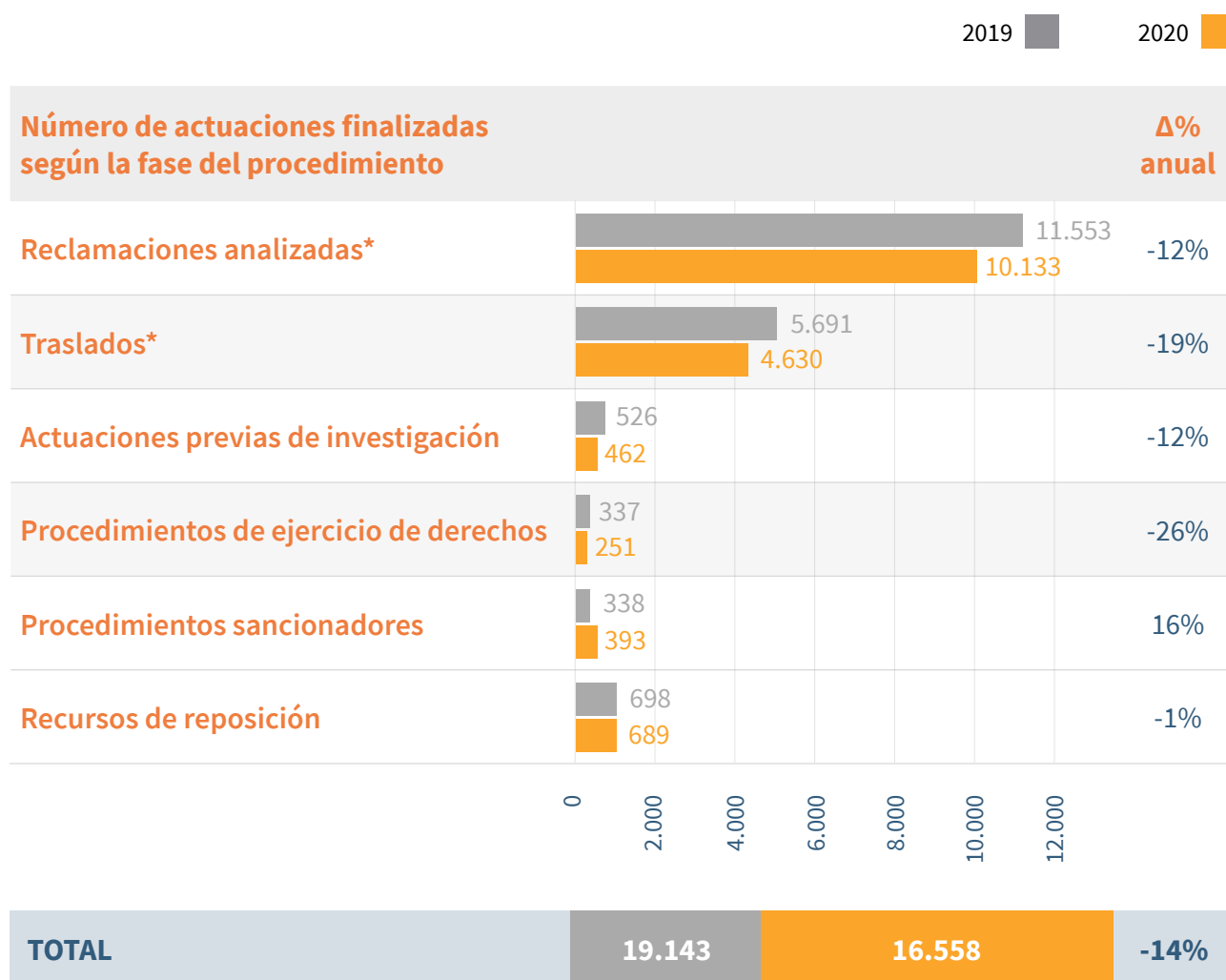
\* Incluyen reclamaciones relacionadas con el ejercicio de derechos

\*\* Los tiempos medios han aumentado en esta fase del procedimiento debido a todos los expedientes de investigación que se han abierto relacionados con la COVID-19 y la protección de datos personales.



### 3. Actuaciones realizadas

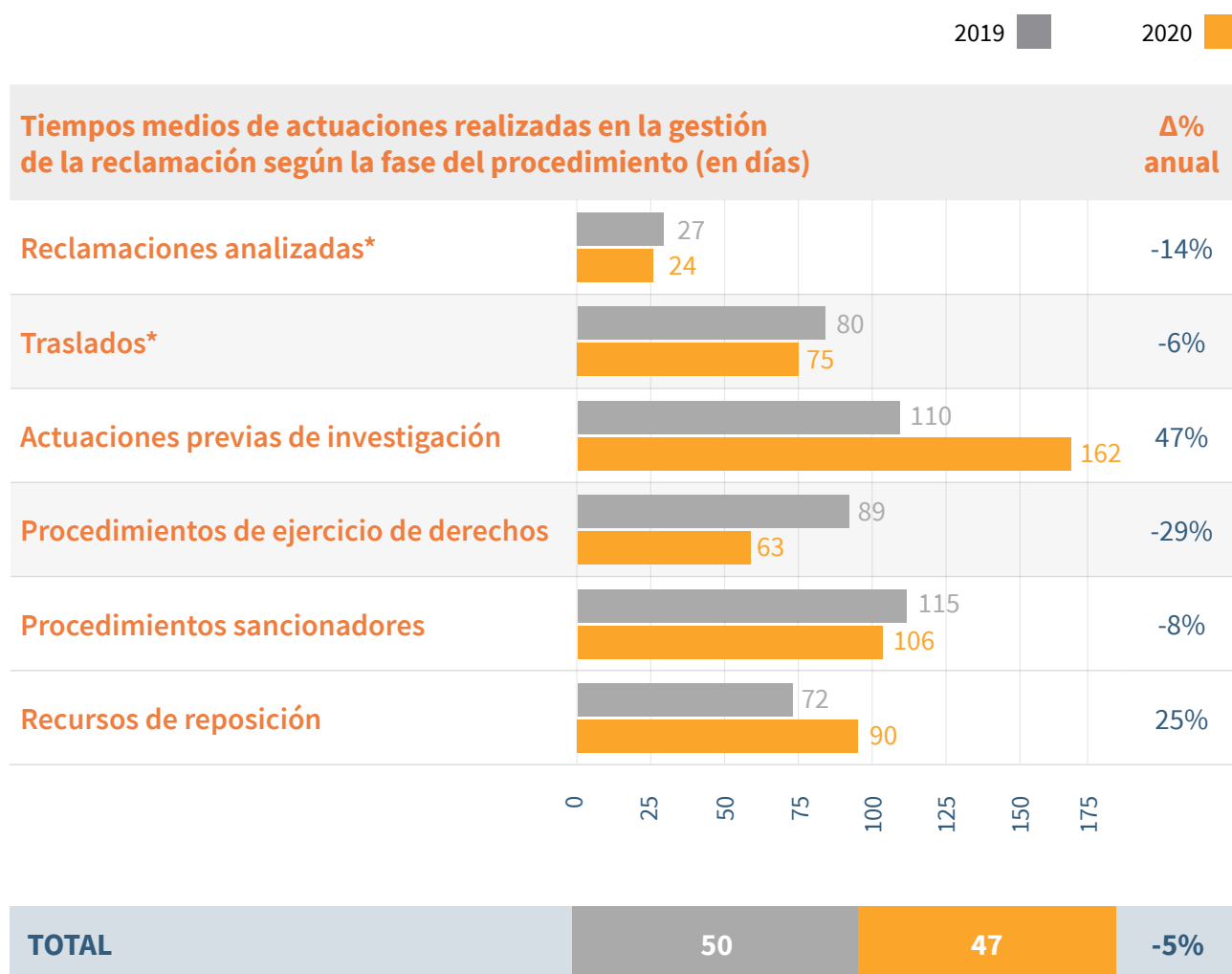
Las cifras que se muestran a continuación dan una perspectiva del total de las actuaciones realizadas en la Subdirección General de Inspección de Datos que finalizan una fase del procedimiento administrativo, pero que no lo concluyen y, por lo tanto, no dan lugar a resoluciones. Un ejemplo de ello sería una actuación previa de investigación que da lugar a un procedimiento sancionador; esta actuación no genera una resolución y, por lo tanto, no aparece detallada en el apartado anterior, pero, sin embargo, sí implica un trabajo que es el que se indica en este epígrafe. En el caso de procedimientos de ejercicio de derechos, sancionadores o recursos de reposición, que siempre ponen fin al procedimiento administrativo y producen, por tanto, una resolución, las cifras son coincidentes con las dadas en el apartado anterior.



\* Incluyen reclamaciones relacionadas con el ejercicio de derechos

## Tiempos medios de resolución

Los tiempos que aparecen en este apartado se refieren a los tiempos medios de actuaciones de cada una de las fases individuales relacionadas con la gestión de la reclamación. Estos tiempos medios se miden en días desde el inicio de cada fase hasta su finalización.



\* Incluyen reclamaciones relacionadas con el ejercicio de derechos

\*\* Los tiempos medios han aumentado en esta fase del procedimiento debido a todos los expedientes de investigación que se han abierto relacionados con la COVID-19 y la protección de datos personales.

## 4. Recursos

Los recursos interpuestos frente a resoluciones de los procedimientos de Inspección se muestran a continuación, según hayan sido de reposición, extraordinarios de revisión, o contencioso-administrativos. Los

Tipo de recurso	2019	2020	Δ% anual
Recursos de reposición	797	674	-15%
Recursos extraordinarios de revisión	14	7	-50%
Recursos contencioso-administrativos	109	63	-42%
<b>TOTAL</b>	<b>920</b>	<b>744</b>	<b>-19%</b>

recursos de reposición y revisión resueltos anualmente por la AEPD se muestran en la siguiente tabla:

Tipo de recurso	2019	2020	Δ% anual
Recursos de reposición	698	689	-1%
Recursos extraordinarios de revisión	11	8	-27%
<b>TOTAL</b>	<b>709</b>	<b>697</b>	<b>-2%</b>



## 5. Clasificaciones

### Reclamaciones planteadas con mayor frecuencia

Se muestran las 10 áreas de actividad con mayor número de reclamaciones recibidas en 2020:

Reclamaciones planteadas con mayor frecuencia	2019	2020	% relativo	Δ% 2018/19
<b>TOP 10</b>	<b>8.826</b>	<b>7.751</b>	<b>75%</b>	<b>-12%</b>
Servicios de Internet	1.529	1.602	16%	5%
Ficheros de morosidad	1.407	1.510	15%	7%
Videovigilancia	1.415	1.189	12%	-16%
Publicidad (excepto spam)	784	681	7%	-13%
Reclamación de deudas	1.059	656	6%	-38%
Administración pública	776	503	5%	-35%
Entidades financieras/acreedoras	464	473	4%	-6%
Comercios, transporte y hostelería	508	405	4%	-20%
Sanidad	460	388	4%	-16%
Telecomunicaciones	424	380	4%	-10%
<b>Otros</b>	<b>2.764</b>	<b>2.573</b>	<b>25%</b>	<b>-7%</b>
<b>TOTAL</b>	<b>11.590</b>	<b>10.324</b>	<b>100%</b>	<b>-11%</b>

## Áreas más frecuentes en procedimientos sancionadores

Se muestran las 10 áreas de actividad con mayor número de procedimientos sancionadores finalizados en 2020:

Grupo de actividad	2019	2020	% relativo	Δ% anual
<b>TOP 10</b>	<b>275</b>	<b>324</b>	<b>82%</b>	<b>18%</b>
Videovigilancia	106	94	24%	-11%
Servicios de Internet	58	73	19%	26%
Administración Pública	15	39	10%	160%
Telecomunicaciones	21	27	7%	29%
Comercios, transporte y hostelería	10	23	6%	130%
Publicidad a través de e-mail o teléfono móvil	32	17	4%	-47%
Comunidades de propietarios	4	14	4%	250%
Contratación fraudulenta	13	14	4%	8%
Asuntos laborales	5	13	3%	160%
Asuntos laborales	11	10	3%	-9%
<b>Otros</b>	<b>63</b>	<b>69</b>	<b>18%</b>	<b>10%</b>
<b>TOTAL</b>	<b>338</b>	<b>393</b>	<b>100%</b>	<b>16%</b>

## Reclamaciones relacionadas con la pandemia de COVID-19

El año 2020 ha estado marcado por la crisis sanitaria ocasionada por la pandemia. En la siguiente tabla se muestran las cifras de reclamaciones y otras actuaciones realizadas por iniciativa propia, relacionadas con la materia del virus SARS-COV-2 y su afectación a los distintos ámbitos (laboral, telecomunicaciones, etc):



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:



## 6. Ámbito transfronterizo (EEE)

La aplicación del RGPD desarrolla en su capítulo VII los mecanismos de cooperación entre autoridades de control del Espacio Económico Europeo, donde es de plena aplicación el Reglamento.

### Casos transfronterizos con participación de la AEPD

En los casos con componentes transfronterizos que afectan a ciudadanos o a establecimientos de responsables en España, la AEPD colabora en su resolución. Según se encuentre el establecimiento principal del responsable en España o en otro Estado miembro, en atención al mecanismo de ventanilla única, la participación será como autoridad principal o interesada.

Papel de la AEPD	2019	2020	Δ% anual
Nuevos casos liderados como autoridad principal	21	17	-19%
Nuevos casos en cooperación como autoridad interesada	565	451	-20%
<b>TOTAL</b>	<b>586</b>	<b>468</b>	<b>-20%</b>

### 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 AC, como otras solicitudes de asistencia y consulta recibidos por la AEPD, así como los proyectos de decisión analizados y participados por la AEPD.

Papel de la AEPD	2019	2020	Δ% anual
Casos transfronterizos procedentes de otras AC	790	784	-1%
Solicitudes de asistencia de otras AC	93	207	123%
Consultas de otras AC en procedimientos transfronterizos	119	111	-7%
Proyectos de decisión de casos en los que la AEPD participa*	50	107	114%
Operaciones conjuntas donde la AEPD participa	0	1	-
<b>TOTAL</b>	<b>1.052</b>	<b>1.210</b>	<b>15%</b>

\* 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.

Tipo de notificación	2019	2020	Δ% anual
Casos transfronterizos compartidos de otras AC	86	40	-53%
Solicitudes de asistencia de otras AC	61	90	48%
Consultas a otras AC en procedimientos transfronterizos	46	7	-85%
Proyectos de decisión de casos liderados por la AEPD*	21	24	14%
<b>TOTAL</b>	<b>214</b>	<b>161</b>	<b>-25%</b>

\* 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	2019	2020	Δ% anual
Número de multas	112	167	49%
Importe total	6.295.923	8.018.800	27%

El incremento en la cifra de sanciones impuestas denota que las cifras de gestión vuelven a aproximarse a las existentes antes de la aplicación del RGPD.

### Áreas con mayor importe global de multas

La siguiente tabla desglosa las 6 áreas de actividad con mayor importe en sanciones en 2020:

Importe de multas en euros según el sector de actividad	2019	2020	% relativo	Δ% anual
<b>Seis sectores con mayor importe global de sanciones</b>	<b>1.894.021</b>	<b>7.460.900</b>	<b>93%</b>	<b>294%</b>
Entidades financieras/acreedoras	45.600	5.045.000	63%	10.964%
Telecomunicaciones	641.000	1.009.000	13%	57%
Contratación fraudulenta	620.620	559.000	7%	-10%
Reclamación de deudas	156.000	242.000	3%	55%
Servicios de Internet	144.300	218.900	3%	52%
Ficheros de Morosidad	286.501	387.000	5%	35%
<b>Otros</b>	<b>4.401.902</b>	<b>557.900</b>	<b>7%</b>	<b>-87%</b>
<b>TOTAL</b>	<b>6.295.923</b>	<b>8.018.800</b>	<b>100%</b>	<b>27%</b>

## ► 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
Reclamaciones presentadas ante la AEPD por el Canal Prioritario	184
Comunicaciones del canal de menores (14-18 años) por el Canal Prioritario	174
<b>TOTAL</b>	<b>358</b>

## Entradas tramitadas con carácter de urgencia tras el análisis de la Agencia

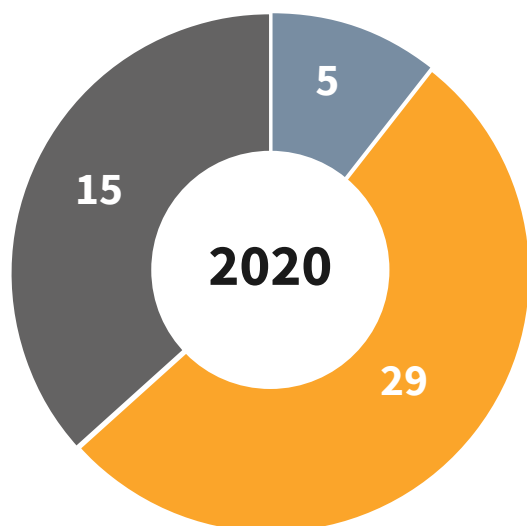
Cada entrada que llega a través del Canal Prioritario se analiza en profundidad para determinar si el caso reúne las características para ser tratado como sensible, en cuyo caso se procede a su tramitación con carácter de urgencia. En el resto de casos, también se puede continuar su tramitación, aunque 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.

Además de estas entradas a través del Canal Prioritario, hay otras reclamaciones que llegan mediante el Canal Ordinario de la Agencia que por su naturaleza también requieren la intervención urgente.

A continuación, se indican los supuestos que han requerido dicha intervención indicando sus canales de origen.

Tipo de entrada	2020
Reclamaciones recibidas por el Canal Prioritario	29
Reclamaciones recibidas por canales ordinarios	5
Comunicaciones del canal de menores (14-18 años)	15
<b>TOTAL</b>	<b>49</b>

## Entradas tramitadas con carácter de urgencia tras el análisis de la Agencia



### Tipo de entrada

- Reclamaciones recibidas por el Canal Prioritario
- Reclamaciones recibidas por canales ordinarios
- Comunicaciones del canal de menores (14-18 años)

## 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 de los 49 señalados anteriormente. A los 20 casos restantes, que no requerían la retirada de contenidos, también se les ha dado un tratamiento prioritario sin adoptar dichas medidas.

Tipo de intervención	2020
Intervenciones con carácter de urgencia para la retirada de contenidos	29
Intervenciones con carácter de urgencia para la retirada de contenidos que han resultado eficaces	25

## 3. Gabinete Jurídico

### Consultas

Administraciones Públicas	
AGE	50
CCAA	6
Entidades locales	2
Otros	14
<b>TOTAL 1</b>	<b>72</b>
Consultas Privadas	
Asociaciones y Fundaciones	1
Empresas	21
Particulares	2
Sindicatos	0
Otros	0
<b>TOTAL 2</b>	<b>24</b>
<b>TOTAL</b>	<b>96*</b>

\* El total suma 100 entradas pero 4 de ellas fueron objeto de acumulación por ser de la misma materia.

### Evolución de consultas por sectores (2019-2020)

	2019	2020
Administraciones Públicas	118	72
Particulares	1	3
Telecomunicaciones	12	15
Asesoría y consultoría	1	1
Sindicatos	1	0
Servicios informáticos	0	0
Asociaciones empresariales	2	0
Asociaciones y fundaciones	0	1
Solvencia patrimonial	1	0
Servicios	0	1
Sanidad y farmacia	0	3
Agua y energías	0	0
Seguridad	0	0
Distribución y venta	0	0
Transporte	0	0
Servicios financieros	0	0
Investigación	0	0
Hostelería	0	0
Banca y seguros	1	0
Partidos políticos	0	1
Comunidades de propietarios	0	0
Alimentación	0	0
Industria y construcción	0	0
Educación	0	2
<b>TOTAL</b>	<b>19*</b>	<b>27</b>

*Nota: Existen consultas que versan sobre más de un sector y son clasificadas en el que más relevancia tienen. Asimismo, otras categorías están en desuso y tienden a desaparecer por la evolución normativa actual y se han mantenido en términos comparativos con el ejercicio anterior.*



### Evolución de consultas por materias (2019-2020)

	2019	2020
Conceptos Generales	68	4
Ámbito de Aplicación	4	8
Licitud	0	0
Derecho de Información y Transparencia	13	18
Finalidad	7	5
Minimización y Proporcionalidad	14	17
Exactitud/Calidad de datos	63	9
Plazo de Conservación	3	4
Integridad y Confidencialidad	0	2
Consentimiento	68	36
Interés Legítimo	0	1
Responsable	10	6
Encargado	5	33
Corresponsable	0	11
Derechos	10	7
Derecho a información y Transparencia	16	15
Tratamientos Videocámaras	0	1
Categorías Especiales de datos	0	15
Datos de salud	0	6
Seguridad en el Tratamiento	6	4
Responsabilidad Activa	0	0
Delegado Protección Datos	39	8
Gestión Riesgo y Evaluación de Impacto	0	1
Transferencias Internacionales	4	1
Transparencia y acceso a registros públicos	4	13

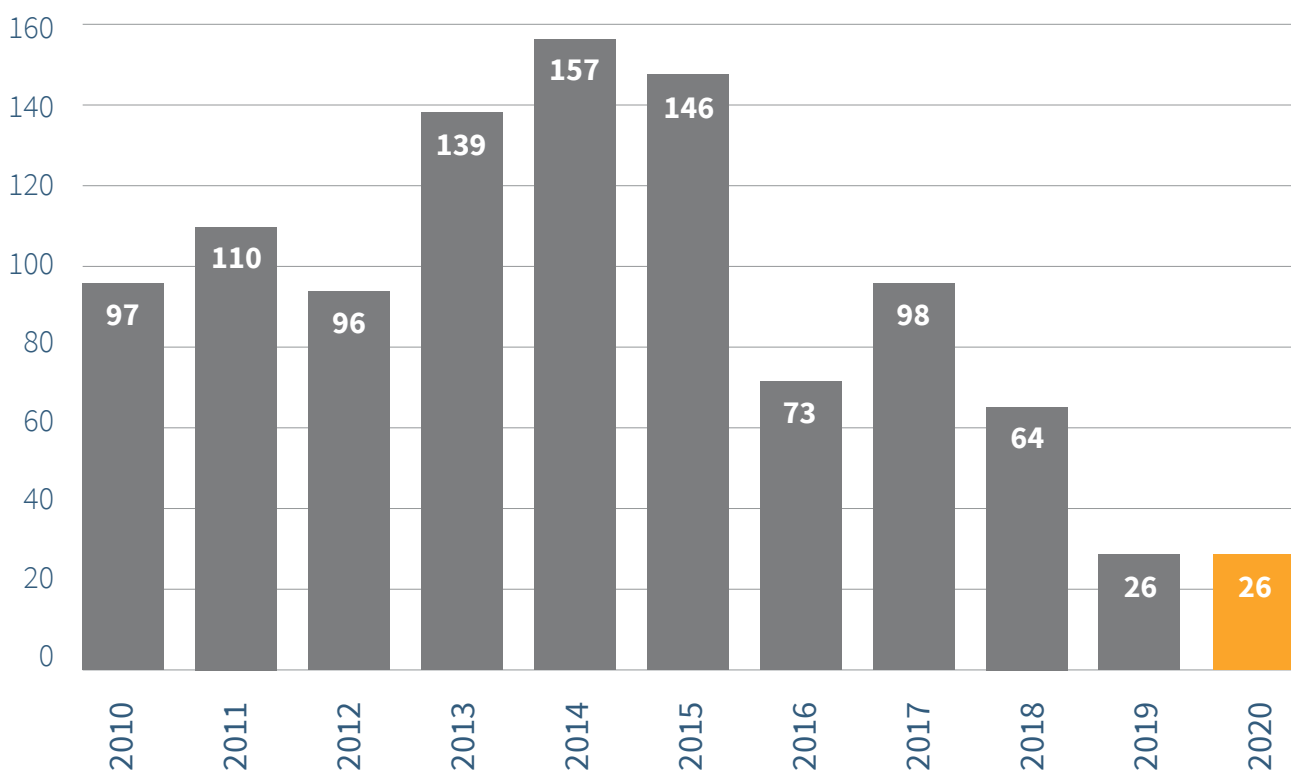
### Evolución de consultas por materias (2019-2020)

	2019	2020
Telecomunicaciones	15	22
Información Crediticia	0	0
Menores	3	3
Administración electrónica	0	0
Estadística	2	2
Prevención Blanqueo	0	0
Spam y Cookies	0	0
Otros	24	31

*Nota: Existen consultas que versan sobre más de una materia 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 (como licitud que es una nueva categoría) y en otras puede no haber coincidencia con los datos que se publicaron en la memoria de 2019 respecto de ese ejercicio.*

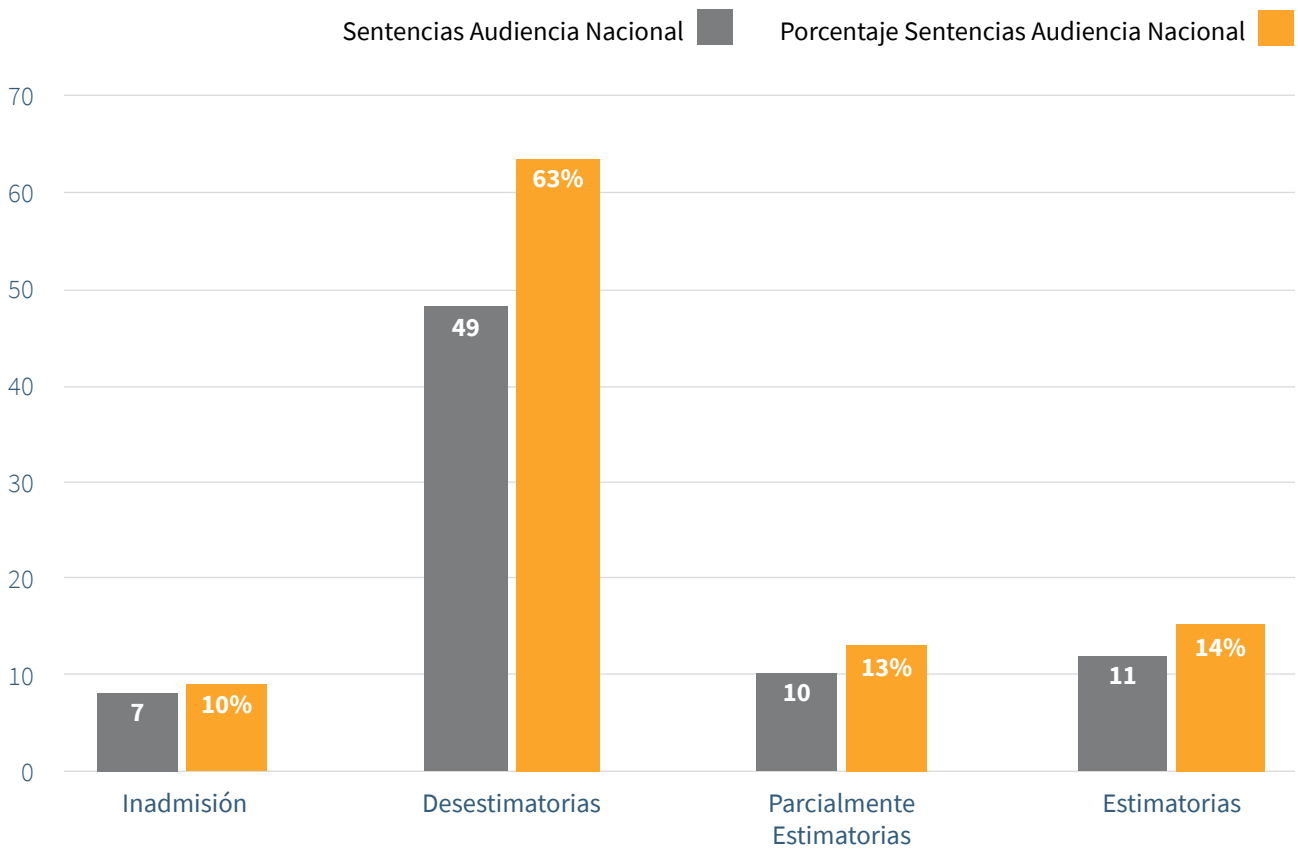
### Evolución de informes preceptivos a disposiciones generales (2010-2020)

#### Disposiciones Generales



Evolución informes preceptivos (2010-2020)				
Año	Disposiciones generales	RD 424/2005	Prec. Otros	Total
2010	97	23	-	120
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
<b>2020</b>	<b>26</b>	<b>15</b>	<b>0</b>	<b>41</b>

## Sentencias Audiencia Nacional 2020

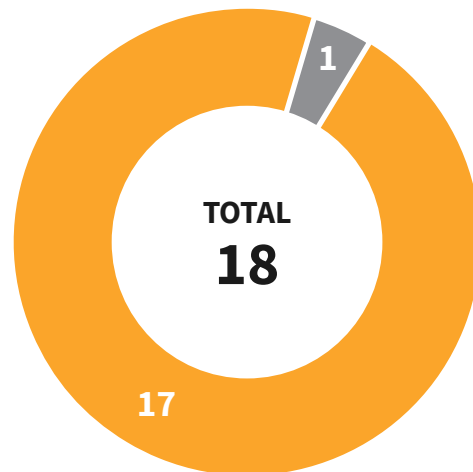


**TOTAL** Sentencias Audiencia Nacional 2020

**77**

## Sentencias Tribunal Supremo (2020)

■ Favorables  
■ Contrarias

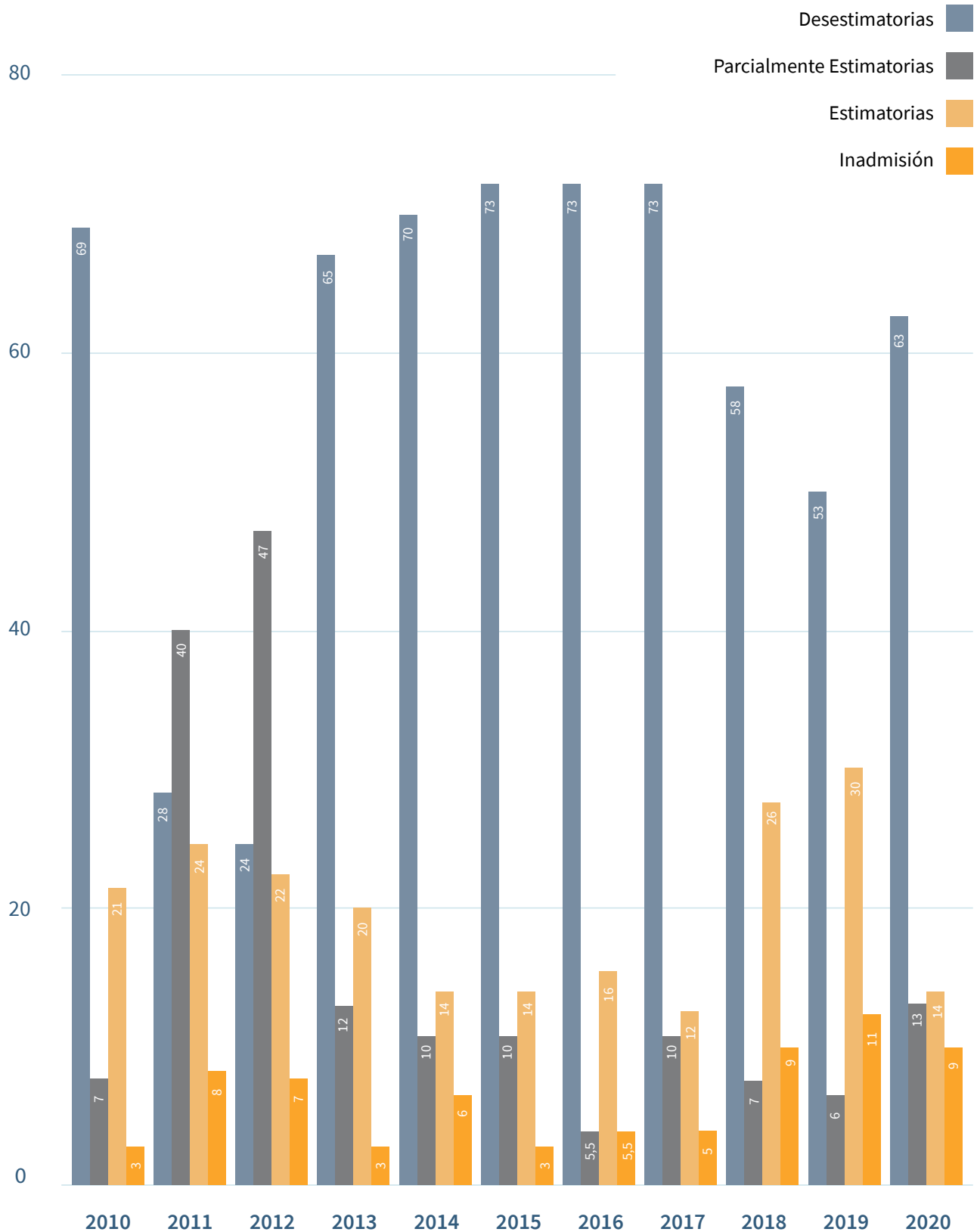


### Evolución por sentido del fallo en porcentajes (2010-2020)

Ejercicio (año)	Desestimatorias	Parcialmente Estimatorias	Estimatorias	Inadmisión
2010	69	7	21	3
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
<b>2020</b>	<b>63</b>	<b>13</b>	<b>14</b>	<b>9</b>



## Evolución por sentido del fallo en porcentajes (2010-2020)



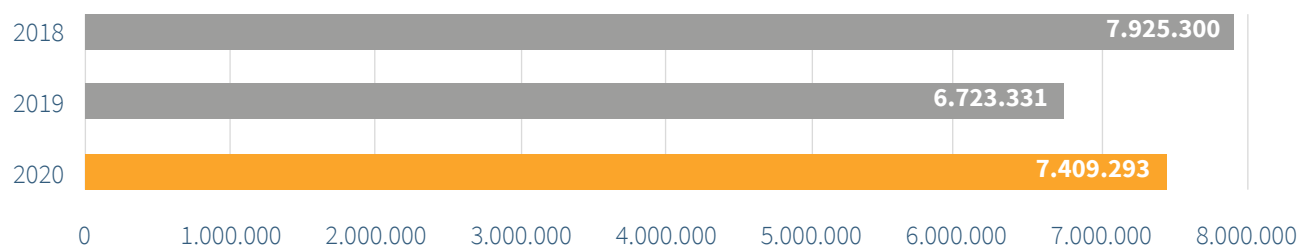
Comparativa por sector recurrente (2019-2020)		
	2019	2020
Publicidad y prospección	18	0
Administraciones Públicas	3	1
Salud	1	1
Solvencia patrimonial y crédito	16	7
Distribución y venta	2	2
Sociedad de la información	26	6
Agua y energía	4	1
Banca y seguros	37	3
Particulares	64	47
Telecomunicaciones	16	4
Asociaciones y sindicatos	5	0
Otros	17	5
<b>TOTAL</b>	<b>209</b>	<b>77</b>

## 4. Atención al ciudadano y sujetos obligados

Consultas totales planteadas ante el área de Atención al Ciudadano				
	2018	2019	2020	% 2019-2020
Presenciales	3.455	2.443	310 <sup>1</sup>	-87,31
Telefónicas	88.302	60.288	41.096	-31,83
FAOs	651.650	562.457	724.838	+28,86
Escritas (correo electrónico y sede electrónica)	5.613	10.082	8.280	-17,87
<b>TOTAL</b>	<b>749.020</b>	<b>635.270</b>	<b>774.524</b>	<b>+21,92</b>

<sup>1</sup>Del 1 de enero al 13 de marzo 2020 - La atención presencial dejó de prestarse el 13 de marzo de 2020.

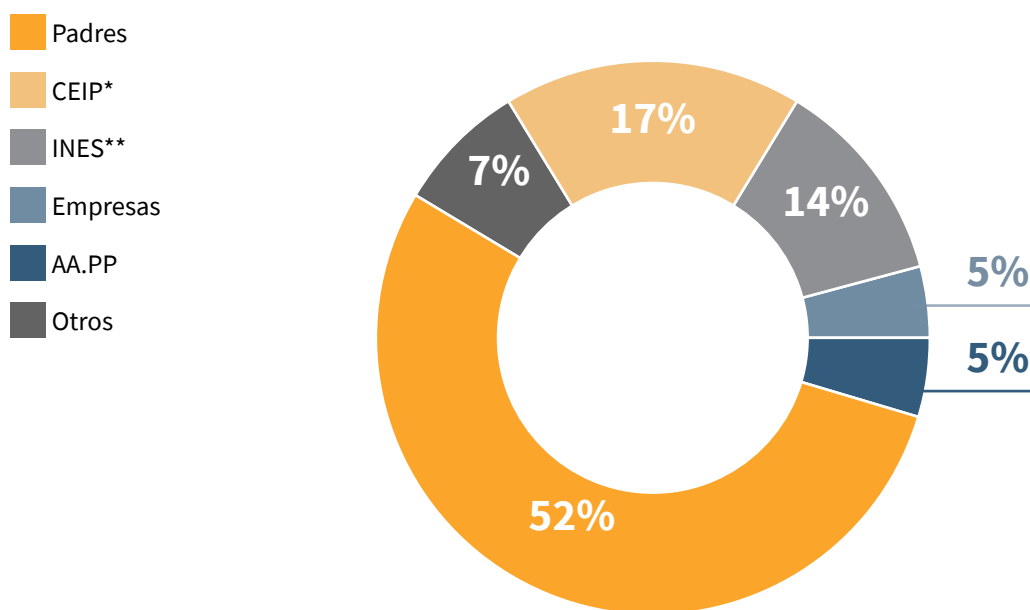
Comparativa de visitas a la web ( <a href="http://www.aepd.es">www.aepd.es</a> )				
	2018	2019	2020	% 2019-2020
Visitas	7.925.300	6.723.331	7.409.293	-10,20



### Consultas especializadas sobre el tratamiento de datos de menores

	2018	2019	2020	% 2019-2020
Teléfono	597	535	552	+3,18
WhatsApp	384	421	424	+0,71
Correo-e	388	380	241	-36,57
Sede electrónica	195	166	176	+6,02
<b>TOTAL</b>	<b>1.564</b>	<b>1.502</b>	<b>1.393</b>	<b>-7,25</b>

### Consultas por categorías<sup>2</sup>



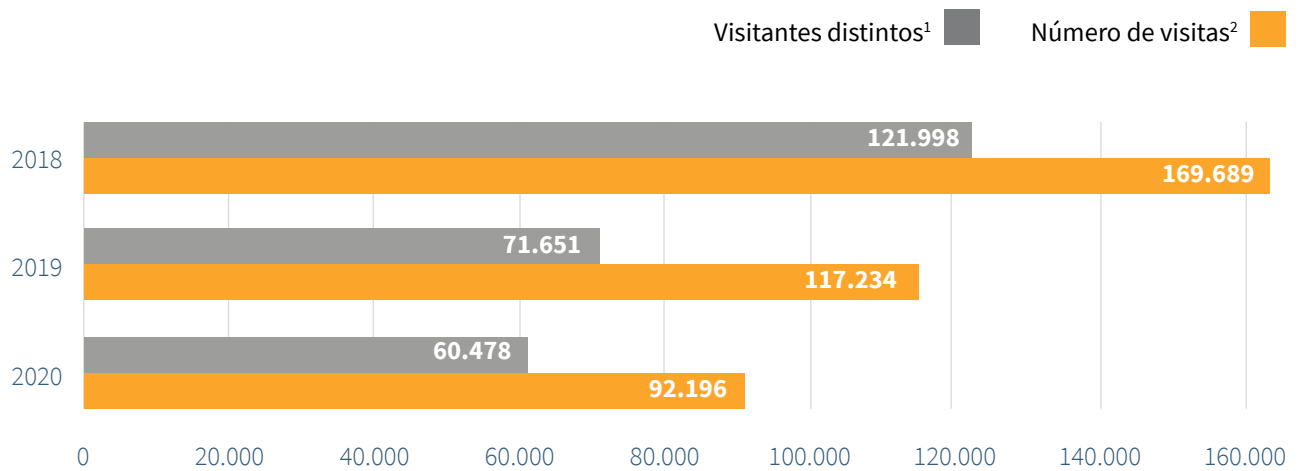
<sup>2</sup>Este epígrafe sólo recoge las consultas recibidas por Canal Joven y Sede electrónica (no se incluyen las recibidas por teléfono o whatsapp).

\* CEIP: Planteadas por Centros de Educación Infantil y Primaria.

\*\* IES: Planteadas por Institutos de Educación Secundaria.

### Accesos a la web www.tudecideseninternet.es

	2018	2019	2020	% 2019-2020
Visitantes distintos <sup>1</sup>	121.998	71.651	60.478	-15,59
Números de visitas <sup>2</sup>	169.689	117.234	92.196	-21,35

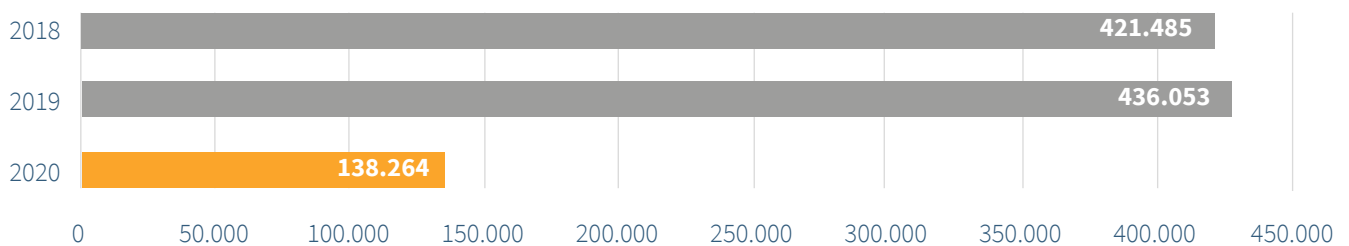


<sup>1</sup> Visitante que ha solicitado al menos una página. Si este visitante ingresa numerosas veces sólo contará como una.

<sup>2</sup> Número de visitas realizadas por todos los visitantes. Si cada visitante tiene una sesión, cada visita que realice aumentará este contador.

### Accesos al portal de transparencia

	2018	2019	2020	% 2019-2020
	421.485	436.053	138.264	-68,29





Canal INFORMA_RGPD			
	(desde marzo 2018)	2019	2020 (hasta 30/10)
Consultas	4.116	2.758	2.895

Canal del DPD <sup>3</sup>	
	2020 (desde 1/11)
Consultas	200

<sup>3</sup> El Canal del DPD sustituye al Canal Informa a partir del 1 noviembre 2020.

Temas más consultados en el catálogo de preguntas frecuentes (FAQs)			
Orden	Temas de consulta	Accesos 2019	Accesos 2020
1	En qué te podemos ayudar y en qué no	268.431	432.954
2	Cuestiones sobre la sede electrónica	32.304	52.888
3	Ámbito de aplicación	11.744	32.617
4	Menores y educación	17.254	21.464
5	Solvencia patrimonial (ficheros de morosos)	17.859	20.474
6	Tratamiento de datos en el ámbito laboral	33.171	19.380
7	Delegado de Protección de Datos	25.777	18.392
8	Videovigilancia	24.336	17.466
9	Sobre la COVID-19	-	17.044
10	Comunidades de propietarios	25.772	16.894

### Temas más consultados en la atención telefónica

Orden	Temas de consulta	2020	%
1	Reclamaciones	6.203	25,3
2	Reglamento general de protección de datos (RGPD)	5.846	23,8
3	Derechos	3.415	13,9
4	Ficheros de solvencia patrimonial	1.818	7,4
5	Videovigilancia	1.727	7,4
6	Herramienta FACILITA	1.380	7,04
7	Delegados de Protección de Datos	544	5,6
8	Comunidades de propietarios Videovigilancia	424	2,2
9	Cuestiones técnicas de la sede electrónica	249	1,7
10	Transparencia y Protección de Datos	186	1,07
11	Otras cuestiones	2.713	11,07

Otros contenidos	
Guías generales	Descargas
Guía sobre el uso de videocámaras para seguridad y otras finalidades	83.126
Guía sobre el uso de las cookies	77.804
Guía para el responsable de tratamiento de datos personales	56.919
Protección de datos: guía para el ciudadano	49.233
Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD	42.225
Guía para pacientes y usuarios de la Sanidad	40.721
Guía para el cumplimiento del deber de informar	33.130
Guía de evaluación de impacto en la protección de datos personales	31.487
Directrices para la elaboración de contratos entre responsables y encargados del tratamiento	26.768
Guía para la gestión y notificación de brechas de seguridad	26.702
Listado de elementos para el cumplimiento normativo	16.113
Guía de Privacidad desde el diseño	15.845
Drones y Protección de Datos	8.099
Guía de Privacidad desde el diseño (versión en inglés)	6.580
Guía sobre el uso de las cookies (versión en inglés)	4.532
Guía para la gestión y notificación de brechas de seguridad (versión en inglés)	3.248
Drones y Protección de Datos (versión en inglés)	939
Guías sectoriales	Descargas
Guía de Privacidad y Seguridad en Internet	36.628
Protección de datos y Administración Local	30.929
Guía de protección de datos y prevención de delitos	24.382
Orientaciones y Garantías en los procedimientos de anonimización	13.011

## Otros contenidos

<b>Guías sectoriales</b>	<b>Descargas</b>
Informe utilización por profesores y alumnos de aplicaciones que almacenan datos en nube...	10.194
Guía para clientes que contraten servicios de Cloud Computing	8.664
Guía de administradores de fincas	8.549
Código de buenas prácticas en protección de datos para proyectos Big Data	8.081
Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para Administraciones Públicas	6.508
Cómo gestionar una fuga de información en un despacho de abogados	4.367
Guía de protección de datos y prevención de delitos: fichas prácticas	3.730
Orientaciones para prestadores de servicios de Cloud Computing	3.293
Compra segura en INTERNET - Guía Práctica	685
<b>Estudios</b>	<b>Descargas</b>
Adecuación a la normativa a 'coste cero' y otras prácticas fraudulentas	11.615
Informe sobre políticas de privacidad en internet. Adaptación al RGPD	9.244
La protección de datos como garantía en las políticas de prevención del acoso: recomendaciones de la AEPD	7.399
Introducción al hash como técnica de seudonimización de datos personales	7.287
Fingerprinting o Huella digital del dispositivo	6.424
LOPD: Novedades para el Sector Pública	5.798
Decálogo para la adaptación al RGPD de las políticas de privacidad en internet	4.820
Consecuencias administrativas, disciplinarias, civiles y penales de la difusión de contenidos sensibles	4.065
LOPD: Novedades para el Sector Privado	4.000
LOPD: Novedades para los ciudadanos	3.881
Análisis de los flujos de información en Android	3.448
Plan de inspección sectorial de oficio Hospitales Públicos	2.310

## Otros contenidos

<b>Estudios</b>	<b>Descargas</b>
25 años de la Agencia Española de Protección de Datos	1.494
Encuesta sobre el grado de preparación de las empresas españolas ante el RGPD (AEPD-CEPYME)	912
Fingerprinting o Huella digital del dispositivo (Versión en Inglés)	838
Análisis de los flujos de información en Android (Versión en Inglés)	225
<b>Infografías</b>	<b>Descargas</b>
Compra segura en internet	15.823
Decálogo para el personal sanitario y administrativo	14.429
Adaptación al RGPD del Sector Privado	7.766
Canal prioritario para comunicar la difusión de contenido sensible y solicitar su retirada	6.507
Los derechos que tienes para proteger tus datos personales	4.465
Adaptación al RGPD de las Administraciones Públicas	2.902
10 consejos básicos para comprar en internet de forma segura	1.897
Protege sus datos en la vuelta a clase	1.039
Cómo evitar la publicidad no deseada	863
Balance Plan Estratégico	688
Protección de datos en vacaciones	552
Reglamento de Protección de Datos	437
Juguetes conectados	388
<b>Memorias</b>	<b>Descargas</b>
Memoria 2019	4.440
Memoria 2018	2.752

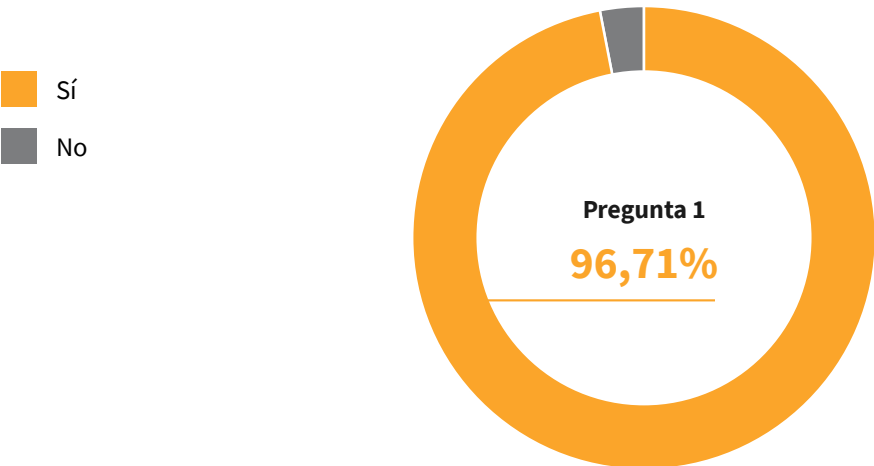
**Servicio de Atención Telefónica**  
**Encuestas de Calidad**

<b>Resumen general</b>	<b>SI</b>	<b>NO</b>
1 ¿Está satisfecho con el contenido de la información recibida?	2.998	102
2 ¿Considera que la persona que le atendió tiene los conocimientos técnicos suficientes?	2.994	106
3 ¿Está satisfecho con la corrección en el trato por parte del operador?	3.044	56
<b>Total de encuestas realizadas</b>	<b>3.100</b>	

<b>Análisis de respuestas</b>	<b>SI</b>	<b>NO</b>
1 ¿Está satisfecho con el contenido de la información recibida?	96,71%	3,29%
2 ¿Considera que la persona que le atendió tiene los conocimientos técnicos suficientes?	96,58%	3,42%
3 ¿Está satisfecho con la corrección en el trato por parte del operador?	98,19%	1,81%
<b>Total de encuestas realizadas</b>	<b>100%</b>	

**Servicio de Atención Telefónica**  
**Encuestas de Calidad - Total 3.100**

**¿Estás satisfecha con el contenido de la información recibida?**



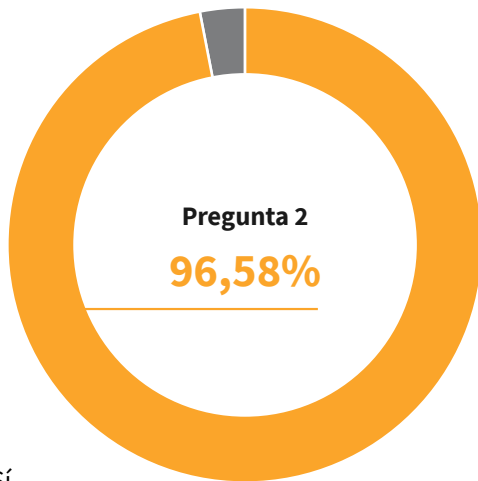


## Servicio de Atención Telefónica

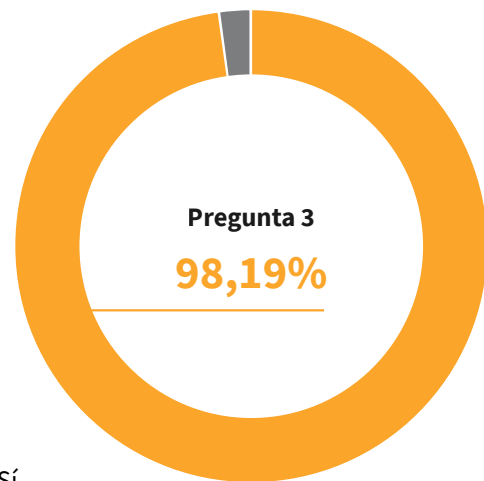
Encuestas de Calidad - Total 3.100

¿Considera que la persona que le atendió tiene los conocimientos técnicos suficientes?

¿Está satisfecho con la corrección en el trato por parte del operador?



■ Sí  
■ No



■ Sí  
■ No

## Códigos de Conducta<sup>4</sup>

Aprobados	Inadmitidos	En tramitación	Iniciativas	Códigos: Tipo cancelados <sup>5</sup>
1	2	12	6	5

<sup>4</sup> En el proceso de códigos de conducta a lo largo de 2020, se han mantenido varias reuniones con todos los promotores, con el fin de aclarar las cuestiones relativas a la tramitación de los códigos.

<sup>5</sup> Disposición transitoria segunda LOPDPGDD.

Herramienta Facilita RGPD <sup>6</sup>			
	2018	2019	2020
Accesos a Facilita RGPD	622.550	197.279	124.460
Cuestionarios finalizados	150.360	49.086	26.504

<sup>6</sup> Facilita RGPD, herramienta para facilitar la adecuación al RGPD de empresas y profesionales, implantada en septiembre de 2017.



Herramienta Facilita EMPRENDE <sup>7</sup>	
	2020
Accesos a Facilita EMPRENDE	7.682
Cuestionarios finalizados	562

<sup>7</sup> 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 <sup>8</sup>		
Sección	Abierto	Finalizado
Evaluaciones de impacto en la privacidad (EIPD)	5.403	2.750
Análisis de riesgos	5.398	2.651

<sup>8</sup> Gestiona EIPD: Asistente para el análisis de riesgos y evaluaciones de impacto en protección de datos.



Solicitudes de acceso a la información pública						
Año	Solicitudes	Autorizadas	Inadmitidas <sup>9</sup>	Autorizadas parcialmente	Denegadas	Desistidas
2019	94	45	10	-	3	7
2020	145	29	95	11	2	8

<sup>9</sup> Inadmitidas incluye devoluciones a la UIT Central

Registro de Delegados de Protección de Datos comunicados	
Titularidad	Total notificados
Entidades Privadas	57.657
Entidades Públicas	7.383
Administración General del Estado	174
Comunidades Autónomas	375
Entidades Locales	3.334
Otras personas Jurídico-Públicas	3.500
- Consejo General del Poder Judicial	
- Notarios	
- Colegios Profesionales	
- Universidades	
- Cámaras de Comercio	
- Comunidades Regantes	
<b>TOTAL</b>	<b>65.040</b>

Transferencias Internacionales		
	2020	Total
Autoridades de BCR emitidas por la AEPD	2	2
Actuaciones en la adopción de Normas Corporativas Vinculantes (BCR)	12 <sup>10</sup>	81

<sup>10</sup> La AEPD actúa como correvisora en 4 y como autoridad líder en 8.

Esquema de Certificación de DPD (AEPD-DPD)			
	2018	2019	2020
Auditorías	43	21	9
Revisión de preguntas de examen	5.125	4.300	1.927
Elaboración de exámenes	6	46	61
Seguimiento de entidades de formación	47	36	68
Seguimiento de entidades de certificación	10	11	7
Reconocimiento de formación universitaria	0	0	0
DPD Certificados	145	269	200

## 5. Secretaría General

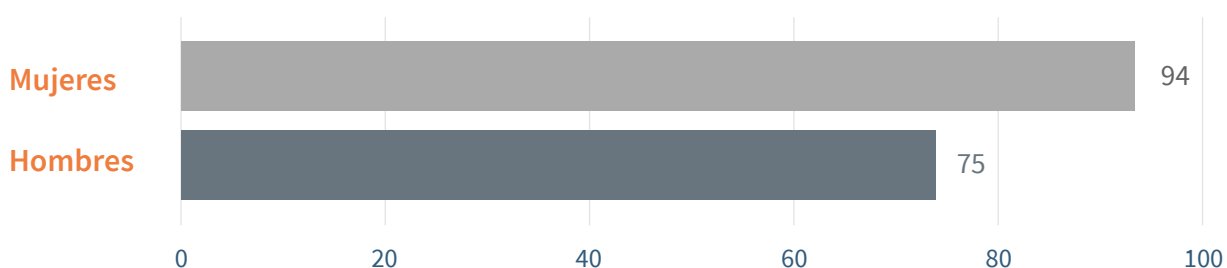
Evolución del presupuesto			
	2018	Crédito Ejercicio 2019	2020
Capítulo I	7.986.570	7.986.570	7.986.570
Capítulo II	5.071.756	4.956.060	4.956.060
Capítulo III	80.950	40.950	40.950
Capítulo IV	284.440	284.440	284.440
Capítulo VI	937.860	937.860	937.860
Capítulo VIII	22.800	22.800	22.800
<b>TOTAL</b>	<b>14.384.376</b>	<b>14.228.680</b>	<b>14.228.680</b>

## Secretaría general

### Gestión de recursos humanos a 31 de Diciembre 2020

	Dotación	Cubierto
Fundionarios	189	165*
Laborales	4	1
Laborales fuera de Convenio	2	2
Alto cargo	1	1
<b>TOTAL</b>	<b>196</b>	<b>169</b>

\* 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	7	3	29	59	0	21	3	29	2	5	4	3
Grupo					A1	A2	C1	C2				
Efectivos					39	60	31	35				

## 6. 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.

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	28 y 29 de enero 18 y 19 de febrero 19 y 20 de marzo (reunión cancelada por COVID-19)	Bruselas (Bélgica)
	3, 7, 14, 21 y 24 de abril 5, 8, 12, 19 y 26 de mayo 2, 9, 16 y 30 de junio 22 y 23 de julio 2 y 14 de septiembre 7, 8 y 20 de octubre 9, 10 y 19 de noviembre 15 de diciembre	Videoconferencia

### Reuniones de subgrupos del Comité Europeo de Protección de datos

Reunión	Fecha	Lugar
Reunión de Coordinadores de Subgrupos	24 de junio	Videoconferencia
Subgrupo sobre Reglas de Procedimiento	16 de julio 10 y 18 de septiembre 2 de octubre	Videoconferencia
Subgrupo de asesoramiento (Strategic advisory)	8 de enero	Bruselas (Bélgica)
	6 de julio 22 de julio 31 de agosto 5 de noviembre 1 y 16 de diciembre	Videoconferencia
Grupo de trabajo COVID-19	8 y 29 de abril	Videoconferencia



Reuniones de subgrupos del Comité Europeo de Protección de datos		
Reunión	Fecha	Lugar
Grupo de trabajo TikTok	24 de julio 17 de septiembre	Videoconferencia
Grupo de trabajo sobre las 101 denuncias presentadas tras la sentencia Schrems II del TJUE	2 y 27 de octubre 7 de diciembre	Videoconferencia
Medios Sociales Digitales (Social Media)	7 de febrero 15, 20 y 27 de mayo 6 de julio 6 de octubre 2 de diciembre	Videoconferencia
Usuarios de sistemas de información del CEPD (IT Users)	18 de junio 3 de diciembre	Videoconferencia
Cooperación	4 de febrero 24 de marzo <i>(reunión cancelada por COVID-19)</i>	Bruselas (Bélgica)
	22, 27 y 29 de abril 27 de mayo 12 y 24 de junio 13 y 14 de julio 22 de septiembre 21 de octubre 10 y 24 de noviembre 9 de diciembre	Videoconferencia
Asuntos financieros	21 de enero	Bruselas (Bélgica)
	6 de abril 20 de mayo 25 de junio 15 de septiembre 5 de noviembre	Videoconferencia
Multas	6 de febrero 25 de marzo <i>(reunión cancelada por COVID-19)</i>	Bruselas (Bélgica)
	25 de mayo 11 de junio 4 de septiembre 1 y 28 de octubre 25 de noviembre 4 y 16 de diciembre	Videoconferencia

## Reuniones de subgrupos del Comité Europeo de Protección de datos

Reunión	Fecha	Lugar
	11 y 12 de febrero	Bruselas (Bélgica)
<b>Transferencias Internacionales</b>	31 de marzo 27 de abril 6, 11 y 12 de mayo 5, 12, 15, 17 y 23 de junio 1 y 24 de julio 1, 8, 9, 10, 21 y 25 de septiembre 13 y 14 de octubre 3 y 4 de noviembre 7, 8 y 11 de diciembre	Videoconferencia
	6 de febrero 26 de marzo <i>(reunión cancelada por COVID-19)</i>	Bruselas (Bélgica)
<b>Fronteras, viajeros y aplicación legislativa (BTLE)</b>	23 de abril 7 de mayo 4 de junio 1 de julio 29 de septiembre 23 y 29 de octubre 18 de noviembre 10 y 17 de diciembre	Videoconferencia
<b>Disposiciones clave (Key Provisions)</b>	14 y 15 de enero 3 y 4 de marzo <i>(reunión cancelada por COVID-19)</i>	Bruselas (Bélgica)
<b>Disposiciones clave (Key Provisions)</b>	31 de marzo 28 de abril 5, 13 y 28 de mayo 2, 4, 9, 23, 24, 29 y 30 de junio 16 de julio 27 y 28 de agosto 9 de septiembre 6 y 21 de octubre 17 y 27 de noviembre 3 de diciembre	Videoconferencia

## Reuniones de subgrupos del Comité Europeo de Protección de datos

Reunión	Fecha	Lugar		
<b>Supervisión del cumplimiento (Enforcement)</b>	16 de enero 5 de febrero 26 de marzo <i>(reunión cancelada por COVID-19)</i>	Bruselas (Bélgica)		
	23 de abril 19 de mayo 10 de junio 1 y 14 de julio 15, 23 y 30 de septiembre 15, 22 y 29 de octubre 3, 5, 6, 18, 19 y 26 de noviembre 10 de diciembre		Videoconferencia	
	15 de enero 4 y 5 de marzo <i>(reunión cancelada por COVID-19)</i>	Bruselas (Bélgica)		
	1 de abril 13 de mayo 10 y 11, 22 y 26 de junio 2 de julio 17 y 18 de septiembre 15, 16 y 23 de octubre 13 de noviembre 4 de diciembre			Videoconferencia
	13 de enero 11 de marzo <i>(reunión cancelada por COVID-19)</i>	Bruselas (Bélgica)		
	2, 3, 7, 8, 9, 14, 16, 17, 20 y 29 de abril 7, 14 y 25 de mayo 4, 8, 12, 15, 18, 22, 23, 25 y 30 de junio 7, 9 y 22 de julio 7, 10, 11, 14 y 17 de septiembre 8 y 9 de octubre 5, 6 y 23 de noviembre 7 y 8 diciembre			

## Control de Agencias y Grandes Sistemas de Información UE

Reunión	Fecha	Lugar
Grupo de Supervisión Coordinada CIS	15 de junio	
Grupo de Supervisión Coordinada del SIS II	17 de junio 25 de noviembre	Videoconferencia
Grupo de Supervisión Coordinada del VIS + EURODAC	18 de junio 26 de noviembre	
Grupo de Supervisión Coordinada de EUROPOL	24 de noviembre	

## Otras Reuniones

Reunión	Fecha	Lugar
<p><b>Global Privacy Assembly</b> (antigua conferencia internacional de comisionados de protección de datos y privacidad)</p> <p>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</p>	13 al 15 de octubre	Videoconferencia
<p><b>Foro Internacional de Protección de Datos Personales: Privacidad para la Persecución del Delito y la Rendición de Cuentas.</b></p> <p>Organizado por el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, con la finalidad de favorecer una perspectiva global acerca de las circunstancias actuales en materia de justicia y rendición de cuentas, así como el tratamiento de datos personales en posesión de organizaciones policiacas, fuerzas de seguridad y la transferencia de los mismos.</p>	27 al 30 de enero	México D.F. (México)

## Otras Reuniones

Reunión	Fecha	Lugar
<b>Consejo de Europa:</b> - 41ª Plenario del Comité Consultivo del Convenio 108 - 50ª reunión de la mesa de trabajo del Comité Consultivo del Convenio 108 - 51ª reunión de la mesa de trabajo del Comité Consultivo del Convenio 108		- Inicialmente previsto en Estrasburgo del 1 al 3 de julio, debido al COVID-19 finalmente se celebró del 18 al 20 de noviembre mediante videoconferencia.  - Inicialmente prevista en París del 25 al 27 de marzo, debido al COVID-19 finalmente se celebró del 28 al 30 de septiembre mediante videoconferencia.
<b>Comité Schengen (Evaluación Alemania)</b> Visitas de evaluación Schengen in situ específica para Alemania de conformidad con el artículo 10 del Reglamento (UE) 1053/2013.		- Inicialmente prevista en Berlín del 22 al 27 de marzo, debido al COVID-19 finalmente se celebró del 30 de noviembre al 4 de diciembre mediante videoconferencia