

Antes de entrar a analizar el texto sometido a informe es preciso señalar que, habida cuenta de la fundamentación legal del informe que inmediatamente va a evacuarse y su carácter preceptivo, a tenor de lo dispuesto en las normas que acaban de señalar, debería indicarse en la Exposición de Motivos de la norma que la misma ha sido sometida al previo informe de la Agencia Española de Protección de Datos.

El proyecto remitido tiene por objeto la creación de la Agencia Estatal de Administración Digital, en virtud de lo previsto en la Disposición adicional centésima décima séptima de la Ley 22/2021, de 28 de diciembre, de Presupuestos Generales del Estado para el año 2022, así como la aprobación de su estatuto.

La creación de la Agencia, prevista en el apartado 9.4 del Plan de Digitalización de las Administraciones Públicas, referido a la reforma normativa para la transformación de la Secretaría General de Administración Digital para dotarla de la capacidad y flexibilidad suficientes para garantizar la ejecución de los fondos europeos recibidos en el marco del Plan de Recuperación, Transformación y Resiliencia, responde al cumplimiento de una serie de fines vinculados con la transformación digital de la Administración:

- la digitalización del sector público, mediante el ejercicio de las funciones de dirección, coordinación y ejecución del proceso de transformación digital e innovación de la Administración a través de las tecnologías de la información y de las comunicaciones.
- la prestación eficiente de los servicios públicos, a través de la adopción de soluciones digitales, en el marco de los Esquemas Nacionales de Seguridad e Interoperabilidad.
- La transformación digital de las Administraciones Públicas a través de la coordinación de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes, y de la cooperación con las Administraciones Públicas para la implantación de las estrategias nacionales e internacionales en materia de administración digital.
- la coordinación funcional de la actuación de las unidades de Tecnologías de la Información y Comunicaciones (en lo sucesivo, TIC) de la Administración General del Estado y el apoyo informático a aquellos departamentos ministeriales que lo precisen.

I

Desde la perspectiva de la normativa de protección de datos personales, el proyecto remitido atribuye a la Agencia Estatal de Administración Digital una serie de fines, funciones y competencias que inciden directamente en esta materia, en la medida en van a afectar a los tratamientos de datos personales que se realicen en el sector público.

De este modo, atendiendo a los fines atribuidos en materia de digitalización transformación digital y prestación eficiente de los servicios públicos, se le atribuyen competencias específicas respecto del adecuado cumplimiento de la normativa sobre protección de datos personales, como son las relativas a *la definición e impulso del desarrollo por parte de la Agencia de las políticas corporativas de seguridad de la información, ciberseguridad y protección de datos personales de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes y la colaboración al respecto con otras Administraciones Públicas* y a la realización de auditorías en el ámbito de la seguridad de la información, ciberseguridad y protección de datos personales, que el artículo 18 a), apartados 1 y 8, atribuye a la Subdirección General de Planificación de la Ciberseguridad del Departamento de Ciberseguridad, Tecnologías Disruptivas e Integridad de los Datos; o la prevista en el artículo 19 c) apartado 7, al atribuir a la Subdirección General de Asuntos Generales de la Secretaría General el *ejercicio de las competencias relativas al delegado de protección de datos*.

Asimismo, y sin ánimo exhaustivo, a lo largo del articulado se le atribuyen otras competencias que incidirán en la materia en la medida en que afectan a datos de carácter personal, como son las referidas a *la coordinación e impulso de las tareas de análisis, diseño, desarrollo, implantación tecnológica, mantenimiento y evolución de sistemas y soluciones tecnológicas de análisis y entrega de datos, gobierno del dato, cuadros de mando, datos masivos o "Big Data", inteligencia de datos, generación y gestión de conocimiento y a la elaboración de pruebas de concepto, proyectos de innovación y actividades de difusión y promoción de las actuaciones realizadas en materia de tecnologías emergentes, como, por ejemplo, Inteligencia Artificial, Analítica del Dato y Blockchain para las unidades TIC de la Administración General del Estado y de sus organismos Públicos y entidades de derecho público vinculados o dependientes* (atribuidas a la Subdirección General de Nuevos Servicios innovadores del Departamento de Administración Digital (artículo 16, b) apartados 5 y 9) al impulso a la renovación tecnológica de aplicaciones de gestión para la integración con tecnología de analítica de datos e Inteligencia Artificial (atribuidas a las Subdirección General de Servicios Digitales para la Gestión del mismo Departamento en el artículo 16, c) apartado 1), la de *diseño, provisión, explotación y evolución de los centros de proceso de datos de referencia, gestionados por la Agencia, para la prestación de*

servicios comunes (atribuida a la Subdirección General de Infraestructuras y Cloud del Departamento de Infraestructuras y Operaciones por el artículo 17.a) apartado 5) la de *diseño, provisión y explotación de los servicios, soluciones tecnológicas y las infraestructuras de comunicaciones unificadas de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes, así como de la conocida como Red SARA* (atribuida a la Subdirección General de Comunicaciones de ese mismo Departamento por el artículo 17c) apartado 1º) o las competencias en materia de *creación de espacios de compartición de datos entre Administraciones Públicas de manera segura y el empleo masivo de los datos en estas mediante tecnologías Big Data e Inteligencia Artificial, entre otras* (que el artículo 18.c) 4 atribuye a la Subdirección General de Tecnologías Disruptivas e Integridad de la Información del Departamento de Ciberseguridad, Tecnologías Disruptivas e Integridad de los Datos).

En el ejercicio de todas las competencias que incidan en los tratamientos de datos de carácter personal por el sector público o implique la realización de dichos tratamientos por la Agencia Estatal de Administración Digital deberá observarse la normativa general sobre protección de datos personales, constituida por el por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD), lo que debería reflejarse adecuadamente en el texto remitido.

De este modo, además de una referencia genérica a dicha normativa al regular la posición jurídica que, en relación con dichos tratamientos, le corresponda a la Agencia Estatal de Administración Digital, a la que posteriormente nos referiremos, debería recogerse expresamente en el artículo 2 al regular los fines de la misma, al menos en su apartado b), en el cual ya se hace mención al Esquema Nacional de Seguridad e Interoperabilidad proponiéndose la siguiente redacción:

b) La prestación eficiente de los servicios públicos a través de la adopción de soluciones digitales, en el marco **de la normativa sobre protección de datos personales** y de los Esquemas Nacionales de Seguridad e Interoperabilidad.

A este respecto, debe recordarse, singularmente, que tal y como viene señalando de manera reiterada esta Agencia, existen diferencias importantes entre la seguridad de la información y la protección de datos de carácter personal, (por todos, Informe 64/2021 sobre el Proyecto de Real Decreto por el que se regula el Esquema Nacional de Seguridad), de modo que *la seguridad*

de la información aparece como una obligación más de los responsables y encargados del tratamiento, quienes deberán aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para los derechos y libertades de los interesados, pero sin que se limite exclusivamente al ámbito de la seguridad de dicha información, en cuanto que la protección de datos personales tiene un ámbito mucho más extenso que abarca, a un conjunto de principios, derechos, medidas y garantías mucho más amplio, entre ellas medidas sobre el concepto del tratamiento, políticas de protección de datos, protección de datos desde el diseño y por defecto o notificación y comunicación de brechas de datos personales, bajo la garantía administrativa de las “autoridades de control” previstas en dicha normativa.

Asimismo, debe hacerse referencia a los tratamientos de datos personales que puedan realizarse como consecuencia de la implantación de medidas de seguridad que tengan un objetivo distinto que la protección de datos personales, cuestión que fue igualmente objeto de análisis en nuestro informe 64/2021, sobre el Proyecto de Real Decreto por el que se regula el Esquema Nacional de Seguridad, y cuyas observaciones han sido incorporadas al Real Decreto 311/2022, de 3 de mayo:

III

Para concluir, además de las observaciones sustanciales recogidas en el apartado anterior debe resaltarse que, al igual que las medidas de seguridad aplicables a los sistemas de información que traten datos personales deben adecuarse a la normativa sobre protección de datos personales, al objeto de dotarlos de una protección ajustada a la misma, dicha normativa deberá aplicarse igualmente a aquellas medidas de seguridad previstas en el ENS que, independientemente de los sistemas a los que se apliquen, supongan tratamientos de datos personales, lo que requerirá, entre otros requisitos, una adecuada valoración de la proporcionalidad de las mismas.

Así se recoge, por ejemplo, en el artículo Artículo 24, que regula el Registro de la actividad y detección de código dañino:

Con el solo propósito de satisfacer el objeto del presente real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones públicas, y de conformidad con lo dispuesto en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), los sujetos comprendidos en el artículo 2 de este real decreto podrán analizar las comunicaciones entrantes o salientes, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

Aun cuando en este supuesto, al referirse a tratamientos de datos personales vinculados a la actividad de las Administraciones Públicas, la base jurídica que legitima dichos tratamientos se encontraría en la letra e) del artículo 6.1 del RGPD “el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento”, al no ser aplicable a los tratamientos de la Administración el interés legítimo, tal y como se señaló en nuestro Informe 175/2018, procede traer a colación lo señalado en el Considerando 49 del RGPD, en cuanto se refiere específicamente a la “seguridad de la red y de la información”:

Constituye un interés legítimo del responsable del tratamiento interesado el tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema información de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos, y la seguridad de los servicios conexos ofrecidos por, o accesibles a través de, estos sistemas y redes, por parte de autoridades públicas, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad. En lo anterior cabría incluir, por ejemplo, impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de

«denegación de servicio» y daños a los sistemas informáticos y de comunicaciones electrónicas.

De dicho Considerando interesa destacar la importancia que se da a que el tratamiento lo sea **“en la medida estrictamente necesaria y proporcionada”**, ya que siendo los principios de necesidad y de proporcionalidad principios aplicables a todos los tratamientos de datos personales conforme al artículo 5.1. del RGPD, el propio legislador comunitario ha querido destacar específicamente en este supuesto.

Del mismo modo, dicho principio de proporcionalidad ha sido reiteradamente destacado por nuestro Tribunal Constitucional, tal y como recuerda la Sentencia del Tribunal Constitucional 14/2003, de 28 de enero:

“En otras palabras, de conformidad con una reiterada doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan basta con recordar que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto; SSTC 66/1995, de 8 de mayo, F. 5; 55/1996, de 28 de marzo, FF. 7, 8 y 9; 270/1996, de 16 de diciembre, F. 4.e; 37/1998, de 17 de febrero, F. 8; 186/2000, de 10 de julio, F. 6).”

Por ello, debería recogerse en el texto del citado artículo 24 una referencia expresa a los citados principios, proponiéndose la siguiente redacción:

Registro de la actividad y detección de código dañino:

Con el solo propósito de satisfacer el objeto del presente real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información **estrictamente** necesaria para monitorizar, analizar, investigar y

documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

*Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones públicas, y de conformidad con lo dispuesto en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), los sujetos comprendidos en el artículo 2 de este real decreto podrán, **en la medida estrictamente necesaria y proporcionada**, analizar las*

comunicaciones entrantes o salientes, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

*Por otro lado, siendo la presente norma la que establece los correspondientes tratamientos de datos personales, **debería incluirse en dicho precepto o en los Anexos otras garantías adicionales concretas, derivadas de los demás principios del artículo 5 del RGPD**, como pueden ser, entre otros, el principio de limitación de la finalidad, prohibiendo el tratamiento de los datos personales para fines distintos; del principio de minimización de datos, identificando los datos personales o las categorías de datos personales que pudieran ser tratados; o del principio de limitación del plazo de conservación, identificando los plazos máximos de conservación de los datos personales.*

Estas cautelas deben ser especialmente rigurosas en lo que se refiere al análisis de las comunicaciones entrantes y salientes al que hace referencia el segundo párrafo del precepto, para evitar que se vulneren los derechos fundamentales de los afectados, incluido, además del de la protección de datos personales, el del secreto de las comunicaciones, cuya limitación requeriría norma con rango de ley ajustada a los principios señalados por la jurisprudencia del Tribunal Constitucional.

Tal y como resulta del citado informe, si la implementación de medidas de seguridad con otras finalidades (por ejemplo, continuidad de procesos,

seguridad física, seguridad del Estado, protección de la confidencialidad de la información, la propiedad intelectual o la industrial, etc.) supone un tratamiento adicional de datos personales deberá procederse al cumplimiento íntegro del RGPD y, en particular y como señala el propio Considerando 49, realizar un análisis de si el tratamiento es una medida “estrictamente necesaria y proporcionada”, para cuya valoración deberá contarse con el asesoramiento del DPD.

II

Teniendo en cuenta lo señalado anteriormente y en relación con la protección de datos de carácter personal, deben recordarse las importantes competencias que el RGPD atribuye a esta Agencia Española de Protección de Datos en cuanto autoridad de control independiente, que incluyen, partiendo de su función genérica de controlar la aplicación del RGPD y hacerlo aplicar, además de los poderes de investigación y correctivos, los poderes de autorización y consultivos entre los cuales se encuentran, conforme al artículo 58.3 del RGPD:

a) asesorar al responsable del tratamiento conforme al procedimiento de consulta previa contemplado en el artículo 36;

b) emitir, por iniciativa propia o previa solicitud, dictámenes destinados al Parlamento nacional, al Gobierno del Estado miembro o, con arreglo al Derecho de los Estados miembros, a otras instituciones y organismos, así como al público, sobre cualquier asunto relacionado con la protección de los datos personales;

En relación con la consulta previa del artículo 36, el mismo exige que la misma se realice “antes de proceder al tratamiento”. Este carácter previo de la consulta al inicio del tratamiento fue ya destacado, asimismo, por el Grupo del 29, predecesor del Comité Europeo de Protección de Datos Personales, en sus *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*, adoptadas definitivamente el 4 de octubre de 2017, página 18 y se destaca, igualmente, en la *Guía sobre Gestión del riesgo y evaluación de impacto en tratamientos de datos personales* elaborada por la AEPD.

Asimismo, debe tenerse en cuenta que uno de los principios recogidos en el RGPD, como manifestación del principio de responsabilidad proactiva, es el de protección de datos desde el diseño y por defecto contemplado en su artículo 25.

Por todo ello, dada la importancia de las competencias que el proyecto atribuye en materia de protección de datos personales y la incidencia que el

ejercicio de esas competencias puede tener respecto de la realización de dichos tratamientos en todo el sector público y al objeto de recoger adecuadamente la colaboración de la Agencia Estatal de Administración Digital con esta Agencia Española de Protección de Datos, permitiendo que esta última pueda ejercer adecuadamente sus poderes consultivos desde el diseño, debería incluirse un precepto específico en el que así se recogiera, proponiéndose la siguiente redacción:

Por otro lado, la disposición adicional centésima trigésima de la Ley 22/2021, de 28 de diciembre, de Presupuestos Generales del Estado para el año 2022 contempla, asimismo, la creación de la Agencia Española de Supervisión de Inteligencia Artificial en España a la que corresponderá llevar a cabo *“medidas destinadas a la minimización de riesgos significativos sobre la seguridad y salud de las personas, así como sobre sus derechos fundamentales, que puedan derivarse del uso de sistemas de inteligencia artificial. Estas medidas incluirán actuaciones propias, actuaciones en coordinación con otras autoridades competentes, cuando sea aplicable, y actuaciones de apoyo a entidades privadas”*.

Asimismo, *“se encargará del desarrollo, supervisión y seguimiento de los proyectos enmarcados dentro de la Estrategia Nacional de Inteligencia Artificial, así como aquellos impulsados por la Unión Europea, en particular los relativos al desarrollo normativo sobre inteligencia artificial y sus posibles usos”*

Atendiendo a dichas competencias, y sin perjuicio del preceptivo informe que deberá emitir esta AEPD cuando se proceda a la tramitación del estatuto de la Agencia Española de Supervisión de Inteligencia Artificial en España, teniendo en cuenta que dichas actuaciones deberán llevarse a cabo en colaboración con la Agencia Española de Protección de Datos en cuanto afecten al derecho fundamental a la protección de datos personales y, en el ámbito de sus competencias, con la Agencia Estatal de Administración Digital, con el objeto de articular adecuadamente dicha colaboración, debería reflejarse igualmente en el presente texto.

Artículo 6 Colaboración con la Agencia Española de Protección de Datos y con la Agencia Española de Supervisión de Inteligencia Artificial en España.

En particular, se adoptarán las medidas oportunas que faciliten una colaboración eficaz entre la Agencia y la Agencia Española de Protección de Datos, permitiendo recabar su asesoramiento temprano en relación con los tratamientos de datos de carácter personal, de conformidad con lo previsto en el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y en la Ley Orgánica 3/2018, de 5 de

diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Asimismo, se garantizará la adopción de medidas que garanticen la colaboración eficaz y temprana entre la Agencia, la Agencia Española de Supervisión de Inteligencia Artificial en España y la Agencia Española de Protección de datos en relación con los sistemas de inteligencia artificial.

III

Por otro lado, debe analizarse la posición jurídica que corresponderá a la Agencia Estatal de Administración Digital en relación con los tratamientos de carácter personal en los que participe.

Esta Agencia, en varias ocasiones, ha tenido ocasión de pronunciarse acerca de la naturaleza de responsables o encargados del tratamiento de los órganos de las Administraciones Públicas a los que se atribuyen reglamentariamente competencias en relación con el desarrollo, implantación y gestión de las herramientas de las tecnologías de la información y las comunicaciones de otros órganos de la correspondiente Administración, siendo irrelevante a tal efecto la existencia o inexistencia de una relación de dependencia orgánica entre el gestor de las aplicaciones o sistemas y el órgano que ostenta la competencia material que justifica el tratamiento de los datos. Del mismo modo, la Agencia ha analizado en determinados supuestos si la atribución de esas funciones de gestión, implantación y ejecución ha de entenderse suficiente para entender cumplidos los requisitos formales exigibles para que pueda apreciarse la existencia de un encargo del tratamiento.

A este respecto, debe destacarse el análisis realizado en el Informe 84/2018, en el que se concluía la condición de encargado del tratamiento de la Secretaría General de Administración Digital.

Más recientemente, tras la entrada en vigor de la LOPDGDD, en el Informe 79/2022, analizando las competencias que se atribuyen a la Dirección General de Transformación digital de la Administración de Justicia y después de recoger los sucesivos pronunciamientos de esta Agencia, señalábamos lo siguiente:

II

Los criterios indicados en los informes citados en el apartado anterior son plenamente aplicables a la presente consulta, atendiendo a las competencias que el ordenamiento jurídico atribuye a la Dirección General de Transformación Digital de la Administración de Justicia, quien ostentaría respecto de los tratamientos de datos personales en las aplicaciones y servicios digitales diseñados, desarrollados o en

mantenimiento por parte de la misma la condición de encargada del tratamiento, tal y como acertadamente se recoge en la propuesta remitida.

Tal y como ha venido señalando reiteradamente esta Agencia en relación con la atribución de la condición de responsable o encargado del tratamiento, son diferentes los supuestos que pueden darse, atendiendo a las circunstancias del caso concreto, la relación jurídica que se haya establecido entre los sujetos intervinientes y sus concretas obligaciones, así como las obligaciones que puedan venir impuestas por el ordenamiento jurídico para la correcta prestación del servicio, lo que será determinante al objeto de valorar si se actúa en condición de responsable del tratamiento o de encargado del tratamiento.

Para ello, es necesario partir de las definiciones que establece el RGPD en su artículo 4:

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; 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 miembros;

8) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

Como ya señalaba el Grupo del artículo 29, en su Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», el concepto de responsable era un concepto funcional dirigido a la asignación de responsabilidades, indicando que “El concepto de «responsable del tratamiento» y su interacción con el concepto de «encargado del tratamiento» desempeñan un papel fundamental en la aplicación de la Directiva 95/46/CE, puesto que determinan quién debe ser responsable del cumplimiento de las normas de protección de datos y la manera en que los interesados pueden ejercer sus derechos en la práctica. El concepto de responsable del tratamiento de datos también es esencial a la hora de determinar la legislación nacional aplicable y para el ejercicio eficaz de las tareas de supervisión conferidas a las autoridades de protección de datos”.

Asimismo, el citado Dictamen destacaba “las dificultades para poner en práctica las definiciones de la Directiva en un entorno complejo

en el que caben muchas situaciones hipotéticas que impliquen la actuación de responsables y encargados del tratamiento, solos o conjuntamente, y con distintos grados de autonomía y responsabilidad” y que “El Grupo reconoce que la aplicación concreta de los conceptos de responsable del tratamiento de datos y encargado del tratamiento de datos se está haciendo cada vez más compleja. Esto se debe ante todo a la creciente complejidad del entorno en el que se usan estos conceptos y, en particular, a una tendencia en aumento, tanto en el sector privado como en el público, hacia una diferenciación organizativa, combinada con el desarrollo de las TIC y la globalización, lo cual puede dar lugar a que se planteen cuestiones nuevas y difíciles y a que, en ocasiones, se vea disminuido el nivel de protección de los interesados”.

No obstante, en el momento actual, hay que tener en cuenta que el RGPD ha supuesto un cambio de paradigma al abordar la regulación del derecho a la protección de datos personales, que pasa a fundamentarse en el principio de «accountability» o «responsabilidad proactiva» tal y como ha señalado reiteradamente la AEPD (Informe 17/2019, entre otros muchos) y se recoge en la Exposición de motivos de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD): “la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan”. Dentro de este nuevo sistema, es el responsable del tratamiento el que, a través de los instrumentos regulados en el propio RGPD como el registro de actividades del tratamiento, el análisis de riesgos o la evaluación de impacto en la protección de datos personales, debe garantizar la protección de dicho derecho mediante el cumplimiento de todos los principios recogidos en el artículo 5.1 del RGPD, documentando adecuadamente todas las decisiones que adopte al objeto de poder demostrarlo.

Asimismo, partiendo de dicho principio de responsabilidad proactiva, dirigido esencialmente al responsable del tratamiento, y al objeto de reforzar la protección de los afectados, el RGPD ha introducido nuevas obligaciones exigibles no sólo al responsable, sino en determinados supuestos, también al encargado del tratamiento, quien podrá ser sancionado en caso de incumplimiento de las mismas.

A este respecto, las Directrices 07/2020 del Comité Europeo de Protección de Datos (CEPD) sobre los conceptos de responsable del tratamiento y encargado en el RGPD hacen especial referencia

(apartado 91) a la obligación del encargado de garantizar que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria (artículo 28, apartado 3); la de llevar un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable (Artículo 30.2); la de aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo (artículo 32); la de designar un delegado de protección de datos bajo determinadas condiciones (artículo 37) y la de notificar al responsable del tratamiento sin dilación indebida las violaciones de la seguridad de los datos personales de las que tenga conocimiento (artículo 33 (2)). Además, las normas sobre transferencias de datos a terceros países (capítulo V) se aplican tanto a los encargados como a los responsables. Y por ello el CEPD considera que el artículo 28 (3) del RGPD impone obligaciones directas a los encargados, incluida la obligación de ayudar al responsable del tratamiento a garantizar el cumplimiento.

Sin perjuicio de la atribución de obligaciones directas al encargado, las citadas Directrices, partiendo de que los conceptos de responsable y encargado del RGPD no han cambiado en comparación con la Directiva 95/46 / CE y que, en general, los criterios sobre cómo atribuir los diferentes roles siguen siendo los mismos (apartado 11), reitera que se trata de conceptos funcionales, que tienen por objeto asignar responsabilidades de acuerdo con los roles reales de las partes (apartado 12), lo que implica que en la mayoría de los supuestos deba atenderse a las circunstancias del caso concreto (case by case) atendiendo a sus actividades reales en lugar de la designación formal de un actor como "responsable" o "encargado" (por ejemplo, en un contrato), así como de conceptos autónomos, cuya interpretación debe realizarse al amparo de la normativa europea sobre protección de datos personales (apartado 13), y teniendo en cuenta (apartado 24) que la necesidad de una evaluación fáctica también significa que el papel de un responsable del tratamiento no se deriva de la naturaleza de una entidad que está procesando datos sino de sus actividades concretas en un contexto específico, por lo que la misma entidad puede actuar al mismo tiempo como responsable del tratamiento para determinadas operaciones de tratamiento y como encargado para otras, y la calificación como responsable o encargado debe evaluarse con respecto a cada actividad específica de procesamiento de datos.

En este mismo sentido se viene pronunciando nuestro Tribunal Supremo, tal y como se recoge en la Sentencia de 15 de junio de 2020:

“Fundamento de Derecho Quinto:

“(…) Argumentación que exige poner de manifiesto la consolidada doctrina de esta Sala que, de conformidad con las previsiones legales, tanto de la LOPD como del nuevo Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, distingue entre las figuras de responsable del tratamiento y de encargado del tratamiento. Diferencia que se contiene en los apartados d) y g) del artículo 3 de la LOPD, así como en el artículo 5.q) del Real Decreto 1720/2007 por el que se aprueba el Reglamento de desarrollo de la LOPD, siendo a tal responsable del tratamiento a quien la Ley impone las obligaciones derivadas del régimen jurídico de la protección de datos y quien ha de sufrir las sanciones junto al encargado del tratamiento (art. 43 LOPD) cuando dichas obligaciones no se respetan.

En tal sentido, ya la Sentencia del Tribunal Supremo de 5 de junio de 2004, que confirma, en casación para Unificación de Doctrina, la de esta AN de 16 de octubre de 2003, haciéndose eco de lo argumentado por esta Sala refiere la diferenciación de dos responsables en función de que el poder decisión vaya dirigido al fichero o al propio tratamiento de datos. Así, el responsable del fichero es quien decide la creación del fichero y su aplicación, y también su finalidad, contenido y uso, es decir, quien tiene capacidad de decisión sobre la totalidad de los datos registrados en dicho fichero. El responsable del tratamiento, sin embargo, es el sujeto al que cabe imputar las decisiones sobre las concretas actividades de un determinado tratamiento de datos, esto es, sobre una aplicación específica. Se trataría de todos aquellos supuestos en los que el poder de decisión debe diferenciarse de la realización material de la actividad que integra el tratamiento.

Con ello, como asimismo argumenta la STS de 26 de Abril de 2005 (casación para unificación de doctrina 217/2004), el legislador español pretende adaptarse a las exigencias de la Directiva 95/46/CE, que tiene como objetivo dar respuesta legal al fenómeno, que cada vez es más frecuente, de la llamada externalización de los servicios informáticos, donde actúan múltiples operadores, muchos de ellos insolventes, creados con el objetivo de buscar la impunidad o irresponsabilidad de los que le siguen en los eslabones siguientes de la cadena.

En la actualidad, el nuevo Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (por el que se deroga la Directiva 95/46/CE, y de aplicación directa a partir del 25 de mayo

de 2018) distingue asimismo entre las figuras del responsable y del encargado del tratamiento.

La primera se define en el apartado 7) del artículo 4 como "persona física o jurídica (...) que determine los fines y medios del tratamiento". Y el encargado de tratamiento en el apartado 8) del mismo artículo 4 como aquel que "trate datos personales por cuenta del responsable del tratamiento".

Ello en relación con los Artículos 24 y 28 del mismo Reglamento Europeo de Protección de Datos. Responsable y encargado del tratamiento de datos que, sin lugar a duda, resultan asimismo responsables de las infracciones en materia de protección de datos, en tal nuevo marco normativo, de conformidad con lo previsto en el artículo 82.2 del repetido Reglamento (UE) 2016/679 a cuyo tenor: Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente Reglamento. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del presente Reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable. (...)”

En el presente caso, tratándose de la actuación de organismos públicos, debe atenderse, tal y como se ha indicado en los informes anteriormente citados, a las normas jurídicas que atribuyen las correspondientes competencias, criterio recogido asimismo en las Directrices 07/2020 del CEPD, al referirse a los supuestos de control emanado de disposiciones legales:

22. En algunos casos, el control puede inferirse de una competencia legal explícita; p. ej., cuando la designación del responsable del tratamiento o los criterios específicos de su nombramiento se establecen en el Derecho nacional o de la UE. En este sentido, el artículo 4, punto 7, establece que «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 miembros». A pesar de que el artículo 4, punto 7, solo hace referencia al «responsable del tratamiento» en singular, el CEPD también considera posible que el Derecho de la Unión o de los Estados miembros designe más de un responsable del tratamiento, incluso en calidad de corresponsables del tratamiento.

23. Cuando el responsable del tratamiento se haya identificado expresamente en la normativa, esto se considerará determinante a la hora de establecer quién actúa como tal. Se presupone, por tanto, que el legislador ha designado como responsable del tratamiento al ente con verdadera capacidad para ejercer el control. En algunos países, el Derecho nacional establece que las autoridades públicas son responsables del tratamiento de datos personales en el marco de sus obligaciones.

24. No obstante, es más frecuente el caso en que la legislación, más que nombrar directamente al responsable del tratamiento o fijar los criterios para su nombramiento, establezca un cometido o imponga a alguien el deber de recoger y tratar determinados datos. En tales casos, el objetivo del tratamiento suele venir determinado por la ley. El responsable del tratamiento será normalmente el designado por la ley para cumplir este fin, este cometido público. Este sería, por ejemplo, el caso de un ente al que se le encargaran ciertos cometidos públicos (por ejemplo, la seguridad social) que no se pudieran cumplir sin recoger al menos algunos datos personales, y que, por tanto, creara una base de datos o un registro para realizar dichas tareas. En este caso, aunque indirectamente, la legislación establece quién es el responsable del tratamiento. Con mayor frecuencia, la ley puede imponer a entes públicos o privados la obligación de conservar o facilitar determinados datos. Estos entes se considerarían en principio los responsables del tratamiento necesario para cumplir esta obligación.

Por consiguiente, atendiendo a las competencias legalmente atribuidas, los órganos competentes del Ministerio de Justicia, así como los “juzgados, tribunales, fiscalías, oficinas judicial y fiscal, órganos técnicos auxiliares de la Administración de Justicia, unidades administrativas, órganos y organismos del departamento, así como de otras Administraciones, entidades e instituciones públicas” a los que se refiere la propuesta y respecto de los cuales la Dirección General de Transformación Digital de la Administración de Justicia pondrá a disposición las aplicaciones y servicios digitales, tendrán la consideración de responsables del tratamiento, y su base jurídica de legitimación para el tratamiento de los datos personales vendrá determinada por el cumplimiento de obligaciones legales o el ejercicio de poderes públicos (artículo 6.1.c) y e) del RGPD y artículo 8 de la LOPDGDD) o, en su caso, en el ejercicio de las competencias atribuidas con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la

protección y prevención frente a las amenazas contra la seguridad pública (artículo 1 y 11 de la Ley Orgánica 7/2021, de 26 de mayo).

Por su parte, la Dirección General de Transformación Digital de la Administración de Justicia ostentaría, conforme al criterio reiterado de esta Agencia, respecto de los tratamientos de datos personales objeto de consulta, la condición de encargado del tratamiento, atendiendo a las competencias específicas que a la misma le atribuyen los apartados d) y m) del artículo 6.1. del Real Decreto 453/2020, de 10 de marzo, por el que se desarrolla la estructura orgánica básica del Ministerio de Justicia, y se modifica el Reglamento del Servicio Jurídico del Estado, aprobado por el Real Decreto 997/2003, de 25 de julio, y cuya concreción se lleva a cabo en la propuesta remitida.

Las citadas competencias deben ponerse en relación con la previsión legal ya contemplada en el artículo 157 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, referido a la *Reutilización de sistemas y aplicaciones de propiedad de la Administración*, cuyo apartado 1 prevé que *“Las Administraciones pondrán a disposición de cualquiera de ellas que lo solicite las aplicaciones, desarrolladas por sus servicios o que hayan sido objeto de contratación y de cuyos derechos de propiedad intelectual sean titulares, salvo que la información a la que estén asociadas sea objeto de especial protección por una norma. Las Administraciones cedentes y cesionarias podrán acordar la repercusión del coste de adquisición o fabricación de las aplicaciones cedidas”*.

De este modo, la citada Dirección General no estaría tratando los datos personales para sus fines propios, sino que se trataría de una competencia atribuida normativamente para tratar datos personales por cuenta de los responsables del tratamiento.

Por consiguiente, nos encontramos en el supuesto previsto en el artículo 33.5 de la LOPDGDD:

5. En el ámbito del sector público podrán atribuirse las competencias propias de un encargado del tratamiento a un determinado órgano de la Administración General del Estado, la Administración de las comunidades autónomas, las Entidades que integran la Administración Local o a los Organismos vinculados o dependientes de las mismas mediante la adopción de una norma reguladora de dichas competencias, que deberá incorporar el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.

Los criterios recogidos en el citado informe son plenamente aplicables al presente caso, de modo que los respectivos sujetos integrantes del sector público a los que la Agencia Estatal de Administración Digital preste servicio tendrán la consideración de responsables del tratamiento, mientras que la Agencia actuará como encargado del tratamiento, debiendo darse cumplimiento a lo previsto en el citado artículo 33.5. de la LOPDGDD, que requiere que la norma reguladora de las competencias incorpore el contenido exigido por el artículo 28.3. del RGPD.

Por todo ello, debería incluirse la correspondiente disposición adicional, proponiéndose la siguiente redacción:

Disposición Adicional XXX. Protección de Datos Personales.

- 1. Los tratamientos de datos de carácter personal de las personas físicas se realizarán con estricta sujeción a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.**
- 2. En el tratamiento de datos de carácter personal en las aplicaciones y servicios digitales diseñados, desarrollados o en mantenimiento por parte de la Agencia Estatal de Administración Digital y que hayan sido creados o implantados en el ámbito de sus competencias y puestos a disposición de los órganos de la Administración General del Estado y de las demás Administraciones Públicas, así como de los organismos y entidades de derecho público vinculados o dependientes de las mismas, la Agencia tendrá la consideración de “Encargado del Tratamiento”, correspondiendo a aquéllos la consideración de “Responsable del Tratamiento”, en aplicación del Reglamento (UE) 2016/679.**
- 3. En su condición de encargado del tratamiento y conforme dispone el artículo 28.3 del Reglamento (UE) 2016/679, la Agencia Estatal de Administración Digital:**
 - a) Tratará los datos personales según las instrucciones de los órganos y organismos a cuya disposición se pusieran las aplicaciones y servicios digitales;**
 - b) Garantizará que las personas autorizadas a tratar los datos personales tienen contraído compromiso de confidencialidad, guarden secreto profesional sobre los mismos y no los**

- comuniquen a terceros, salvo en aquellos casos en que deba hacerse en estricto cumplimiento de la ley;
- c) Asistirá al órgano u organismo, a través de medidas técnicas y organizativas apropiadas y siempre que sea posible, para que pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos;
 - d) A la finalización de la puesta a disposición de las aplicaciones y servicios digitales, facilitará la devolución de los datos al órgano u organismo.
 - e) Pondrá a disposición del órgano u organismo beneficiario toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del órgano u organismo o de otro auditor autorizado por aquél.

Con esta redacción, además de darse cumplimiento al mandato legal, no sería ya necesario ningún otro acto jurídico expreso que conste por escrito con el contenido del artículo 28.3 del RGPD en ninguno de los casos en los que se pusieran a disposición de otros organismos las aplicaciones o servicios.

IV

Para concluir, como una medida específica dirigida a garantizar la adecuada protección de los datos de carácter personal y con el objeto de facilitar el ejercicio de sus funciones asesoras y supervisoras, **debería incluirse al delegado de protección de datos en el artículo 10, de modo que se garantice su asistencia a las sesiones del Consejo Rector con voz pero sin voto.**