0031/2026

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 de Orden Ministerial remitido tiene por objeto la aprobación del Sistema de Gobierno, gestión y calidad del dato (Sistema de Gobierno del dato) y de la Estrategia de Datos del Ministerio para la Transición Ecológica y el Reto demográfico (Estrategia).

Esta Estrategia se inspira en los principios recogidos en el Manifiesto por una Administración orientada al dato, impulsado por la Oficina del Dato del Ministerio para la Transformación Digital y de la Función Pública, y constituye el punto de partida de una estrategia global de gobernanza y explotación del dato en el ámbito del Ministerio para la Transición Ecológica y el Reto Demográfico, alineada con las obligaciones derivadas de la normativa europea y con las necesidades de una transición ecológica justa y basada en el conocimiento.

Todo ello se produce dentro del marco establecido por la Brújula Digital 2030, en base a la cual la Unión Europea ha situado la gestión del dato como pilar fundamental de una sociedad digital centrada en el ser humano, aprobando la Estrategia Europea de Datos, cuyo objetivo es posicionar a Europa como referente mundial en la creación de un espacio común de datos basado en la confianza.

La presente Orden se inserta en el contexto de la Estrategia Europea de Datos, presentada por la Comisión Europea en febrero de 2020, que impulsa la creación de espacios comunes europeos de datos como instrumentos destinados a facilitar el intercambio, reutilización y explotación de información en distintos sectores de actividad. El desarrollo normativo de dicha estrategia se ha materializado, entre otras iniciativas, en la aprobación del Reglamento (UE) 2022/868, relativo a la gobernanza europea de datos (DGA), y del Reglamento (UE) 2023/2854 (Data Act).

En España, la Agenda España Digital 2026 articula una visión integral de la digitalización en torno a tres ejes: infraestructuras y tecnología, economía y personas. Dentro del eje estratégico dedicado a la Economía del Dato y la

Inteligencia Artificial, se busca impulsar una transición hacia un modelo digital que promueva la innovación, mejore la competitividad, respalde la sostenibilidad ambiental y contribuya al bienestar social.

I

El proyecto de Orden Ministerial desarrolla el marco normativo establecido en el Real Decreto 503/2024, de 21 de mayo, por el que se regula la estructura orgánica básica del Ministerio para la Transición Ecológica y el Reto Demográfico (MITECO), y se alinea con los principios de la Agenda España Digital 2026 y la Estrategia Europea de Datos. Esta norma responde a la necesidad de consolidar un sistema de gobernanza, gestión y calidad del dato en el ámbito del MITECO, garantizando su interoperabilidad, seguridad y alineación con los estándares nacionales e internacionales, así como con los compromisos de sostenibilidad, innovación y modernización digital.

Según se recoge en la Memoria del Análisis de Impacto Normativo, la aprobación de esta Orden es esencial para:

- Establecer un marco de gobernanza del dato que asegure su gestión eficiente, segura y orientada al valor en todo el Departamento.

- Aprobar la Estrategia de Datos del MITECO, que define los principios, objetivos y líneas de acción para maximizar el valor de los datos como activo estratégico, promoviendo su reutilización, interoperabilidad y trazabilidad.

- Cumplir con las obligaciones derivadas del Derecho de la Unión Europea, en particular el Reglamento (UE) 2022/868 y el Reglamento (UE) 2023/2854, así como con las directrices de la Brújula Digital 2030.

El texto normativo consta de cinco artículos, una disposición adicional y dos disposiciones finales. El Artículo 1 define el objeto de la Orden: regular el Sistema de Gobierno, Gestión y Calidad del Dato y aprobar la Estrategia de Datos del MITECO, cuyo texto se incorpora como anexo. El Artículo 2 atribuye a la Subsecretaría, a través de la División de Estadística y Gestión de la Información, el desarrollo e impulso de este sistema. El Artículo 3 establece los principios rectores del modelo, como la agilidad en la gestión, la calidad continua y la adaptación a los recursos disponibles. El Artículo 4 crea el Consejo de Gobierno del Dato, máximo órgano de decisión para el impulso de la Estrategia, asistido por el Consejo de personas Coordinadoras y Gestoras de Datos. Finalmente, el Artículo 5 designa a la División de Estadística y Gestión

de la Información como Oficina del Dato, encargada de coordinar su implementación.

Como Anexo, se aprueba la Estrategia de Datos del MITECO, que define los principios, objetivos y líneas de acción para maximizar el valor de los datos como activo estratégico, promoviendo su reutilización, interoperabilidad y trazabilidad. Esta Estrategia se estructura en torno a ocho ejes fundamentales: fundamento y principios rectores, objetivos, categorías de datos, alcance y actores implicados, procesos clave, directrices para el sistema de gobierno, implementación y seguimiento, y un plan de formación y comunicación. Entre sus objetivos destacan la optimización de la toma de decisiones basada en evidencia, la eliminación de silos de información, la garantía de la calidad, seguridad y trazabilidad de los datos, y la promoción de una cultura organizativa basada en el dato.

En cuanto al fundamento competencial para su adopción, la presente Orden Ministerial se dicta al amparo del artículo 103.2 de la Constitución Española, que atribuye al Gobierno la potestad de autoorganización de la Administración, y del artículo 24.1.f) de la Ley 50/1997, de 27 de noviembre, del Gobierno, que establece que las disposiciones y resoluciones de los Ministros revestirán la forma de Órdenes Ministeriales. Además, se ajusta a lo dispuesto en la Disposición Final Segunda del Real Decreto 503/2024, de 21 de mayo, por el que se desarrolla la estructura orgánica básica del Ministerio para la Transición Ecológica y el Reto Demográfico, que faculta al titular del Departamento para adoptar las medidas necesarias para su desarrollo. La Orden se adecúa, asimismo, a los principios de buena regulación previstos en el artículo 129 de la Ley 39/2015, de 1 de octubre, al tratarse de una norma de carácter organizativo que no impone cargas administrativas a ciudadanos o entidades privadas, por lo que no ha sido necesario sustanciar los trámites de consulta pública previa ni de audiencia e información pública, de conformidad con lo establecido en los artículos 26.2.a) y 26.6 de la Ley 50/1997, de 27 de noviembre.

II

El presente informe tiene por objeto analizar las implicaciones en materia de protección de datos derivadas de la Orden Ministerial por la que se establece el Sistema de Gobierno, gestión y calidad del dato y se aprueba la Estrategia de Datos del Ministerio para la Transición Ecológica y el Reto Demográfico.

En el punto V de la Estrategia, “*Procesos clave*”, en el apartado relativo a la “*Gestión de seguridad del dato*”, se establece que:

"*Se garantizará la confidencialidad, integridad, disponibilidad y trazabilidad de los datos mediante:*

Clasificaciones de datos y alineamiento al Reglamento (UE) 2016/679 general de protección de datos (RGPD), al Esquema Nacional de Seguridad (ENS), o al estándar internacional ISO 27000: datos personales, categorías especiales de datos personales, datos relativos a condenas e infracciones, etc."

De este modo, la Estrategia contempla operaciones susceptibles de implicar el tratamiento de datos personales, en el sentido del artículo 4.1 del Reglamento (UE) 2016/679, esto es, toda información sobre una persona física identificada o identificable, incluidas categorías especiales de datos y datos relativos a condenas e infracciones penales, de manera que resultarán plenamente aplicables las previsiones del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD), así como de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

Tanto el Sistema de Gobierno del Dato como la Estrategia configuran un modelo de gestión, acceso, intercambio, reutilización y explotación de información sustentado en reglas comunes de gobernanza, calidad, trazabilidad e interoperabilidad, presentando las características propias de lo que, en el marco de la Estrategia Europea de Datos (COM/2020/66 final), viene denominándose un "espacio de datos".

Para realizar este informe deben tenerse especialmente en cuenta las orientaciones contenidas en el Dictamen conjunto 3/2021 del Comité Europeo de Protección de Datos y del Supervisor Europeo de Protección de Datos sobre la propuesta de Reglamento de Gobernanza de Datos (Dictamen conjunto). Aunque el Dictamen conjunto no utilice de forma sistemática la expresión «espacio de datos», dicho concepto constituye el marco en el que se desarrollan tanto el Reglamento de Gobernanza de Datos como las iniciativas nacionales de gobernanza y reutilización de la información.

Junto al Dictamen conjunto, deben observarse las previsiones del documento de la Agencia Española de Protección de Datos "*Aproximación a los Espacios de Datos desde la perspectiva del RGPD*" (Guía), en su versión de mayo de 2023.

Ambos documentos, tanto el Dictamen conjunto como la Guía, abordan la aplicación del RGPD a las iniciativas de gobernanza del dato y a los espacios de datos, por lo que proporcionan un marco interpretativo particularmente relevante para analizar la adecuación de la Orden Ministerial al RGPD, a la Ley Orgánica 3/2018 y a las exigencias derivadas del derecho

fundamental a la protección de datos personales reconocido en el artículo 18.4 de la Constitución Española.

Sin embargo, la Estrategia y el Sistema de Gobierno del Dato no deben ser analizados como si constituyeran por sí mismos un tratamiento de datos personales, debiendo examinarse desde la perspectiva de la protección de datos en cuanto establecen el marco organizativo, técnico y funcional dentro del cual se desarrollarán los futuros tratamientos. Por ello, el análisis debe distinguir claramente entre las garantías de gobernanza incorporadas al propio Espacio de Datos y las obligaciones específicas que deberán cumplirse posteriormente respecto de cada tratamiento concreto que utilice dicha infraestructura.

Esta caracterización resulta esencial, en la medida en que implica que la existencia de dichos espacios no altera ni sustituye el régimen jurídico del RGPD, ni genera por sí misma habilitaciones adicionales para el tratamiento de datos personales.

En consecuencia, resulta necesario examinar las implicaciones que dicho modelo organizativo puede presentar desde la perspectiva de la protección de datos personales cuando los tratamientos desarrollados en su seno afecten a información relativa a personas físicas identificadas o identificables.

Antes de entrar en el análisis del contenido concreto del proyecto normativo, procede examinar las normas con rango de ley que proporcionan cobertura jurídica al modelo organizativo proyectado, así como determinar el alcance material de la habilitación reglamentaria y sus límites desde la perspectiva del derecho fundamental a la protección de datos personales.

La Orden Ministerial debe analizarse, así, desde una doble perspectiva jurídica. Por un lado, como una disposición organizativa mediante la cual un Ministerio ordena internamente sus sistemas de información, sus flujos de datos y sus mecanismos de interoperabilidad, siendo este último uno de los principios rectores, punto II, de la Estrategia. Pero, por otro lado, como una norma que potencialmente articula una arquitectura de reutilización, circulación y gobernanza de información con incidencia directa sobre el derecho fundamental reconocido en el artículo 18.4 de la Constitución Española.

El análisis del proyecto normativo debe realizarse asimismo desde la perspectiva del derecho fundamental a la protección de datos reconocido en el artículo 18.4 de la Constitución Española, en conexión con el principio de reserva de ley del artículo 53.1 CE y el artículo 8 de la LOPDGDD. Conforme a esta configuración constitucional, cualquier limitación del derecho fundamental

exige una **habilitación legal suficiente** y respetuosa con el contenido esencial del derecho.

En este sentido, la jurisprudencia constitucional ha establecido criterios estrictos sobre la intervención normativa en materia de derechos fundamentales. Así, la Sentencia del Tribunal Constitucional 49/1999, de 5 de abril, recuerda que la ley habilitante "*ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención*" (FJ 4), mientras que la STC 292/2000, de 30 de noviembre, señala que la reserva de ley "*no sólo excluye apoderamientos a favor de las normas reglamentarias […], sino que también implica otras exigencias respecto al contenido de la Ley que establece tales límites*" (FJ 15). Asimismo, toda limitación del derecho fundamental deberá respetar en todo caso el principio de proporcionalidad, conforme recuerda la STC 14/2003, de 28 de enero.

Especial relevancia adquiere igualmente el Fundamento Jurídico 14 de la STC 292/2000, de 30 de noviembre, en relación con el alcance constitucionalmente admisible de las remisiones normativas a disposiciones reglamentarias en materia de circulación y cesión de datos entre Administraciones Públicas (comunicación de datos entre Administraciones Públicas):

"14. Pese a la importancia que para garantizar el ejercicio del derecho fundamental poseen los derechos del interesado a ser informado y a consentir la cesión de sus datos personales, como antes se ha declarado, sin embargo, es suficiente según el art. 21.1 LOPD que la comunicación de tales datos entre Administraciones Públicas, para el ejercicio de competencias diferentes o que versen sobre materias distintas, sea autorizada por una norma reglamentaria. Al respecto, ya hemos dicho [STC 127/1994, FJ 5, con remisión a la STC 83/1984, FJ 4, y 99/1987, FJ 3 a)] que incluso en los ámbitos reservados por la Constitución a la regulación por Ley no es imposible una intervención auxiliar o complementaria del Reglamento, pero siempre que estas remisiones restrinjan efectivamente el ejercicio de esa potestad reglamentaria a un complemento de la regulación legal que sea indispensable por motivos técnicos o para optimizar el cumplimiento de las finalidades propuestas por la Constitución o por la propia Ley. De tal modo que esa remisión no conlleve una renuncia del legislador a su facultad para establecer los límites a los derechos fundamentales, transfiriendo esta facultad al titular de la potestad reglamentaria, sin fijar ni siquiera cuáles son los objetivos que la reglamentación ha de perseguir, pues, en tal caso, el legislador no haría sino "deferir a la normación del Gobierno el objeto mismo reservado" (STC 227/1993, de 9 de julio, FJ 4, recogiendo la expresión de la STC 77/1985, de 27 de junio, FJ 14).

La remisión a la regulación reglamentaria de materia ligada a la reservada a la Ley es preciso, pues, que se formule en condiciones tales que

no contraríe materialmente la finalidad de la reserva, de la cual se derivan, según la STC 83/1984, "ciertas exigencias en cuanto al alcance de las remisiones o habilitaciones legales a la potestad reglamentaria, que pueden resumirse en el criterio de que las mismas sean tales que restrinjan efectivamente el ejercicio de esa potestad a un complemento de la regulación legal que sea indispensable por motivos técnicos o para optimizar el cumplimiento de las finalidades propuestas por la Constitución o por la propia Ley". Es en este segundo plano en el que se encuentra el núcleo argumental del recurso interpuesto por el Defensor del Pueblo que es acogido en esta Sentencia, el cual considera que al establecer el art. 21.4 LOPD que esas cesiones no requieren del previo consentimiento del afectado permite al reglamento imponer un límite al derecho fundamental a la protección de datos personales, que como se ha dicho ya, defrauda la previsión del art. 53.1 de la Constitución (STC 101/1991, de 13 de mayo, FJ 3).

En conclusión, el Tribunal Constitucional admite la posibilidad de una intervención auxiliar o complementaria del reglamento incluso en ámbitos sujetos a reserva de ley, pero únicamente cuando dicha remisión se limite a aspectos técnicos u organizativos indispensables para optimizar el cumplimiento de las finalidades legalmente establecidas, sin que pueda producirse una transferencia al reglamento de la definición material de los límites del derecho fundamental ni de las condiciones esenciales de legitimación de los tratamientos.

Esta doctrina resulta particularmente relevante en el contexto de los sistemas de gobierno del dato y de los espacios de datos, en los que la arquitectura normativa puede incidir de forma estructural en la circulación de información entre entidades, en la medida en que dichos sistemas permiten articular mecanismos complejos de circulación, reutilización y tratamiento compartido de información entre múltiples entidades, sistemas y plataformas tecnológicas, incluyendo eventualmente datos personales sometidos al ámbito de aplicación del RGPD.

Por consiguiente, antes de entrar en el análisis del contenido concreto del proyecto normativo, procede examinar las normas con rango de ley que proporcionan cobertura jurídica al modelo organizativo proyectado, así como determinar el alcance material de la habilitación reglamentaria y sus límites desde la perspectiva del derecho fundamental a la protección de datos personales.

Este apartado tiene por objeto determinar si el ordenamiento jurídico vigente proporciona una base legal suficiente para la implantación de un sistema de gobierno del dato en el ámbito de la Administración, así como delimitar el alcance de las habilitaciones contenidas en la legislación sectorial aplicable. En particular, se analiza si dichas normas permiten no solo la

organización de los sistemas de información, sino también la configuración de flujos de datos y mecanismos de reutilización en el marco de la estrategia de datos de la Administración.

En el marco del desarrollo de estrategias de dato, espacios de datos y modelos de interoperabilidad administrativa, debe partirse de que tales instrumentos constituyen **mecanismos organizativos, técnicos y de gobernanza** destinados a facilitar el acceso, intercambio, reutilización y control de la información dentro de las Administraciones Públicas y de los ecosistemas digitales asociados. Su finalidad principal consiste en ordenar y racionalizar los flujos de información, garantizar la interoperabilidad, mejorar la calidad del dato y facilitar modelos de gestión basados en el uso eficiente de la información.

Las previsiones contenidas en la Ley 40/2015, de Régimen Jurídico del Sector Público (LRJSP), y particularmente los principios de eficacia, coordinación, interoperabilidad, racionalización y cooperación administrativa recogidos en su artículo 3, proporcionan cobertura organizativa suficiente para la implantación de modelos corporativos de gobierno del dato, así como para la aprobación de estructuras de gestión, catalogación y coordinación de la información en el ámbito de la Administración General del Estado.

Del mismo modo, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), al configurar el procedimiento y el expediente administrativos en formato electrónico (artículo 70.2) y reconocer el derecho y, en determinados casos, la obligación de relacionarse electrónicamente con las Administraciones Públicas (artículo 14), hace necesaria la implantación de mecanismos avanzados de gestión, interoperabilidad, trazabilidad y gobernanza de la información pública.

Asimismo, la Ley 37/2007, sobre reutilización de la información del sector público, proporciona un fundamento específico para promover políticas de reutilización y apertura de información pública, especialmente respecto de información no personal o adecuadamente anonimizada, en línea con la Directiva (UE) 2019/1024 sobre datos abiertos y reutilización de la información del sector público.

En consecuencia, desde el punto de vista organizativo y funcional, existe cobertura legal suficiente para que un Ministerio cree un Sistema de Gobierno, gestión y calidad del dato como instrumento de aplicación de la Estrategia de Datos, así como la aprobación de esta misma.

No obstante, estas normas cumplen esencialmente una función organizativa, estructural y de habilitación institucional de los espacios de datos, sin que de ellas pueda derivarse, por sí sola, una base jurídica suficiente para legitimar nuevos tratamientos o reutilizaciones de datos personales. La competencia de una Administración para organizar sus sistemas de información

y establecer mecanismos de interoperabilidad no habilita autónomamente cualquier reutilización o tratamiento ulterior de datos personales, ni convierte la interoperabilidad, la transformación digital o la reutilización de información en bases jurídicas independientes de legitimación del tratamiento.

Por lo tanto, todo tratamiento de datos personales que se realice en el marco del Sistema de Gobierno del Dato deberá encontrar su **base jurídica** en el artículo 6 del RGPD, ya sea en el cumplimiento de una obligación legal del responsable del tratamiento conforme al artículo 6.1.c), o en el ejercicio de poderes públicos o misión realizada en interés público conforme al artículo 6.1.e), en conexión con el artículo 8 de la LOPDGDD, que exige que dicha misión derive de una norma con rango de ley.

III

En este primer plano de análisis no se examinan tratamientos concretos, sino la adecuación del marco de gobernanza que soportará los futuros tratamientos. El análisis se estructura en torno a los elementos esenciales que deben conformar una arquitectura de datos compatible con el RGPD desde el diseño.

El Dictamen conjunto advierte expresamente del riesgo de que los marcos de reutilización y gobernanza de datos puedan derivar en regímenes paralelos o excepcionales respecto del sistema europeo de protección de datos, subrayando la necesidad de que el RGPD se integre de forma estructural en el diseño de estos sistemas y no como una referencia accesoria o meramente declarativa.

Desde esta perspectiva, la Estrategia y el Sistema de Gobierno del Dato constituyen instrumentos de planificación, organización, interoperabilidad y gobernanza de la información destinados a facilitar el acceso, compartición, reutilización y explotación de datos dentro del ecosistema definido por la Orden Ministerial. Sin embargo, como ya se dijo anteriormente, ni la Estrategia ni el propio Sistema constituyen por sí mismos tratamientos de datos personales ni generan bases jurídicas autónomas para dichos tratamientos.

La Orden Ministerial prevé la existencia de estructuras de gobernanza específicas, singularmente el Consejo de Gobierno del Dato y la Oficina del Dato, artículos 4 y 5 respectivamente. No obstante, las funciones atribuidas a dichos órganos deberán entenderse sin perjuicio de las obligaciones y responsabilidades que correspondan, en cada caso, conforme al RGPD, a los responsables, encargados o corresponsables del tratamiento, en función de las concretas funciones efectivamente desempeñadas en relación con los tratamientos de datos personales.

La existencia de infraestructuras interoperables y mecanismos compartidos de reutilización de información puede dar lugar a escenarios complejos de distribución de responsabilidades entre las distintas entidades participantes. En consecuencia, deberá evitarse que la mera pertenencia al Sistema de Gobierno del Dato o la participación en sus órganos de gobernanza determine automáticamente la atribución de la condición de responsable, corresponsable o encargado del tratamiento, debiendo dicha calificación realizarse atendiendo a las funciones efectivamente desempeñadas en cada tratamiento concreto conforme a los artículos 4.7, 4.8, 26 y 28 del RGPD.

Asimismo, resulta conveniente que la arquitectura de gobernanza permita identificar claramente las responsabilidades funcionales y organizativas asociadas a la gestión de los activos de información, la autorización de accesos y reutilizaciones, la supervisión del cumplimiento de las políticas de gobierno del dato y la administración técnica de la infraestructura.

Igualmente, deberá garantizarse la intervención del Delegado de Protección de Datos en aquellos tratamientos de datos personales que se desarrollen en el marco del Sistema de Gobierno del Dato y de la Estrategia de Datos, especialmente en relación con las evaluaciones de impacto, la supervisión del cumplimiento normativo y el asesoramiento en materia de protección de datos, de conformidad con los artículos 37 a 39 del RGPD y el artículo 34 de la LOPDGDD.

Por último, se recomienda que el Sistema de Gobierno del Dato incorpore mecanismos organizativos de verificación previa a la admisión de nuevos casos de uso o iniciativas de reutilización, orientados a comprobar que las entidades promotoras han identificado adecuadamente las implicaciones en materia de protección de datos personales y han previsto, cuando resulte exigible, la realización de las evaluaciones de impacto y demás medidas previstas en la normativa aplicable.

Esta recomendación se fundamenta en los principios de responsabilidad proactiva y protección de datos desde el diseño establecidos en los artículos 24 y 25 del RGPD, sin que ello implique la asunción por los órganos de gobernanza de las obligaciones o responsabilidades que corresponden a los responsables de los tratamientos concretos, ni una validación sustantiva de la licitud de los tratamientos.

El artículo 6.4 del RGPD exige valorar la compatibilidad entre la finalidad inicial del tratamiento y cualquier finalidad ulterior, teniendo en cuenta factores tales como la relación entre ambas finalidades, el contexto en el que se recogieron los datos, la naturaleza de la información tratada y las posibles consecuencias para los interesados. En el ámbito de las Administraciones

Públicas, dicha valoración deberá realizarse además de conformidad con el artículo 6.3 del RGPD, el artículo 8 de la LOPDGDD y el principio de reserva de ley.

Esta exigencia resulta particularmente relevante en entornos de gobierno del dato, interoperabilidad y reutilización de información, en los que pueden producirse intercambios transversales entre distintas unidades administrativas, organismos públicos y, en su caso, otras entidades participantes.

La Estrategia, en el punto 2 del apartado I, "*Fundamento*", prevé expresamente la promoción de la interoperabilidad entre direcciones generales y la reutilización de datos considerados críticos para la gestión de políticas públicas, así como la puesta a disposición de conjuntos de datos reutilizables e interoperables para favorecer la investigación, la innovación y la transparencia institucional.

A este respecto, se considera conveniente que el Sistema de Gobierno del Dato establezca mecanismos que permitan identificar las finalidades originarias asociadas a los distintos conjuntos de datos, así como las condiciones bajo las cuales pueden producirse reutilizaciones posteriores por parte de los responsables del tratamiento.

Dichas reutilizaciones deberán basarse preferentemente en finalidades previamente definidas y documentadas, siempre que resulten compatibles con la finalidad inicial y con la base jurídica que legitimó el tratamiento originario, conforme al artículo 6.4 del RGPD.

Cuando la reutilización proyectada exceda materialmente el ámbito de la finalidad inicial, altere sustancialmente el contexto del tratamiento o no resulte compatible con la misión pública o base jurídica que justificó la recogida de los datos, corresponderá a los responsables del tratamiento identificar una nueva finalidad y la correspondiente base jurídica habilitante. En ningún caso las finalidades podrán entenderse implícitamente autorizadas por la mera existencia del Espacio de Datos o de sus infraestructuras de gobernanza.

El Sistema deberá articularse de forma respetuosa con los principios previstos en el artículo 5 del RGPD, que resultan aplicables a todo tratamiento de datos personales. Estos principios comprenden la licitud, lealtad y transparencia; la limitación de la finalidad; la minimización de datos; la exactitud; la limitación del plazo de conservación; la integridad y confidencialidad; y la responsabilidad proactiva.

La Orden Ministerial contempla mecanismos de clasificación, catalogación y gestión de activos de información. No obstante, dichos instrumentos deberán diseñarse de forma compatible con los principios de

protección de datos personales en los términos en que resulten aplicables a los tratamientos efectivamente realizados.

En particular, los mecanismos de catalogación, gestión de metadatos, trazabilidad y reutilización de información deberán permitir documentar adecuadamente la procedencia de los datos, las condiciones de acceso y reutilización, las finalidades asociadas, las restricciones aplicables y los responsables de gestión de cada conjunto de datos.

Asimismo, deberán facilitar que las operaciones de acceso, circulación y reutilización de información queden suficientemente delimitadas, documentadas y sujetas a mecanismos efectivos de control y supervisión.

También deberán observarse las exigencias derivadas de los artículos 24 y 25 del RGPD relativas a la responsabilidad proactiva y a la protección de datos desde el diseño y por defecto.

Aunque la Estrategia no define tratamientos concretos, sí configura la arquitectura organizativa y tecnológica sobre la que dichos tratamientos podrán desarrollarse. En consecuencia, resulta conveniente que incorpore mecanismos que favorezcan la aplicación efectiva de los principios de protección de datos, incluyendo la minimización de accesos, la segregación funcional de entornos, la gestión granular de permisos, la trazabilidad de operaciones y la existencia de procedimientos de evaluación y autorización de nuevas reutilizaciones de información.

La Guía de la Agencia Española de Protección de Datos sobre espacios de datos insiste en la necesidad de integrar en estos ecosistemas mecanismos de gobernanza, trazabilidad, delimitación de finalidades, gestión del riesgo y control efectivo de las reutilizaciones de información, evitando que la interoperabilidad o la compartición de datos generen, por sí mismas, nuevas habilitaciones para el tratamiento de datos personales.

Asimismo, cuando la naturaleza de los datos y las finalidades perseguidas lo permitan, deberán promoverse técnicas de seudonimización u otras medidas orientadas a reducir la identificación directa de las personas afectadas y a minimizar la circulación de datos personales dentro del ecosistema. La utilización de estas técnicas deberá valorarse desde las fases iniciales de diseño de los sistemas y casos de uso, sin perjuicio de la necesidad de analizar los riesgos de reidentificación que puedan derivarse de la combinación de conjuntos de datos procedentes de distintas fuentes.

Los sistemas de trazabilidad, compartición y reutilización de información previstos en la Estrategia deberán incorporar garantías adecuadas de

integridad, confidencialidad y control de accesos, permitiendo acreditar el cumplimiento de las obligaciones derivadas del RGPD y del principio de responsabilidad proactiva.

La Estrategia debería prever mecanismos que permitan conocer el ciclo completo de vida de los datos, incluyendo su origen, transformaciones, accesos, reutilizaciones, cesiones y operaciones de explotación realizadas. Asimismo, deberán incorporarse capacidades de auditoría y registro que permitan identificar quién accede a la información, cuándo lo hace, con qué finalidad y bajo qué condiciones de utilización.

Deberán adoptarse las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, de conformidad con el artículo 32 del RGPD y con el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y con el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

Tanto el Dictamen conjunto 3/2021 del CEPD y del SEPD como la Guía de la Agencia Española de Protección de Datos destacan que los espacios de datos presentan riesgos específicos derivados de la acumulación progresiva de información, de la reutilización secundaria de datos y de la posibilidad de usos incompatibles con las finalidades inicialmente previstas.

Por ello, el principal ámbito de análisis de la Estrategia desde la perspectiva de la protección de datos debe situarse en la configuración de los mecanismos de gobernanza, reutilización, control, trazabilidad y supervisión de la información. Por el contrario, cuestiones tales como la determinación de las categorías de datos personales tratadas, la existencia de categorías especiales de datos o de datos relativos a condenas e infracciones penales, la concreta base jurídica del tratamiento, la necesidad de realizar evaluaciones de impacto o la determinación de responsables y encargados deberán analizarse respecto de cada tratamiento concreto que se implemente mediante el Espacio de Datos.

No obstante, cuando la propia Estrategia o el Sistema de Gobierno del Dato prevean expresamente tratamientos que eventualmente afecten a categorías especiales de datos personales o a datos relativos a condenas e infracciones penales, la mera remisión genérica al cumplimiento del RGPD o a la adopción futura de medidas técnicas y organizativas apropiadas podría resultar insuficiente. En tales supuestos, y conforme a la doctrina constitucional, entre otras, de la STC 76/2019, las garantías esenciales aplicables al tratamiento no deberían quedar completamente indeterminadas ni remitidas íntegramente a desarrollos posteriores, debiendo existir una delimitación suficiente de las finalidades perseguidas, categorías de datos

afectadas, condiciones de reutilización y mecanismos básicos de garantía aplicables.

IV

Sin perjuicio de las consideraciones anteriores relativas a la gobernanza, supervisión y funcionamiento del Sistema de Gobierno del Dato, todo caso de uso, proyecto, servicio o actividad que implique el tratamiento de datos personales mediante la infraestructura del Espacio de Datos deberá someterse al correspondiente análisis de conformidad con el Reglamento (UE) 2016/679 (RGPD), la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), así como el resto de normativa sectorial aplicable.

Tal y como señalan la Guía de la Agencia Española de Protección de Datos sobre espacios de datos y el Dictamen conjunto 3/2021 del Comité Europeo de Protección de Datos y del Supervisor Europeo de Protección de Datos sobre la propuesta de Reglamento de Gobernanza de Datos, la existencia de una infraestructura de compartición, reutilización o explotación de información no sustituye ni altera las obligaciones derivadas de la normativa de protección de datos respecto de los tratamientos concretos realizados en su seno.

Deberá analizarse, con carácter previo, si la información objeto del caso de uso constituye datos personales en los términos del artículo 4.1 del RGPD o si, por el contrario, se trata de datos efectivamente anonimizados o de información no personal.

Asimismo, deberán identificarse y documentarse las finalidades concretas perseguidas por el tratamiento, verificando su correspondencia con las competencias, funciones o misiones legalmente atribuidas a las entidades participantes.

Todo tratamiento de datos personales deberá apoyarse en una base jurídica válida de las previstas en el artículo 6 del RGPD. En el ámbito de las Administraciones Públicas, dicha base jurídica se sustentará normalmente en el cumplimiento de una obligación legal del responsable del tratamiento conforme al artículo 6.1.c) del RGPD o en el ejercicio de poderes públicos o el cumplimiento de una misión realizada en interés público conforme al artículo 6.1.e), en relación con el artículo 8 de la LOPDGDD y con la correspondiente habilitación establecida por el Derecho de la Unión o por una norma con rango de ley.

La pertenencia al Espacio de Datos, la existencia del Sistema de Gobierno del Dato o la mera disponibilidad técnica de la información no

constituyen, por sí mismas, bases jurídicas habilitantes para el tratamiento de datos personales.

Cuando los datos hayan sido obtenidos inicialmente para una finalidad distinta, deberá analizarse la compatibilidad entre la finalidad originaria y la finalidad ulterior conforme a los criterios previstos en el artículo 6.4 del RGPD. La compatibilidad de finalidades debe analizarse conjuntamente con la habilitación legal de la misión de interés público o del ejercicio de potestades públicas. Cuando la reutilización exceda del marco de compatibilidad o altere sustancialmente el contexto inicial del tratamiento, deberá identificarse una nueva base jurídica que legitime el tratamiento ulterior.

De acuerdo con el punto III de la Estrategia se establecen diversas clasificaciones relativas a las categorías de datos que vayan a ser objeto de tratamiento. Respecto a los diversos tratamientos que vayan a efectuarse en dicho espacio, deberán identificarse con precisión las categorías de datos personales utilizadas en cada tratamiento, su procedencia, alcance y nivel de detalle, verificando en todo momento el cumplimiento del principio de minimización previsto en el artículo 5.1.c) del RGPD.

La determinación de las categorías de datos afectadas constituye un elemento esencial para la evaluación de los riesgos asociados al tratamiento y para la identificación de las garantías que resulten exigibles.

Cuando el tratamiento implique categorías especiales de datos contempladas en el artículo 9 del RGPD o datos relativos a condenas e infracciones penales a que se refiere el artículo 10 del mismo Reglamento, deberán identificarse expresamente las circunstancias habilitantes que permitan su tratamiento y verificarse el cumplimiento de las garantías reforzadas previstas por la normativa aplicable.

Además de la concurrencia de una base jurídica conforme al artículo 6 del RGPD, será necesaria la existencia de alguna de las circunstancias previstas en el artículo 9.2 del Reglamento o, en el caso de los datos relativos a condenas e infracciones penales, la correspondiente habilitación legal o el control por una autoridad pública competente.

La reutilización de estas categorías de datos exigirá una interpretación especialmente restrictiva de los criterios de compatibilidad de finalidades, necesidad y minimización, así como la adopción de medidas técnicas y organizativas reforzadas. Entre ellas podrán incluirse técnicas de seudonimización o anonimización, compartimentación organizativa, utilización de entornos seguros de tratamiento y mecanismos reforzados de auditoría, trazabilidad y control de accesos.

La reutilización de estas categorías de datos no podrá fundamentarse exclusivamente en criterios generales de interoperabilidad, eficiencia administrativa o explotación analítica de la información.

Respecto de cada tratamiento concreto desarrollado mediante el Espacio de Datos, deberá determinarse de forma precisa la condición de responsable, corresponsable o encargado del tratamiento, atendiendo a la capacidad efectiva de cada entidad para determinar los fines y medios del tratamiento y formalizando, cuando proceda, los instrumentos previstos en los artículos 26 y 28 del RGPD.

Esta identificación no deberá derivarse de forma automática de la participación en el Espacio de Datos o en el Sistema de Gobierno del Dato, sino de un análisis funcional de las actividades efectivamente desarrolladas por cada entidad participante.

Con carácter previo al tratamiento deberán evaluarse los riesgos para los derechos y libertades de las personas afectadas atendiendo a la naturaleza, alcance, contexto y finalidades de la operación.

Los tratamientos desarrollados en entornos de interoperabilidad y reutilización intensiva de información pueden presentar factores de riesgo especialmente relevantes, tales como el tratamiento masivo de datos, la combinación de conjuntos de datos procedentes de múltiples fuentes, la utilización de nuevas tecnologías, la existencia de categorías especiales de datos o el tratamiento de información relativa a colectivos vulnerables.

En este contexto, deberá valorarse la procedencia de realizar una evaluación de impacto relativa a la protección de datos conforme al artículo 35 del RGPD, especialmente cuando concurran los criterios identificados por las Directrices del antiguo Grupo de Trabajo del Artículo 29 y por las listas publicadas por la Agencia Española de Protección de Datos.

Cuando proceda, también deberá valorarse la necesidad de realizar consulta previa a la autoridad de control conforme al artículo 36 del RGPD.

En aquellos supuestos en los que el tratamiento incorpore mecanismos de elaboración de perfiles o decisiones automatizadas, deberá analizarse la aplicación de los artículos 4.4 y 22 del RGPD.

Cuando las decisiones se basen exclusivamente en tratamientos automatizados y produzcan efectos jurídicos o significativamente similares para

los interesados, deberán garantizarse las salvaguardas previstas en dicho precepto, incluyendo la posibilidad de intervención humana significativa, la revisión de la decisión y el ejercicio de los derechos reconocidos por la normativa de protección de datos.

Deberán implantarse medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, de conformidad con los artículos 24, 25 y 32 del RGPD, así como con el Esquema Nacional de Seguridad y el resto de normativa sectorial aplicable.

Entre otras medidas, deberán valorarse mecanismos de seudonimización, cifrado, segregación de funciones, control de accesos, gestión de privilegios, registro de actividades, trazabilidad de operaciones, monitorización continua y utilización de entornos seguros de tratamiento cuando resulte necesario.

Deberán analizarse específicamente las comunicaciones de datos entre entidades participantes, los accesos por terceros, las posibles transferencias internacionales y cualquier otra operación que implique circulación de información fuera del ámbito inicialmente previsto, verificando la concurrencia de las condiciones jurídicas exigidas por el RGPD.

Los tratamientos deberán incorporar mecanismos organizativos y procedimentales que permitan garantizar el ejercicio efectivo de los derechos reconocidos en los artículos 12 a 22 del RGPD, incluyendo los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y, cuando proceda, portabilidad.

Particularmente en entornos interoperables en los que intervengan múltiples entidades o sistemas, deberán establecerse mecanismos de coordinación, trazabilidad y gestión que permitan determinar con claridad los puntos de contacto y los procedimientos aplicables para la atención de los derechos de los interesados.

Todos los tratamientos desarrollados mediante el Espacio de Datos deberán documentarse adecuadamente y quedar sujetos a mecanismos de supervisión, revisión y control que permitan acreditar el cumplimiento efectivo de la normativa de protección de datos, de conformidad con el principio de responsabilidad proactiva previsto en el artículo 5.2 del RGPD.

A tal efecto, deberán mantenerse actualizados los registros de actividades de tratamiento, los análisis de riesgos, las evaluaciones de impacto

que resulten exigibles y la documentación acreditativa de las medidas técnicas y organizativas implantadas

V

A la vista del análisis precedente, la correcta integración del Reglamento (UE) 2016/679 en el marco de la Estrategia de Datos y del Sistema de Gobierno del Dato **exige entender dichos instrumentos como elementos de carácter organizativo y de planificación, que no constituyen por sí mismos habilitaciones jurídicas para el tratamiento de datos personales ni sustituyen el régimen de garantías establecido por la normativa de protección de datos**.

En este sentido, la existencia del Espacio de Datos, de sus infraestructuras de interoperabilidad o de sus mecanismos de reutilización **no puede interpretarse como una habilitación implícita o automática para el tratamiento de datos personales, siendo en todo caso necesario que cada operación de tratamiento se fundamente en una base jurídica específica conforme al artículo 6 del RGPD y, en su caso, a los artículos 9 y 10 del mismo Reglamento, en relación con la normativa nacional aplicable.**

Asimismo, la arquitectura del Sistema de Gobierno del Dato debe entenderse sin perjuicio del principio de determinación funcional de responsabilidades, de modo que la condición de responsable, corresponsable o encargado del tratamiento no deriva de la mera pertenencia al Sistema, sino del análisis concreto de las actividades de tratamiento efectivamente desarrolladas.

Del mismo modo, la reutilización de datos en entornos interoperables debe sujetarse estrictamente al principio de limitación de la finalidad y a los criterios de compatibilidad previstos en el artículo 6.4 del RGPD, evitando interpretaciones extensivas que deriven de la mera disponibilidad técnica de los datos o de la existencia de infraestructuras compartidas.

Por último, la correcta aplicación del modelo exige que las garantías previstas en el RGPD se concreten en cada tratamiento específico que se lleve a cabo en el marco del espacio de datos, sin que la existencia de mecanismos generales de gobernanza sustituya la necesidad de análisis individualizado de licitud, riesgo y garantías.