

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 anteproyecto de ley remitido persigue un triple objeto, al establecer:

a) El proceso de co-gobernanza por el cual el Estado y las comunidades autónomas adoptarán por acuerdo unas condiciones básicas que aseguren la igualdad en el ejercicio de los derechos sociales derivados del capítulo tercero de la Constitución Española cuando estos dependen de cuidados y apoyos sociales prestados por los servicios sociales.

b) La gobernanza de la red integrada de sistemas públicos de servicios sociales y las formas de colaboración entre las diferentes Administraciones Públicas y otras entidades interesadas para desarrollar los preceptos incluidos en esta ley.

c) Un sistema estable de Información Estatal de Servicios Sociales que facilite el conocimiento real y efectivo de la red integrada de sistemas públicos de servicios sociales, de cara a lograr evaluar, basándose en evidencias, el despliegue, la eficacia y la eficiencia de los servicios sociales, una adecuada planificación de los recursos y la adaptación de los mismos a las necesidades cambiantes de la sociedad.

I

El marco normativo aplicable a los tratamientos de datos de carácter personal que puedan realizarse al amparo de la norma proyectada está constituido, con carácter general, 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).

Desde esta perspectiva, de dicha regulación destacan las siguientes cuestiones, que serán objeto de análisis en el presente informe: a) la aplicación, con carácter general, de la normativa sobre protección de datos personales a los tratamientos de datos personales por parte de la red integrada de sistemas públicos de servicios sociales; b) la creación del Sistema de Información Estatal de Servicios Sociales; c) la regulación de la historia social única en formato digital y el correspondiente intercambio de información.

En cuanto a la primera de las cuestiones, resulta innegable la aplicación de la normativa sobre protección de datos personales a los diferentes tratamientos de este tipo de datos que puedan realizarse por los servicios sociales, de los cuales serán responsables, en primer término, las Comunidades Autónomas correspondientes, dada la competencia que en esta materia les atribuye el artículo 148.1.20 de la Constitución, así como, en su caso, las entidades locales con competencias en la materia.

Esta cuestión es tratada en el texto remitido si bien de manera limitada, centrándose en aspectos parciales de la protección derivada de este derecho fundamental, como es la relativa a la seguridad de los datos y, más concretamente, a la confidencialidad. En este sentido, al artículo 11.1.l) incluye entre los derechos de las personas el de *“Confidencialidad, protección de datos y secreto profesional de cuanta información conste en su expediente personal, así como la disponibilidad de espacios de atención adecuados que garanticen la intimidad de las personas usuarias”*, e incluye un artículo 12 referido a la protección de datos con el siguiente contenido:

Artículo 12. Protección de datos.

La confidencialidad y la protección de datos de todos los intervinientes en los servicios sociales se hará en coherencia con el artículo 5 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y demás normativa aplicable en la materia.

Tal y como ha señalado reiteradamente esta Agencia, el derecho fundamental a la protección de datos personales tiene un contenido mucho más amplio que la mera seguridad de los datos personales.

Por lo que se refiere a la seguridad de la información, la misma comprende el conjunto de técnicas y medidas orientadas a garantizar la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para cualquier organización, independientemente del formato que tengan.

Por el contrario, la protección de datos de carácter personal de las personas físicas se configura como un auténtico derecho fundamental que encuentra su fundamento en el artículo 18.4 de la Constitución Española, conforme al cual *“la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”*. Así lo ha reconocido nuestro Tribunal Constitucional, destacando en la Sentencia 94/1998, de 4 de mayo que el citado artículo 18.4 *“no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, sino que consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona -a la «privacidad» según el neologismo que reza en la Exposición de Motivos de la LORTAD- pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos”*. Posteriormente, en su Sentencia 292/2000, de 30 de noviembre, el Tribunal lo considera como *“un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso”*.

Y en este mismo sentido se pronuncia el RGPD, que tiene por objeto *“proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales”* (artículo 1.2.), destacando en su Considerando 1 que *“la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental”* y en su Considerando 10 que *“para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos deber ser equivalente en todos los Estados miembros. Debe garantizarse en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogéneo”*.

Consecuentemente, el derecho a la protección de datos de carácter personal de las personas físicas es un derecho fundamental y, por tanto, situado en el máximo nivel de protección jurídica, que actualmente se encuentra regulado directamente por la normativa comunitaria, estableciendo el citado RGPD un conjunto de principios, derechos, obligaciones y una estructura organizativa tendentes a garantizar dicho derecho fundamental. Dentro de los mismos, 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, que incluirán, entre otros factores *“la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia*

permanentes de los sistemas y servicios de tratamiento” y “la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico” (artículo 32.2. b) y c) del RGPD).

Por lo tanto, no cabe duda de que la garantía de la seguridad de los datos personales adquiere una especial trascendencia en cuanto a su protección, pero sin que ésta 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, como decíamos, a un conjunto de principios, derechos y obligaciones mucho más amplio.

Y todo ello bajo la garantía administrativa de las “autoridades de control”, funciones que en España asume, sin perjuicio de las competencias que corresponde a las autoridades de las Comunidades Autónomas en su ámbito competencial, la Agencia Española de Protección de Datos, que actúan con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes (Artículo 52 RGPD) y son las únicas competentes para *“asesorar sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento”* (artículo 57.1.c) RGPD).

Partiendo de lo anterior, esta Agencia considera que las referencias que el proyecto remitido contiene a la normativa sobre protección de datos personales son insuficientes para garantizar un adecuado cumplimiento de la misma, en la que, como se ha indicado, 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.

En consecuencia, esta Agencia considera que el derecho a la protección de datos personales debe citarse en el artículo 11 de manera autónoma, en un apartado dedicado en exclusiva al mismo.

En cuanto al artículo 12, debe modificarse su redacción, para recoger con carácter general que los tratamientos de datos de carácter personal de las personas físicas que sean necesarios para la aplicación

de la presente ley 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.

Todo ello sin perjuicio de las observaciones particulares que se realizan a continuación respecto a concretos tratamientos de datos personales regulados por la norma.

II

La siguiente y fundamental cuestión que plantea la norma remitida es la referente a la creación del Sistema de Información Estatal de Servicios Sociales, el cual regula en el Capítulo II del Título IV, en los artículos 28 a 31, que por su importancia se transcriben a continuación:

CAPÍTULO II

Sistema de información de la red integrada de sistemas públicos de servicios sociales

Artículo 28. Sistema de Información Estatal de la red integrada de sistemas públicos de servicios sociales.

Se crea el Sistema de Información estatal de Servicios Sociales que integrará los datos derivados de la gestión de los servicios sociales públicos de todo el territorio estatal, con finalidad estadística, de cara a favorecer el desarrollo de políticas públicas y la toma de decisiones, aportando información actualizada, comparable y continuada en el tiempo.

Artículo 29. Principios que rigen el Sistema de Información Estatal de Servicios Sociales.

La transmisión de la información en el Sistema de Información Estatal de Servicios Sociales estará fundamentada en los principios de:

a) Cooperación entre Administraciones Públicas, permitiendo la interoperabilidad técnica y semántica y la transferencia de datos.

b) Seguridad, mediante la puesta a disposición de las Administraciones Públicas usuarias de una plataforma para el intercambio de información que permita el trasvase de forma segura. El acceso a la aplicación se realizará mediante el uso de certificados digitales u otros modos de autenticación electrónica que garantice la seguridad del acceso y la identificación unívoca de las personas usuarias de acuerdo con la normativa vigente.

c) Responsabilidad y calidad: respetar la información aportada por las Administraciones Públicas a través de los medios telemáticos e incorporar estándares de trazabilidad de la información.

d) *Transparencia y rendición de cuentas:* los datos del Sistema de Información Estatal de Servicios Sociales se ofrecerán siguiendo estándares de datos abiertos, asegurando al mismo tiempo el cumplimiento de la normativa vigente en lo que a protección de datos personales se refiere y el secreto estadístico.

e) *Interoperabilidad:* las Administraciones Públicas se relacionarán a través de medios electrónicos que aseguren la interoperabilidad técnica y semántica, la seguridad de los sistemas y soluciones adoptadas y la protección de los datos de carácter personal, así como que faciliten la coordinación y prestación conjunta de servicios a los interesados.

Artículo 30. Características del Sistema de Información Estatal de Servicios Sociales.

1. *El Sistema de Información Estatal de Servicios Sociales estará concebido para registrar información y datos desagregados mediante la interoperabilidad técnica y semántica de los sistemas de información existentes en las comunidades autónomas de acuerdo con lo establecido en 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.*

2. *El Sistema de Información Estatal de Servicios Sociales contendrá información relativa a la población atendida, las apoyos sociales, servicios y prestaciones que reciben, la calidad en la prestación de los servicios y prestaciones, las infraestructuras de la red y los resultados obtenidos con el objetivo de lograr un conjunto coherente, riguroso y actualizado de datos que proporcione el conocimiento de la realidad del Sistema Público de Servicios Sociales y responda a la demanda de información de las Administraciones Públicas, los agentes sociales y económicos y de la ciudadanía con el aprovechamiento de las fuentes de información existentes.*

3. *El Sistema de Información Estatal de Servicios Sociales incluirá la variable sexo de forma transversal para facilitar la incorporación de la perspectiva de género de manera sistemática y avanzar en nuevas estrategias que permitan mejorar la medición de las desigualdades debidas al género.*

4. *La concreción de la información y los datos que contendrá el Sistema de Información Estatal de Servicios Sociales así como los plazos y condiciones para su transmisión se determinará, en la forma que reglamentariamente se establezca, a propuesta de la Conferencia Sectorial de Servicios Sociales, teniendo en cuenta que los plazos y frecuencia de grabación de la información, por parte de las comunidades autónomas, deben garantizar la disponibilidad de información actualizada y facilitar la toma de decisiones.*

5. *De acordarse en el seno de la Conferencia Sectorial de Servicios Sociales que el sistema de información incluya cualquier tipo*

de dato personal cuyo tratamiento esté inicialmente prohibido por Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas, se desarrollará en el reglamento del sistema de información las razones legítimas del levantamiento de dicha prohibición, en coherencia con los casos establecidos en el artículo 6 del Reglamento (UE) 2016/679.

6. Con la finalidad de asegurar la comparabilidad y facilitar la integración de las fuentes y los sistemas de información, el Ministerio competente en materia de servicios sociales elaborará las reglas para la normalización en la codificación de las variables, siguiendo estándares nacionales e internacionales.

7. El Sistema de Información Estatal de Servicios Sociales contendrá información sobre Servicios Sociales para personas con discapacidad, personas mayores, personas en situación de dependencia, protección a la infancia, sistema de garantía de rentas, servicios sociales de atención primaria, situaciones de violencia contra niños, niñas y adolescentes regulados en el artículo 44 de la Ley Orgánica 8/2021, de 4 de junio, y sobre cualquier otra materia que se decida en el seno de la Conferencia Sectorial de Servicios Sociales, mediante la transmisión de información con otros sistemas públicos de información, tal y como se desarrolle reglamentariamente.

8. El uso y transmisión de la información personal recogida en el Sistema estará sometido al cumplimiento de 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 sus 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), y en la Ley Orgánica 3/2018, de 5 de diciembre.

9. El Sistema de Información Estatal de Servicios Sociales posibilitará la explotación de información, de forma organizada, anonimizada, estructurada y estandarizada y contemplará específicamente la realización de estadísticas en materia de servicios sociales, a todos los niveles territoriales de producción de dicha información (estatal, autonómico, local, centros, unidad y equipos de intervención) así como las de interés general supracomunitario y las que se deriven de compromisos con organizaciones supranacionales e internacionales.

10. Los datos contenidos en el Sistema de Información Estatal de Servicios Sociales serán datos abiertos de acceso público y estarán disponibles de forma gratuita en formatos que permitan utilizar, reutilizar y redistribuir la información de forma ágil y sencilla sin mayores condiciones restrictivas al acceso que la anonimización de la información, el secreto estadístico, la protección de datos personales y la confidencialidad de procedimientos administrativos o judiciales.

Artículo 31. Competencias de las distintas administraciones en relación con el Sistema de Información Estatal de Servicios Sociales.

1. El Ministerio competente en la materia de servicios sociales será el encargado de desarrollar y mantener el Sistema de Información Estatal de Servicios Sociales, así como el responsable del tratamiento de los mismos, garantizando la disponibilidad y el flujo de información, la seguridad y la protección de los datos.

2. El Ministerio competente en la materia de servicios sociales se encargará de recabar, elaborar y dar a conocer la información registrada en el Sistema Estatal, con criterios de transparencia, rendición de cuentas y objetividad.

3. El Ministerio competente en la materia de servicios sociales será el responsable de asegurar que la información contenida en el Sistema de Información Estatal de Servicios Sociales cumple con los requisitos de datos abiertos de acceso público y de ponerlos a disposición de la ciudadanía de forma gratuita en formatos que faciliten su utilización, reutilización y redistribución de forma ágil y sencilla, cumpliendo la normativa vigente en materia de protección de datos de carácter personal y respetando el secreto estadístico.

4. Tanto para la transmisión de datos, como para el acceso al Sistema, las Administraciones Públicas competentes habilitarán el correspondiente perfil de persona usuaria en razón de sus competencias, a fin de garantizar el estricto cumplimiento de normativa vigente en materia de protección de datos de carácter personal.

5. Las comunidades autónomas y Ciudades de Ceuta y Melilla serán responsables de recabar la información generada en cada sistema público autonómico de servicios sociales, y asegurar el flujo de datos desde sus sistemas de información al sistema estatal. Serán las CC.AA., en coherencia con el reparto competencial, las que regulen las historias sociales digitales, cumpliendo con todos los requerimientos que establezca la actual normativa de protección de datos e incluyendo las categorías de datos recogidas en el Sistema de Información Estatal en Servicios Sociales.

6. Será igualmente función de las comunidades autónomas y Ciudades de Ceuta y Melilla recabar datos procedentes de aquellas entidades privadas que presten apoyos sociales de titularidad pública.

7. Los entes locales serán responsables de proveer a las comunidades autónomas de la información generada en los servicios de su competencia.

8. El Ministerio competente en la materia de servicios sociales podrá, dado el caso, firmar convenios de colaboración, como mecanismo regulador de garantía y seguridad, con entidades locales para asegurar el flujo de datos desde los municipios al Sistema de Información Estatal de Servicios Sociales.

Dicha regulación plantea una serie de dudas y contradicciones desde la perspectiva del cumplimiento de la normativa de protección de

datos personales que permiten adelantar el criterio negativo de esta Agencia respecto de dicha regulación, que no se ajusta tampoco a la doctrina jurisprudencial relativa a las limitaciones de este derecho fundamental.

A este respecto, llama clamorosamente la atención la falta de referencias al funcionamiento del citado Sistema en la MAIN, que únicamente contiene menciones muy genéricas respecto del mismo que impiden conocer las finalidades perseguidas y la forma en la que se pretende organizar su funcionamiento.

De este modo, la MAIN se limita a señalar entre los objetivos que se persiguen con la propuesta (página 4) el de *“Desarrollar un sistema estatal de información de servicios sociales para conocer con más detalle las distintas situaciones por las que atraviesa la ciudadanía y el impacto de las políticas públicas de cara a diseñar mejores intervenciones”*, entre los cambios que se introducen (página 13) el de *“El desarrollo de un sistema de información común, equivalente al de otros sistemas de protección, que maximice el potencial de los datos para conocer con más detalle las distintas situaciones por las que atraviesa la ciudadanía y el impacto de las políticas públicas de cara a diseñar mejores intervenciones. Este sistema no sustituiría en ningún caso a los empleados a día de hoy por las comunidades autónomas, si no que se construiría en base a la interoperabilidad técnica y semántica de los mismos”* y en cuanto a la adecuación de la norma al orden de distribución de competencias (página 27) que *“Por último, el artículo 149.1.31.^a de la Constitución Española, desarrollado en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, otorga a la Administración General del Estado la competencia en estadística estatal y, en coherencia con esta competencia estatal, la presente ley establece los pasos necesarios para el desarrollo de un sistema de información complejo y moderno, basado en la interoperabilidad técnica de los distintos sistemas autonómicos”*.

Por otro lado, tal y como se analizará posteriormente, tampoco se explica la forma en la que se va a articular el sistema interoperable de comunicación que permita el traslado automático de la información que sea necesaria para el acceso y disfrute de los servicios y prestaciones básicos en caso de movilidad territorial al que se refiere el artículo 19.3 del anteproyecto, ni la relación que pueda tener ese sistema con el Sistema de Información Estatal de Servicios Sociales, habida cuenta de la diferente finalidad para la que se configura cada uno de ellos, ya que el primero responde a una finalidad de gestión de los servicios sociales, similar a la contemplada respecto de la historia clínica en el artículo 56 de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud y el segundo a una finalidad meramente estadística.

Pese a la trascendencia que tienen dichos preceptos, en la medida en que van a suponer tratamientos de datos de carácter personal que afectan a categorías especiales de datos, la MAIN no contiene información al respecto que permita comprender los tratamientos que se pretenden realizar y la finalidad de los mismos, la posición que ostentan las Administraciones Públicas intervinientes, las categorías de sujetos afectados o los datos personales que se pretende que sean objeto de tratamiento, así como la forma en la que se procederá al mismo, las garantías que se pretenden adoptar para proteger los derechos y libertades de los afectados e, incluso, si lo que se pretende es tratamientos individualizados o va a implicar un tratamiento masivo de datos personales.

Por consecuencia, y tal y como ha informado esta Agencia en otros supuestos análogos al presente (como en el Informe 25/2022 referente al Proyecto de Real Decreto por el que se establece el procedimiento para el reconocimiento, declaración y calificación del grado de discapacidad) debería haberse realizado un análisis riguroso de los tratamientos de datos personales que se pretenden realizar mediante los instrumentos previstos en el RGPD y haberlo incluido en la MAIN, al objeto de poder valorar su licitud, proporcionalidad, alcance y afectación a los derechos y libertades de los afectados y que permitiera identificar, en su caso, las garantías específicas que fuera necesario trasladar a los correspondientes textos normativos, garantías que adquieren una especial relevancia cuando se tratan categorías especiales de datos personales, tal y como recordó el Tribunal Constitucional en su Sentencia 76/2019, de 22 de mayo, a la que posteriormente se hará referencia.

Del mismo modo, no se contiene referencia ni explicación alguna respecto del posible sustitución del vigente Sistema de Información de Usuarios de los Servicios Sociales (SIUSS) y su aplicación informática, que el ministerio competente en materia de servicios sociales viene poniendo a disposición de las Comunidades Autónomas y las Corporaciones Locales mediante la suscripción de los correspondientes convenios de colaboración desde el año 1994, y que *“permite la recogida de los datos básicos de las personas usuarias de los servicios sociales de atención primaria y comunitaria, información necesaria para realizar una intervención profesional como respuesta a una demanda social. Además de recabar datos básicos, esta aplicación tiene los siguientes objetivos: disponer de un instrumento útil y ágil que permita el seguimiento de la intervención y posibilitar el conocimiento de las características y perfil de las personas usuarias e intervenciones realizadas, así como los recursos aplicados. Esto contribuirá a la planificación, coordinación e impulso del Sistema Público de Servicios Sociales y el conocimiento de la evolución de las necesidades y adecuación de los recursos sociales en la Comunidad Autónoma”* (Términos en los que se expresa el exponiendo segundo del Convenio de Cooperación entre la Administración Pública de la Comunidad Autónoma de Canarias, a través de la Consejería de Derechos Sociales, Igualdad, Diversidad y Juventud, y el Ayuntamiento de

Valverde para la implantación del SIUSS, acceso a su aplicación informática e intercambio de información, de 15 de diciembre de 2022 (BOC de 3 de enero de 2023).

En los tratamientos de datos personales que se realizan en el SIUSS, actúan como responsables del tratamiento, en virtud de las competencias que tienen legalmente atribuidas, las Comunidades Autónomas y las Corporaciones Locales competentes en materia de servicios sociales, quienes estarán obligadas en los términos previstos en su normativa específica a compartir la información que posean, tanto relativa a servicios y prestaciones como a las personas usuarias del sistema público de servicios sociales, cuando sea necesario para el ejercicio de sus respectivas competencias.

Entre los datos personales que se gestionan en este sistema se incluyen categorías especiales de datos, como pueden ser los datos de violencia de género y malos tratos, datos de salud, datos sobre situación de discapacidad o dependencia, datos sobre origen racial o étnico, opiniones religiosas, orientación sexual y datos relativos a procedimientos judiciales, condenas e infracciones penales. Asimismo se incluyen otra serie de datos personales que, sin estar incluidos entre dichas categorías deben ser objeto de una especial protección al suponer su tratamiento un alto riesgo para los derechos y libertades de los afectados, como pueden ser los datos e indicadores de vulnerabilidad o de riesgo social (apartado 2 de la cláusula tercera del citado convenio de 15 de diciembre de 2022).

Por el contrario, en virtud de estos convenios, el ministerio actúa como un encargado del tratamiento, limitándose su actuación al simple alojamiento y realización de tareas de backup y a la prestación al responsable de los servicios necesarios para que éste pueda usar la información, cargarla y explotarla, sin que pueda, en ningún caso, acceder a los datos personales que el fichero contiene. De este modo en los convenios se recoge expresamente la prohibición del ministerio de acceder a los datos personales contenidos en SIUSS, si bien “el Ministerio de Derechos Sociales y Agenda 2030, en el ejercicio de sus competencias podrá realizar explotaciones de la información contenida en SIUSS siempre que la misma se haga sin datos de carácter personal. Esto es, se disocie la información de las personas físicas del resto de las informaciones relevantes garantizando que en ningún caso pudiera llegarse a identificar a las mismas” (así se recoge, por ejemplo, en la cláusula cuarta “*Encargado del tratamiento*”, apartado 4 “*Medidas organizativas, técnicas y de seguridad*”, del Convenio entre el Ministerio de Derechos Sociales y Agenda 2030 y la Comunidad Autónoma de Andalucía, con acuerdo de adhesión de las entidades locales, para la difusión e implantación del Sistema de Información de Usuarios de Servicios Sociales (SIUSS), su aplicación informática y el intercambio de información de 24 de marzo de 2021 (BOE de 8 de abril de 2021).

Esta Agencia ha tenido la oportunidad de analizar, si bien de manera parcial, los tratamientos de datos personales realizados mediante el Sistema de Información de Usuarios de los Servicios Sociales (SIUSS) en diversas ocasiones, tal y como se recoge en el Informe 82/2020:

La consulta se refiere al Convenio de Colaboración a suscribir entre el Ministerio de Derechos Sociales y Agenda 2030 y las consejerías competentes de las Comunidades Autónomas en relación con la utilización del Sistema de Información de Usuarios de los Servicios Sociales (SIUSS) y su aplicación informática en el que aparece como responsable de los datos la Comunidad Autónoma, la cual se compromete a la difusión e implantación del SIUSS en las Corporaciones Locales de su territorio, dando acceso al programa informático.

Según se señala en la consulta, “Se trata, ese, de un compromiso (el a la difusión e implantación del SIUSS en las Corporaciones Locales del territorio de la Comunidad Autónoma que suscribe el Convenio), que se asume igualmente en el modelo de Convenio por el que los responsables del tratamiento de datos son las Corporaciones Locales del ámbito de la Comunidad Autónoma, en el que, sin embargo, se supedita el que se les dé acceso al programa informático a que suscriban el Acuerdo de Adhesión que se acompaña a ese Convenio, a lo que añadimos en nuestro informe sobre dicho modelo a que garanticen las Corporaciones Locales la inscripción del Fichero SIUSS (o denominación equivalente) en la Agencia Española de Protección de Datos” y que “suscitando dudas a este Servicio Jurídico, la cláusula del modelo de Convenio en que la responsable del tratamiento de datos es la Comunidad Autónoma que lo suscribe, en cuanto a su compromiso de dar acceso al programa informático a las Corporaciones Locales de su territorio, sin más condicionante, y sin ser estas Corporaciones responsables del tratamiento, se eleva a esa Agencia consulta sobre si la Comunidad Autónoma responsable del tratamiento de datos, se puede comprometer a dar acceso al SIUSS a las Corporaciones Locales de su territorio, sin que éstas sean responsables del tratamiento de datos, y en caso de recibir respuesta positiva a esta cuestión, en qué condiciones”.

Se acompaña a la consulta el modelo de Convenio a suscribir entre el Ministerio de Derechos Sociales y Agenda 2030 y las consejerías competentes de las Comunidades Autónomas (no así el modelo de Convenio por el que los responsables del tratamiento de datos son las Corporaciones Locales del ámbito de la Comunidad Autónoma al que se hace referencia en la consulta) y el informe emitido por esta Agencia en relación con una versión anterior de este modelo de

Convenio el 21 de noviembre de 2012 (Informe 404/2012 con Ref. de entrada 49110/2012 y 472867/2012).

I

La presente consulta versa sobre una cuestión muy concreta referente al Convenio de Colaboración a suscribir entre el Ministerio de Derechos Sociales y Agenda 2030 y las consejerías competentes de las Comunidades Autónomas en relación con la utilización del Sistema de Información de Usuarios de los Servicios Sociales (SIUSS) relativa a la posición jurídica que, en relación con el tratamiento de datos de carácter personal, puede corresponder a las Comunidades Autónomas y a las respectivas Corporaciones Locales que se adhieran al mismo, siendo ésta la única cuestión en la que se va a centrar el mismo.

A este respecto, interesa destacar que esta Agencia ha tenido ocasión de pronunciarse en diferentes ocasiones en relación con una versión anterior de dicho Convenio al amparo de la normativa entonces vigente, constituida fundamentalmente por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

En este sentido, en el Informe 386/2011 relativo a la creación del fichero SIUSS dentro de los ficheros gestionado en dicho momento por el entonces Ministerio de Sanidad, Política Social e Igualdad (MSPSI), ya se hacía referencia a que desde el año 1994, el Ministerio de Asuntos Sociales (MAS) había firmado convenios de colaboración con las CCAA para la difusión e implantación del programa informático que sostiene el sistema SIUSS, concediendo licencias de uso para su utilización dentro del ámbito de la Administración Autonómica y las Corporaciones Locales de su territorio, y que hasta ese momento, dicho registro, a excepción de las Corporaciones Locales donde se encontraba implantado, no necesitaba estar dado de alta en la Agencia Española de Protección de Datos. No obstante, la necesidad de inscripción del fichero por el MSPSI se justificaba por el citado departamento en que “La evolución de las tecnologías ha hecho necesaria que dicha aplicación se desarrolle para su trabajo en el entorno Web con la posibilidad de estar centralizado el Servidor que la sustenta en el MSPSI y conteniendo, por tanto, datos personales de los usuarios de la red pública de servicios sociales”, siendo su finalidad la existencia de un “sistema de información de Usuarios de Servicios Sociales”, añadiendo que “posibilita el conocimiento del perfil sociofamiliar de los usuarios así como el proceso de intervención social”, recogándose los datos “directamente del interesado, por parte de los profesionales que les atienden”. No

obstante, en dicho informe ya se cuestionaba hasta qué punto podía considerarse que el departamento ministerial tenía la condición de responsable del tratamiento, por lo que se estimó preciso clarificar en mayor medida el alcance de la finalidad y usos del fichero.

Posteriormente, en el Informe 404/2012, que se ha acompañado a la consulta, y al objeto de clarificar esa cuestión, se señala lo siguiente:

II

Con posterioridad a dicho informe se adjuntó mediante escrito con fecha de entrada en esta Agencia el 1 de febrero de 2012 informe de la Agencia de Protección de Datos de la Comunidad de Madrid de 26 de octubre de 2011, ratificado por otro posterior de 18 de enero de 2012, en el que se ponía de manifiesto, en resume, que la condición de responsable del fichero de usuarios de servicios sociales debería corresponder a las Entidades Locales a las que la Ley otorga la competencia, no siendo la Administración General del Estado en este caso más que una mera encargada del Tratamiento, al no establecerse en la Ley competencia alguna vinculada directamente a las actividades de gestión que constituirían la finalidad por la que se procedía a la creación del sistema; hecho puesto de manifiesto por la circunstancia de que hasta la creación del fichero no existía una aplicación sostenida por el Departamento consultante, sino que el mismo suministraba las herramientas informáticas adecuadas para que la aplicación se ejecutase en modo local.

Posteriormente fue facilitado a esta Agencia informe de la Abogacía del Estado del Ministerio de Sanidad, Servicios Sociales e Igualdad, de 12 de julio de 2012, en que se pone de manifiesto como procedimiento adecuada para subsanar la situación actualmente existente, sin perjuicio de la opinión de esta Agencia, la firma de un Convenio de colaboración con las Entidades Locales o con las Comunidades Autónomas, con el compromiso de exigir a las entidades locales la información acerca del tratamiento de los datos en el fichero SIUSS.

Finalmente, se celebró en la Agencia Española de Protección de Datos una reunión, en fecha 13 de septiembre de 2012, en la que nuevamente se puso de relieve la inexistencia de competencia de la Administración General del Estado para el tratamiento de los datos del sistema SIUSS, salvo en lo referente a su uso para fines estadísticos sin que el acceso se diese en ningún caso a datos de carácter personal no sometidos

previamente a un procedimiento de disociación. Igualmente, se analizó la existencia de una competencia general de las Comunidades Autónomas en relación con la gestión de los servicios sociales, sin perjuicio del ejercicio de la misma por parte de las entidades locales.

Se concluye, en definitiva, de los antecedentes mencionados hasta el presente lugar que el Ministerio de Sanidad, Servicios Sociales e Igualdad únicamente podrá actuar en relación con el sistema de información al que se refiere la consulta como encargado del tratamiento, pudiendo ostentar la condición de responsables las distintas Comunidades Autónomas, en virtud de las competencias atribuidas a las mismas por sus Estatutos de Autonomía, sin perjuicio de las especialidades que puedan establecer las mismas en casos concretos, como el referido a las competencias de los Consejos Insulares en las Islas Baleares.

III

De este modo, se somete a informe de esta Agencia el Convenio de Colaboración entre las Administraciones de las Comunidades Autónomas y el Departamento consultante para que pueda llevarse a cabo el desarrollo de la actividad del sistema, ostentando el Ministerio la condición de encargado del tratamiento. Dicho Convenio se acompaña de una carta dirigida a cada una de las Administraciones Autonómicas en la que se señala que “La AEPD nos ha indicado que, aunque el Servidor esté centralizado en el Ministerio, la responsabilidad del mismo recae en la Corporación Local. Sin embargo, la C.A, en base a sus competencias en servicios sociales podría asumir la responsabilidad de todos los ficheros de su ámbito territorial que acceden a SIUSS, de manera similar a las que disponen de un aplicativo propio. Y, mediante un acuerdo con el Ministerio se le haría a este último una encomienda de gestión para el tratamiento de los datos”.

Así, deben entenderse resueltas las cuestiones planteadas en el escrito con fecha de entrada en esta Agencia el 1 de febrero de 2012 en el que se consultaba a la misma acerca de la condición de responsable o encargado del tratamiento de la Administración General del Estado en relación con el sistema de información al que se viene haciendo referencia, al haberse finalmente considerado por esta Agencia que en virtud de las competencias atribuidas legalmente a las Comunidades Autónomas por sus Estatutos de Autonomía es a las mismas a las que corresponde la competencia para el tratamiento de los datos

y las que cuentan con la legitimación exigida por el artículo 7.3 de la Ley Orgánica 15/1999 en lo referente al tratamiento de datos relacionados con la salud de las personas, siendo el Ministerio consultante encargado del tratamiento de dichas Administraciones Públicas.

Por consiguiente, el criterio adoptado por la Agencia Española de Protección de Datos al amparo de la normativa entonces vigente fue el de considerar responsables del tratamiento a las Comunidades Autónomas y al Ministerio la condición de encargado del tratamiento, razón por la cual en el posterior Informe 1/2013 se informó favorablemente “la supresión del fichero Sistema de información de usuarios de servicios sociales (SIUSS), creado por la Orden SPI/3495/2011, de 14 de diciembre, como consecuencia de lo señalado por esta Agencia en informes de 7 de noviembre de 2011 y 21 de noviembre de 2012”.

Por otro lado, las entidades locales que se adhirieran al sistema tendrían la consideración de responsables del fichero, al amparo de la distinción entre responsable del fichero y responsable del tratamiento que se establecía en el artículo 3.d) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento) y que el Tribunal Supremo, en su sentencia de 5 de junio de 2004 diferenció del siguiente modo: “Se desprende asimismo de los repetidos apartados del art. 3, como ya se ha manifestado, la diferenciación de dos responsables en función de que el poder de 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”.

No obstante, dicha diferenciación no se recoge en la normativa vigente, que igualmente ha suprimido, como consecuencia del principio de responsabilidad proactiva, la obligatoriedad de la inscripción de los ficheros en la Agencia Española de Protección de Datos, tal y como se analiza a continuación.

II

En el momento presente, la normativa vigente en materia de protección de datos de carácter personal se encuentra recogida 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 (RGPD en lo sucesivo) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD en lo sucesivo), por lo que deberá atenderse a las disposiciones contenidas en dichas normas respecto a las categorías de intervinientes en los tratamientos de datos de carácter personal.

Como punto de partida debemos acudir a lo indicado en el Considerando 79 del RGPD que señala que

(...)La protección de los derechos y libertades de los interesados, así como la responsabilidad de los responsables y encargados del tratamiento, también en lo que respecta a la supervisión por parte de las autoridades de control y a las medidas adoptadas por ellas, requieren una atribución clara de las responsabilidades en virtud del presente Reglamento, incluidos los casos en los que un responsable determine los fines y medios del tratamiento de forma conjunta con otros responsables, o en los que el tratamiento se lleve a cabo por cuenta de un responsable.(...)

El RGPD recoge la necesidad de establecer claramente el mapa de intervinientes en todo tratamiento de datos, al objeto de determinar con acierto la atribución de responsabilidades de acuerdo con la citada norma.

Esta regulación pretende que no queden supuestos de actuación fuera de su ámbito de aplicación, con el fin de dotar a las autoridades de supervisión, de los elementos necesarios para desarrollar su función y en definitiva para brindar a los ciudadanos europeos, la protección que merecen sus datos de carácter personal. Por tanto, cualquier actividad que conlleve el tratamiento de datos personales será atribuible a algún sujeto que cumpla los requisitos de las distintas categorías que ofrece el RGPD.

De acuerdo con lo indicado, el RGPD establece con carácter general (y sin perjuicio de las figuras del destinatario y tercero) tres supuestos de intervinientes en el tratamiento de datos personales: el

responsable del tratamiento, los corresponsables del tratamiento, y el encargado del tratamiento.

El RGPD define en su artículo 4.7 la figura del responsable del tratamiento o responsable como “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.”

Junto a esta figura, el RGPD define en su artículo 26, el corresponsable del tratamiento determinando el régimen jurídico a que debe someterse:

“1. Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos. Dicho acuerdo podrá designar un punto de contacto para los interesados.

2. El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados. Se pondrán a disposición del interesado los aspectos esenciales del acuerdo.

3. Independientemente de los términos del acuerdo a que se refiere el apartado 1, los interesados podrán ejercer los derechos que les reconoce el presente Reglamento frente a, y en contra de, cada uno de los responsables.”

Por tanto, para determinar el cumplimiento de obligaciones y la asunción de responsabilidades de cada corresponsable, habrá que estar al acuerdo que dé cobertura a su relación.

En el mismo sentido, para determinar la responsabilidad de cada corresponsable, el artículo 29 de la LOPDGDD ofrece otro parámetro adicional al citado acuerdo, al indicar que “La determinación de las responsabilidades a las que se refiere el artículo 26.1 del Reglamento

(UE) 2016/679 se realizará atendiendo a las actividades que efectivamente desarrolle cada uno de los corresponsables del tratamiento”.

En definitiva, la relación entre corresponsables vendrá determinada formalmente por el acuerdo que se prevé en el artículo 26 RGPD y materialmente de acuerdo con las actividades que realicen en relación con el tratamiento que se lleve a cabo.

Por otro lado, El RGPD define en su artículo 4.8) la figura del encargado del tratamiento o encargado como “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 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 aplicarán 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 al responsable del tratamiento 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 ha 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 otros, y la calificación como responsable o encargado debe evaluarse con respecto a cada actividad específica de procesamiento de datos.

En el presente caso, refiriéndose la consulta a tratamientos de datos personales necesarios para la prestación de los servicios sociales, y por lo tanto, amparados en lo previsto en la letra 6.1.e) 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" deberá atenderse a las normas jurídicas que atribuyen la correspondiente competencia para su prestación, al objeto de determinar quién ostenta la condición de responsable por decidir sobre los fines y los medios del tratamiento, teniendo en cuenta que, de acuerdo con lo previsto en el artículo 4.7) del RGPD in fine, "si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembro".

En este sentido, las citadas Directrices 07/2020 del Comité Europeo de Protección de Datos sobre los conceptos de responsable del tratamiento y encargado en el RGPD diferencia dos supuestos. Por un lado, los supuestos en los que el poder de decisión puede inferirse de una competencia legal explícita, por ejemplo, cuando el responsable del

tratamiento o los criterios específicos para su nominación son designados por la legislación nacional o de la Unión. Cuando el responsable del tratamiento haya sido identificado específicamente por ley, esto será determinante para establecer quién actúa como responsable. Esto presupone que el legislador ha designado como responsable a la entidad que tiene una capacidad genuina para ejercer el control. Y que en algunos países, legislación nacional establece que las autoridades públicas son responsables del tratamiento de datos personales dentro del contexto de sus funciones (apartado 21). Y por otro, el supuesto más común en que, en lugar de nombrar directamente al responsable del tratamiento o establecer los criterios para su designación, la ley establece una tarea o impone un deber a alguien para captar y tratar ciertos datos. En esos casos, el fin del tratamiento a menudo está determinado por la ley y el responsable del tratamiento será normalmente el designado por ley para la realización de esta finalidad, como sería el caso cuando una entidad a la que se le confían determinadas tareas públicas (por ejemplo, seguridad social) que no puede cumplirse sin recopilar al menos algunos datos personales, establece una base de datos o registro para cumplir con esas tareas públicas. En ese caso, la ley, aunque indirectamente, establece quién es el responsable. De manera más general, la ley también puede imponer una obligación tanto a entidades públicas como privadas para retener o proporcionar ciertos datos. Estas entidades entonces normalmente se considerarían como responsables con respecto al tratamiento que es necesario para ejecutar esta obligación (apartado 22).

Precisamente, el ejemplo concreto que recogen las citadas directrices relativo a la existencia de una previsión legal va referido a la prestación de servicios sociales:

“Example: Legal provisions

The national law in Country A lays down an obligation for municipal authorities to provide social welfare benefits such as monthly payments to citizens depending on their financial situation. In order to carry out these payments, the municipal authority must collect and process data about the applicants’ financial circumstances. Even though the law does not explicitly state that the municipal authorities are controllers for this processing, this follows implicitly from the legal provisions”.

III

Por consiguiente, teniendo el Sistema de Información de Usuarios de Servicios Sociales (SIUSS), un carácter instrumental respecto a las competencias que las leyes otorgan para la prestación de servicios sociales procede analizar dichas competencias para determinar quiénes pueden ostentar la condición de responsable del tratamiento.

En primer lugar, tal y como ya se señalaba en nuestro Informe 404/2012, la totalidad de las Comunidades Autónomas, al amparo de lo previsto en el artículo 148.1.20 de la Constitución, que incluye, dentro de las materias en que las mismas pueden asumir competencias la correspondiente a “asistencia social”, han asumido en sus respectivos estatutos de autonomía la competencia exclusiva en materia de servicios sociales, competencia reiterada en las más recientes reformas estatutarias, aprobando sus propias leyes de servicios sociales, en los cuales se definen sus principios orientadores, además de las prestaciones y servicios (Ley 9/2016, de 27 de diciembre, de Servicios Sociales de Andalucía, Ley 5/2009, de 30 de junio, de Servicios Sociales de Aragón, Ley 1/2003, de 24 de febrero, de servicios sociales del Principado de Asturias, Ley 4/2009, de 11 de junio, de servicios sociales de las Illes Balears, Ley 16/2019, de 2 de mayo, de Servicios Sociales de Canarias, Ley de Cantabria 2/2007 de 27 de marzo, de Derechos y Servicios Sociales, Ley 14/2010, de 16 de diciembre, de Servicios Sociales de Castilla-La Mancha, Ley 16/2010, de 20 de diciembre, de servicios sociales de Castilla y León, Ley 12/2007, de 11 de octubre, de Servicios Sociales de Cataluña, Ley 14/2015, de 9 de abril, de Servicios Sociales de Extremadura, Ley 13/2008, de 3 de diciembre, de servicios sociales de Galicia, Ley 11/2003, de 27 de marzo, de Servicios Sociales de la Comunidad de Madrid, Ley 3/2003, de 10 de abril, del Sistema de Servicios Sociales de la Región de Murcia, Ley Foral 15/2006, de 14 de diciembre, de Servicios Sociales de Navarra, Ley 12/2008, de 5 de diciembre, de Servicios Sociales del País Vasco, Ley 7/2009, de 22 de diciembre, de Servicios Sociales de La Rioja y Ley 3/2019, de 18 de febrero, de la Generalitat, de Servicios Sociales Inclusivos de la Comunitat Valenciana).

Por otro lado, las corporaciones locales pueden ostentar competencias en materia de servicios locales al amparo de lo previsto en la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, si bien las mismas se han visto limitadas tras las modificaciones realizadas por la Ley 27/2013, de 27 de diciembre, de racionalización y sostenibilidad de la Administración Local, algunos de cuyos preceptos han sido declarados inconstitucionales por la Sentencia del Tribunal Constitucional 41/2016, de 3 de marzo de 2016.

Precisamente, la citada sentencia recuerda el carácter autonómico de la competencia, señalando lo siguiente:

“13. Se impugnan las disposiciones adicionales undécima y decimoquinta y transitorias primera, segunda y tercera de la Ley de racionalización y sostenibilidad de la Administración local.

a) Las disposiciones transitorias primera y segunda de la Ley de racionalización y sostenibilidad de la Administración local abordan dos servicios típicamente municipales: «los servicios sociales y de promoción y reinserción social» y «la participación en la gestión de la atención primaria de la salud». Tales servicios se refieren a materias previstas como autonómicas en los apartados 20 («asistencia social») y 21 («sanidad e higiene») del art. 148.1 CE y en los Estatutos de Autonomía.

Se trata de servicios de competencia autonómica habitualmente desplegados en el nivel municipal porque así lo decidieron (o permitieron) las Comunidades Autónomas (al amparo de sus Estatutos) o el Estado (mediante la regulación ex art. 149.1.18 CE de servicios mínimos y habilitaciones directas) o, simplemente, porque fueron desarrollados de hecho por los Ayuntamientos. Vienen a señalarlo las propias disposiciones controvertidas al indicar de modo algo impreciso que la anterior legislación preveía estas tareas «como propias del Municipio» (apartado 1 de ambas disposiciones). Más precisamente, son servicios que, incluidos en el anterior listado de materias del art. 25.2 LBRL, muchos municipios venían prestando, bien de hecho, bien al amparo de normas jurídicas, en particular: 1) legislación autonómica (dictada al amparo de los Estatutos en el marco del art. 25.2 LBRL); 2) las cláusulas generales de la Ley reguladora de las bases de régimen local –antes de que la Ley de racionalización y sostenibilidad de la Administración local las reformulara (art. 25.1 LBRL) o derogara (art. 28 LBRL)–; 3) la habilitación directa para la «prestación de servicios sociales», configurada como obligatoria en municipios de más de 20.000 habitantes [redacción anterior del art. 26.1 c) LBRL].

La Ley de racionalización y sostenibilidad de la Administración local ha excluido estos servicios del elenco de materias dentro de las que «en todo caso» las leyes autonómicas deben atribuir competencias propias (art. 25.2 LBRL, en la redacción dada por el art. 1.8 de la Ley de racionalización y sostenibilidad de la Administración local). A su vez, no las habilita directamente: la «prestación de servicios sociales» [redacción anterior del art. 26.1 c) LBRL] no figura ya entre los servicios mínimos obligatorios en municipios con población superior a 20.000 habitantes [art. 26.1 c) LBRL, en la redacción dada por el art. 1.9 de la Ley de racionalización y sostenibilidad de la Administración local]. Más aún, a través de las disposiciones controvertidas establece la prohibición tanto de que las Comunidades Autónomas atribuyan estos servicios como competencias propias locales como de que

los entes locales los desarrollen como competencia «distinta de las propias o atribuidas por delegación» al amparo de la regla general habilitante del art. 7.4 LBRL (en la redacción dada por el art. 1.3 de la Ley de racionalización y sostenibilidad de la Administración local); todo ello aunque con anterioridad estuvieran previstas como competencias «propias del Municipio» y aunque «su ejercicio se hubiese venido realizando por Municipios, Diputaciones Provinciales o entidades equivalentes, o cualquier otra Entidad Local» (apartado 1 de las disposiciones transitorias primera y segunda). Un ente local podrá ejercer tales competencias solo si las recibe por delegación (apartados 4 y 5 de las disposiciones transitorias primera y segunda).

Otros preceptos de la Ley de racionalización y sostenibilidad de la Administración local acotan el alcance de esta prohibición. Entre las materias en que, conforme a la nueva redacción del art. 25.2 LBRL, la ley debe «en todo caso» atribuir competencias propias municipales subsisten la «evaluación e información de situaciones de necesidad social y la atención inmediata a personas en situación o riesgo de exclusión social» [letra e)] y otras relacionadas con la salud o la sanidad: «protección de la salubridad pública» [letra j)], «abastecimiento de agua potable a domicilio y evacuación y tratamiento de aguas residuales» [letra c)], «cementerios y actividades funerarias» (letra k)], «ferias, abastos, mercados, lonjas y comercio ambulante» [letra i)] y «medio ambiente urbano», que incluye la «gestión de residuos sólidos urbanos y protección contra la contaminación acústica, lumínica y atmosférica en las zonas urbanas» [letra b)]. A su vez, la actual redacción del art. 26.1 c) LBRL habilita directamente a los municipios con población superior a los 20.000 habitantes a ejercer la competencia de «evaluación e información de situaciones de necesidad social y la atención inmediata a personas en situación o riesgo de exclusión social», que queda establecida como servicio obligatorio. Habilita igualmente competencias relacionadas con la salud y la sanidad estableciéndolas como servicios obligatorios en todos los municipios [apartado 1, letra a): «recogida de residuos» y «abastecimiento de agua potable»] o en los de determinado nivel poblacional [apartado 1, letras b) y d): «tratamiento de residuos» y «medio ambiente urbano», respectivamente].

Consecuentemente, la prohibición de que los municipios ejerzan competencias de asistencia social y atención primaria a la salud (disposiciones transitorias primera y segunda de la Ley de racionalización y sostenibilidad de la Administración local) no se extiende a las concretas tareas asistenciales y sanitarias directamente atribuidas a los Ayuntamientos por el art. 26 LBRL o configuradas como ámbito material dentro del cual la ley autonómica debe conferir «en todo caso» competencias

municipales propias (art. 25.2 LBRL). Acotado así el alcance de la prohibición, tratándose de servicios de titularidad autonómica (por virtud de los Estatutos) que el nivel local no puede ya desarrollar (por virtud de las disposiciones impugnadas), la Ley controvertida prevé el traspaso a las Comunidades Autónomas. Incluye, además, normas sobre el modo en que ha producirse el indicado traspaso y la ulterior gestión de los servicios traspasados.

Así, la Ley de racionalización y sostenibilidad de la Administración local prevé un «plan para la evaluación, reestructuración e implantación de los servicios» que ha de elaborar la Comunidad Autónoma (apartados 1 y 2 de las disposiciones transitorias primera y segunda). Fija un plazo cerrado (hasta el 31 de diciembre de 2018, en un caso, y hasta el 31 de diciembre de 2015, en otro) para ejecutarlo (apartado 1 de las disposiciones transitorias primera y segunda). En el caso de los servicios sanitarios, la disposición transitoria primera.2 concreta, además, el ritmo del proceso: cada año las Comunidades Autónomas asumirán un veinte por ciento de la gestión de los servicios asociados a las competencias sanitarias mencionadas.

A ello se añaden otras condiciones, en particular: a) la Comunidad Autónoma debe sufragar íntegramente estos servicios cuando, habiéndose resistido a asumirlos, el nivel municipal esté llevándolos a cabo; y b) en este caso, si no proporciona al municipio las cuantías precisas, el Estado puede aplicar retenciones en las transferencias que le correspondan en aplicación de su sistema de financiación (apartado 5 de las disposiciones transitorias primera y segunda). La disposición adicional undécima de la Ley de racionalización y sostenibilidad de la Administración local establece otras condiciones, vinculadas a la anterior: la Comunidad Autónoma debe comunicar al Ministerio de Hacienda y Administraciones públicas tanto la asunción de aquellos servicios y competencias como las obligaciones que tuviera reconocidas y estuvieran pendientes de pago a los municipios; todo ello «al objeto de la realización, en los términos que se determinen reglamentariamente, de compensaciones entre los derechos y obligaciones recíprocos, el posterior ingreso del saldo resultante a favor de la Administración que corresponda y, en su caso, recuperación mediante la aplicación de retenciones en el sistema de financiación de la Administración pública que resulte deudora». Asumida la gestión del servicio, opera igualmente una exigencia relativa al modo en que la Comunidad Autónoma debe llevarla a cabo: «no podrá suponer un mayor gasto para el conjunto de las Administraciones Públicas» (apartado 3 de las disposiciones transitorias primera y segunda).

b) El recurso de inconstitucionalidad alega que las Comunidades Autónomas son titulares nada más que de las competencias que les atribuyen sus Estatutos. Señala que la ampliación competencial extraestatutaria es posible, pero solo a través de los instrumentos previstos en la Constitución: ley marco (art. 150.1 CE) y ley orgánica de transferencia y delegación (art. 150.2 CE). Solo mediante este tipo de leyes puede el Estado atribuir unilateralmente competencias a las Comunidades Autónomas. Las disposiciones transitorias primera y segunda habrían transferido competencias sin ajustarse al procedimiento constitucionalmente establecido. Admite que las Comunidades Autónomas habían asumido y ejercido competencias en materia de salud y servicios sociales, pero sin incluir las facultades que ahora se les atribuyen. Consecuentemente, el legislador estatal habría desbordado los límites del art. 149.1.18 CE al articular una ampliación extraestatutaria de las competencias autonómicas al margen del procedimiento constitucionalmente establecido. Por otra parte, el recurso razona que las disposiciones transitorias primera.5 y segunda.5 y adicional undécima incurren en inconstitucionalidad por estos motivos y, además, por los que sostienen la impugnación de otros preceptos de la Ley de racionalización y sostenibilidad de la Administración local, que abordaremos después (disposición adicional octava y art. 1.17, que introduce el art. 57 bis LBRL): vulnerarían la reserva de ley orgánica (art. 157.3 CE) y la autonomía financiera garantizada en el art. 156 CE por autorizar al Estado a compensar determinadas deudas contraídas por las Comunidades Autónomas con los créditos resultantes de su sistema de financiación.

Según ha quedado expuesto en el fundamento jurídico 9, la Constitución distribuye todo el poder público entre el Estado (las competencias atribuidas por el art. 149 CE) y las Comunidades Autónomas (las competencias atribuidas por los Estatutos de Autonomía y las leyes previstas en los apartados 1 y 2 del art. 150 CE). Los entes locales obtienen solo las atribuciones que les confieran el Estado y las Comunidades Autónomas, que en todo caso deben respetar la garantía constitucional de la autonomía local (arts. 137, 140 y 141 CE) [SSTC 214/1989, FJ 3 a), 159/2001, FJ 4, 121/2012, FJ 7].

Ninguna de las partes discute que los servicios mencionados en las disposiciones transitorias primera y segunda se refieren a competencias previstas en los apartados 20 («asistencia social») y 21 («sanidad e higiene») del art. 148.1 CE, efectivamente atribuidas a las Comunidades Autónomas por sus Estatutos de Autonomía. Según ha quedado ya expuesto, se está ante servicios de competencia autonómica que el nivel municipal venía prestando porque así lo decidieron (o permitieron) las Comunidades Autónomas (al amparo de sus Estatutos) o el

Estado (mediante la regulación ex art. 149.1.18 CE de servicios mínimos y habilitaciones directas) o, simplemente, porque fueron desarrollados de hecho por los Ayuntamientos.

La innovación normativa que introducen las disposiciones transitorias primera y segunda no consiste estrictamente en la afirmación de la titularidad autonómica de estos servicios. Consiste, en primer término, en la prohibición de que los entes locales puedan prestarlos como competencias propias o como competencias ex art. 7.4 LBRL. Ello resulta a las claras de la previsión de que los entes locales podrán prestar estos servicios solo de modo transitorio o mediante delegación (apartados 4 y 5 de ambas disposiciones). También de la previsión de que «las Comunidades Autónomas asumirán la titularidad» (apartado 1 de ambas disposiciones), «la gestión de los servicios» (apartado 2 de la disposición transitoria primera) o «la cobertura inmediata de dicha prestación» (apartado 2 de la disposición transitoria segunda). En la medida en que la titularidad era ya autonómica por virtud de los Estatutos, lo que está ordenándose es, simplemente, que el nivel local deje de gestionar aquellos servicios como competencias propias. De modo que el traspaso de la gestión a la Comunidad Autónoma trae causa del doble juego de, por un lado, la prohibición que establecen las previsiones controvertidas y, por otro, las atribuciones competenciales de los Estatutos de Autonomía. En segundo término, las disposiciones impugnadas innovan también en la parte en que regulan tanto el traslado competencial indicado (apartados 1, 2, 4 y 5 de ambas disposiciones) como el modo en que las Comunidades Autónomas gestionarán el servicio (apartado 3 de ambas disposiciones).

A la vista de estas consideraciones, no puede afirmarse que el Estado ha vulnerado el art. 150 CE por llevar a cabo una ampliación extraestatutaria de las competencias autonómicas al margen del cauce constitucionalmente previsto. Como afirma el Abogado del Estado, tal ampliación no se produce estrictamente en la medida en que es el propio Estatuto el que atribuyó en su momento a la Comunidad Autónoma la titularidad de las competencias en materia de asistencia social y sanidad sin perjuicio de los títulos de que dispone el Estado, singularmente los apartados 16 y 17 del art. 149.1 CE. Ahora bien, no por ello estas disposiciones dejan de plantear la posible extralimitación competencial que denuncia la Asamblea legislativa de Extremadura.

El problema constitucional no es si el Estado ha llevado a cabo una ampliación extraestatutaria de competencias autonómicas, sino si ha desbordado los márgenes de lo básico al establecer que el nivel local no puede desarrollar determinadas

competencias (salvo por delegación) e imponer condiciones a un traslado que trae causa en última instancia del propio Estatuto de Autonomía.

c) En consonancia con la estructura territorial compuesta que diseña el art. 137 CE (STC 82/1982, FJ 4), la Constitución no encomienda en exclusiva la distribución del poder local ni al Estado ni a las Comunidades Autónomas, según se ha recordado ya. Cada cual en el marco de sus atribuciones ha de regular y conferir competencias a los entes locales. El art. 149.1.18 CE ampara solo una ordenación básica de las condiciones con que el Estado y las Comunidades Autónomas han de atribuir competencias locales [SSTC 214/1989, FJ 3 a) y b), 159/2001, FJ 4, 121/2012, FJ 7]. El Estado solo podrá atribuir competencias locales específicas, o prohibir que éstas se desarrollen en el nivel local, cuando tenga la competencia en la materia o sector de que se trate. En materias de competencia autonómica, solo las Comunidades Autónomas pueden atribuir competencias locales o prohibir que el nivel local las desarrolle; sujetándose en todo caso a las exigencias derivadas de la Constitución (singularmente, arts. 103.1, 135, 137, 140 y 141 CE), las bases del régimen local ex art. 149.1.18 CE y, en su caso, los Estatutos de Autonomía. Ciertamente, las bases pueden llegar a prefigurar específicamente el poder local en materias de competencia autonómica, pero, de acuerdo con lo razonado en el fundamento jurídico 9 de esta Sentencia, solo para garantizar un núcleo homogéneo de derechos prestacionales del vecino; o para atribuir directamente competencias locales, si ello no supone «un obstáculo a las competencias que corresponden» a las Comunidades Autónomas (STC 214/1989, FJ 12).

Las disposiciones transitorias primera y segunda de la Ley de racionalización y sostenibilidad de la Administración local han superado claramente estos márgenes. No se limitan a dibujar un marco de límites dentro del cual la Comunidad Autónoma puede ejercer sus competencias estatutarias, para distribuir poder local o habilitar directamente determinadas competencias municipales sin obstaculizar el ejercicio de las atribuciones autonómicas. Al contrario, impiden que las Comunidades Autónomas puedan optar, en materias de su competencia, por descentralizar determinados servicios en los entes locales, obligando a que los asuma la Administración autonómica dentro de plazos cerrados y con determinadas condiciones.

Ciertamente, la Ley de racionalización y sostenibilidad de la Administración local halla amparo en el art. 149.1.18 CE cuando impone exigencias a la atribución de competencias propias (art. 25 LBRL) y al ejercicio de las «distintas de las propias y atribuidas por delegación» (art. 7.4 LBRL) para asegurar que el Estado, las Comunidades Autónomas y las propias entidades locales

desarrollen un sistema competencial ajustado a los principios de eficacia (art. 103.1 CE), eficiencia (art. 31.2 CE) y estabilidad presupuestaria (art. 135 CE) sin perder de vista la garantía constitucional de la autonomía local (arts. 137, 140 y 141 CE). Las bases están regulando la atribución de competencias locales, pero no atribuyéndolas directamente por sí, ni impidiendo que las Comunidades Autónomas opten por centralizar o descentralizar en el marco de sus Estatutos. La Ley de racionalización y sostenibilidad de la Administración local también se sitúa dentro de aquel título competencial cuando deja de habilitar directamente a los municipios la prestación de servicios sociales, que han desaparecido del listado de servicios mínimos obligatorios (art. 26.1 LBRL). Tal solución tampoco impide por sí que la Comunidad Autónoma decida atribuir a los municipios de su ámbito territorial esa competencia dentro del indicado marco de límites. Del mismo modo, el art. 149.1.18 CE da cobertura a la exclusión de la asistencia social y la sanidad del elenco de materias dentro del cual las leyes deben asegurar que los Ayuntamientos dispongan «en todo caso» de competencias propias (art. 25.2 LBRL). Tampoco esta previsión impide que la Comunidad Autónoma opte por asegurar a los municipios tales competencias con sujeción a las indicadas condiciones básicas.

Sin embargo, el indicado título no autoriza injerencias en la autonomía política de las Comunidades Autónomas como son, por un lado, la prohibición de que éstas en materias de su competencia atribuyan servicios a los entes locales y, por otro, la sujeción a un determinado régimen de traslación o traspaso (disposiciones transitorias primera y segunda de la Ley de racionalización y sostenibilidad de la Administración local). Las Comunidades Autónomas, siendo competentes para regular aquellos servicios sociales y sanitarios, son competentes para decidir –con sujeción al indicado marco de límites– sobre su descentralización o centralización y, en este segundo caso, para ordenar el correspondiente proceso de asunción competencial y traspaso de recursos.

La Comunidad Autónoma está sometida a los mandatos constitucionales de eficiencia, eficacia y estabilidad presupuestaria (arts. 31.2, 103.1 y 135 CE) -además de a la garantía constitucional de la autonomía municipal (arts. 137 y 140 CE)- así como a las condiciones que establecen ahora los arts. 25 y 7 LBRL –y, en su caso, los Estatutos de Autonomía–. Dentro de este contexto normativo, a ella le debe corresponder la decisión última sobre si los municipios situados en su órbita territorial deben o no prestar servicios reconducibles a los ámbitos competenciales que tiene estatutariamente reservados y, en su caso, sobre el modo en que ha de efectuarse el correspondiente

traslado. Al prohibir la descentralización de aquellos servicios, por un lado, y fijar una serie de plazos y condiciones al traspaso, por otro, las disposiciones transitorias primera y segunda de la Ley de racionalización y sostenibilidad de la Administración local han superado el ámbito que la Constitución asigna a una regulación básica sobre atribuciones locales (art. 149.1.18 CE) y, con ello, han invadido las competencias autonómicas de asistencia social y sanidad, recogidas en los apartados 24 y 27, respectivamente, del art. 9 del Estatuto de Autonomía de Extremadura.

Ciertamente, las disposiciones controvertidas permiten una forma menor de descentralización: la delegación, que no alcanza a la titularidad, pero sí al ejercicio de la competencia. La efectividad de la delegación exige la aceptación del municipio delegado (art. 27.5 LBRL), lo que impide que las Comunidades Autónomas puedan apoyarse en esta técnica para desarrollar una política competencial propia que los Estatutos de Autonomía ordenan que sea establecida por ellas. A su vez, no porque la Comunidad Autónoma conserve la posibilidad de acudir a esta técnica, el legislador básico estatal deja de traspasar los márgenes del art. 149.1.18 CE al prohibir en ámbitos de competencia autonómica la utilización de otras fórmulas (singularmente, la atribución de aquellos servicios como competencias propias municipales), por un lado, y al fijar condiciones y plazos a un traspaso cuya regulación corresponde a las Comunidades Autónomas en virtud de sus Estatutos, por otro.

Sin duda alguna, el Estado, a través del ejercicio de sus competencias, singularmente, en lo que ahora importa, en materia de régimen local (art. 149.1.18 CE), tiene la responsabilidad de perseguir los objetivos constitucionales, en general, y los mandatos de eficiencia, eficacia y estabilidad presupuestaria (arts. 31.2, 103.1 y 135 CE), en particular. Por eso, al valorar si el Estado se ha mantenido dentro de los límites de lo básico, no pueden perderse de vista tales objetivos. Sin embargo, tampoco puede olvidarse que aquellas normas constitucionales se dirigen también a las Comunidades Autónomas, que deben darles cumplimiento en el marco de sus atribuciones estatutarias, tanto ejecutivas como normativas (completas o de desarrollo). De ahí que, frente a las alegaciones del Abogado del Estado, hay que insistir en que el art. 135 CE no puede traducirse en una alteración radical de la doctrina constitucional que permita al Estado eliminar las competencias que los Estatutos de Autonomía, dentro del marco establecido por la Constitución, asignan a las Comunidades Autónomas para organizar sus servicios.

El apartado 1 de esas disposiciones señala que las Comunidades Autónomas asumirán la titularidad de aquellas competencias «de acuerdo con» (o «en los términos previstos en») «las normas

reguladoras del sistema de financiación autonómica y de las Haciendas Locales». Esta mención no abre la interpretación (que sugiere el Abogado del Estado, aunque la desarrolla solo respecto de la disposición adicional decimoquinta de la Ley de racionalización y sostenibilidad de la Administración local, a la que nos referiremos después) de que las normas que podrían eventualmente incurrir en inconstitucionalidad son, no las disposiciones transitorias primera y segunda, sino las reguladoras del sistema de financiación autonómica y de las haciendas locales.

Como destaca el propio Abogado del Estado, las previsiones controvertidas se sitúan en un contexto normativo conforme al que los servicios indicados no son ya, en caso alguno, servicios municipales mínimos (art. 26.1 LBRL en la redacción dada por el art. 1.9 de la Ley de racionalización y sostenibilidad de la Administración local) ni materias sobre las que las leyes autonómicas deben «en todo caso» atribuir competencias municipales propias (art. 25.2 LBRL, en la redacción dada por el art. 1.8 de la Ley de racionalización y sostenibilidad de la Administración local). A la vista de este conjunto normativo se desprende inequívocamente que la intención de las disposiciones transitorias primera y segunda de la Ley de racionalización y sostenibilidad de la Administración local es sustraer los indicados servicios a los entes locales.

A su vez, el tenor literal de estas disposiciones «es concluyente y no concede margen a una interpretación conforme con el orden constitucional de distribución de competencias» (en este sentido, recientemente: STC 209/2014, de 18 de diciembre, FJ 4). Para empezar, el título que las acompaña es altamente expresivo: «Asunción por las Comunidades Autónomas de las competencias relativas a la salud» y «Asunción por las Comunidades Autónomas de las competencias relativas a servicios sociales», respectivamente. Lo mismo cabe afirmar del contenido. Disponen que los entes locales solo podrán prestar estos servicios transitoriamente o por delegación. Establecen además, literalmente, que «las Comunidades Autónomas asumirán la titularidad», «la gestión de los servicios» o la «cobertura inmediata de dicha prestación» «tras la entrada en vigor de esta Ley» y, más aún, antes de determinada fecha (el 31 de diciembre de 2018, en un caso, y el 31 de diciembre de 2015, en otro); conforme a un «plan para la evaluación, reestructuración e implantación de los servicios» ajustado a un específico ritmo (cada año, la Comunidad Autónoma habrá de asumir el 20 por 100 de la gestión de los servicios sanitarios mencionados). No solo estos: además de regular el modo en que la Comunidad Autónoma habrá de prestar el servicio asumido («no podrá

suponer un mayor gasto para el conjunto de las Administraciones Públicas»), asocian consecuencias represivas al incumplimiento de aquellos concretos plazos. La disposición adicional undécima de la Ley de racionalización y sostenibilidad de la Administración local impone una concreta exigencia a las Comunidades Autónomas (la comunicación al Ministerio de Hacienda de la asunción y de las obligaciones pendientes de pago) a los efectos de efectuar compensaciones de créditos y, en su caso, retenciones con cargo al sistema de financiación de la Administración correspondiente.

Consecuentemente, es indudable que las disposiciones transitorias primera y segunda de la Ley de racionalización y sostenibilidad de la Administración local, no porque mencionen las normas reguladoras del sistema de financiación, dejan de desbordar los márgenes de lo básico; imponen claramente la centralización de aquellos servicios y regulan también de modo evidente el consiguiente proceso de traslación competencial. La interpretación que sugiere el Abogado del Estado es demasiado forzada y debe ser en consecuencia rechazada, so pena de «ignorar o desfigurar el sentido de los enunciados legales meridianos» (SSTC 22/1985, de 15 de febrero, FJ 5, y 341/1993, de 18 de noviembre, FJ 2), olvidando «el respeto al propio tenor literal de aquéllos» (STC 222/1992, de 11 de diciembre, FJ 2).

Corresponde, pues, declarar la inconstitucionalidad y nulidad de las disposiciones transitorias primera y segunda de la Ley de racionalización y sostenibilidad de la Administración local. También las de la disposición adicional undécima de la Ley de racionalización y sostenibilidad de la Administración local (igualmente impugnada) en la medida que sus previsiones están estrechamente ligadas a aquellas dos transitorias.”

Partiendo de dicha distribución competencial, en los términos en que ha sido interpretada por el Tribunal Constitucional, las Comunidades Autónomas son las competentes en materia de servicios sociales, sin perjuicio de las competencias que puedan corresponder a las entidades locales de acuerdo con la LBRL, bien como competencia propia, en los términos de la legislación del Estado y de las Comunidades Autónomas, en los supuestos contemplados en el artículo 25.2., entre las que se incluyen la evaluación e información de situaciones de necesidad social y la atención inmediata a personas en situación o riesgo de exclusión social (letra e) y las actuaciones en la promoción de la igualdad entre hombres y mujeres así como contra la violencia de género (letra o, introducida por el Real Decreto-ley 9/2018, de 3 de agosto, de medidas urgentes para el desarrollo del Pacto de Estado contra la violencia de género) y siempre que así haya sido determinado por Ley (apartado 3) o en el caso de municipios de más de 20.000 habitantes y con carácter

obligatorio la evaluación e información de situaciones de necesidad social y la atención inmediata a personas en situación o riesgo de exclusión social (artículo 26.1); o bien como competencia atribuida por delegación en los supuestos, entre otros, de prestación de los servicios sociales, promoción de la igualdad de oportunidades y la prevención de la violencia contra la mujer (artículo 27.3.c), en los términos previstos en el propio artículo 27, debiendo preverse técnicas de dirección y control de oportunidad y eficiencia (artículo 7.3). Asimismo, podrán ejercer competencias distintas de las propias y de las atribuidas por delegación, previo informe vinculante de la Administración competente por razón de la materia en los términos previstos en el artículo 7.4.

Por tanto, habida cuenta de las competencias sobre servicios sociales que ostentan las Comunidades Autónomas en virtud de sus Estatutos de Autonomía, en lo relativo a los tratamientos de datos personales que requieran la prestación de dichos servicios, las mismas ostentarán la condición de responsables del tratamiento, siendo las que determinan, en su ámbito competencial, los fines y medios del tratamiento, por lo que las mismas ostentan la condición de responsable del tratamiento pudiendo suscribir, a estos efectos, el modelo de convenio remitido, cuyo objeto es, precisamente, la difusión e implantación de SIUSS y su aplicación informática y el intercambio de información, mediante utilización del programa informático, en entorno Web, dentro del ámbito de la Administración Autonómica y las Corporaciones Locales de su territorio, por lo que se trata de una decisión directa adoptada sobre los medios del tratamiento, actuando el Ministerio como encargado del tratamiento, en los términos que deben recogerse en el convenio de acuerdo con el artículo 28.3 del RGPD.

Habida cuenta la definición de responsable del tratamiento en el RGPD, dicha condición la ostentan en virtud de la competencia que les atribuye el ordenamiento jurídico, incluso en el supuesto en que no tratan directamente los datos personales, ya que lo esencial es su capacidad para decidir los fines y los medios, recordando las Directrices 7/2020 del CEPD que, teniendo dicha capacidad de influencia, no es necesario que el responsable del tratamiento tenga realmente acceso a los datos que se están procesando” (apartado 42).

Por lo tanto, las CCAA tienen la condición de responsable del tratamiento de los datos personales que sean necesarios para la prestación de los servicios sociales que son competencia de las mismas, asumiendo la obligación de difusión e implantación de SIUSS en las Corporaciones Locales de su territorio, sin especificarse en el convenio la forma en la que las CCAA garantizan dicha implantación, si bien se deduce que la misma será potestativa para las entidades locales, al contemplar el propio convenio la existencia de Unidades de Trabajo

Social que no utilicen SIUSS como herramienta de gestión para los servicios sociales comunitarios municipales.

Por consiguiente, la implantación en las Corporaciones Locales podrá realizarse a través de los correspondientes acuerdos administrativos, bien mediante la adhesión de las mismas al presente convenio, bien mediante la firma de un convenio específico con su CCAA. En todo caso, las entidades locales mantienen su competencia respecto de los servicios sociales que hayan asumido en los términos anteriormente señalados, decidiendo sobre los fines y los medios, por lo que ostentarán igualmente la condición de responsable respecto de los tratamientos de datos personales necesarios para la prestación de los servicios sociales que son de su competencia, tal y como se indica por la Abogacía del Estado consultante, circunstancia que deberá figurar en el correspondiente instrumento administrativo.

III

Por todo ello, tanto las CCAA como las Corporaciones Locales ostentan, en el ámbito de sus respectivas competencias, la condición de responsable del tratamiento, entendiendo esta Agencia que el modelo planteado, en cuanto que son las CCAA las que suscribe el convenio de colaboración con el Ministerio de Derechos Sociales y Agenda 2030, que actúa como encargado del tratamiento, es adecuado, al objeto de determinar en dichos convenios las condiciones a las que deberá ajustarse el correspondiente encargo, en las que deberá observarse estrictamente lo dispuesto en el artículo 28 del RGPD, y siendo las comunidades autónomas las que difundirán e implantarán SIUSS entre las entidades locales de su territorio, las cuales ostentarán la condición de responsable respecto a sus propios tratamientos de datos, asumiendo las condiciones del encargo que se han establecido entre la CCAA y el Ministerio en virtud del correspondiente instrumento jurídico.

No obstante, como bien se indica por la consultante, el texto del convenio omite cualquier referencia a la posición jurídica que corresponde a las entidades locales que implanten SIUSS como aplicación informática, debiendo modificarse el mismo al objeto de recoger que las mismas tendrán la condición de responsables del tratamiento, siendo conveniente que en el propio texto se recogiera también la forma en que se procedería a dicha implantación.

De este modo, quedaría clarificada la posición de las partes intervinientes en los tratamientos de datos personales, haciendo constar

la condición de las comunidades autónomas y las entidades locales que implanten el sistema como responsables del tratamiento y el ministerio como encargado, de acuerdo con lo previsto en el RGPD.

III

De la regulación contenida en el anteproyecto parece deducirse que se pretende sustituir el SIUSS por el nuevo Sistema de Información Estatal de Servicios Sociales que regula, el cual tiene un contenido y alcance más amplio al pretender incluir el tratamiento por el ministerio de datos de carácter personal, así como la configuración del mismo como responsable del tratamiento.

A este respecto, debe recordarse, una vez más, los criterios exigibles a las leyes que regulan el tratamiento de datos por las Administraciones Públicas, que con carácter general quedarán legitimados por lo dispuesto en las letras c) y e) del RGPD:

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

e) 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;

Para estos supuestos, el RGPD contiene previsiones adicionales en los apartados 2 y 3 del propio artículo 6:

2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:

a) el Derecho de la Unión, o

b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.

La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

Complementando dichos preceptos, el artículo 8 de la LOPDGDD especifica lo siguiente:

Artículo 8. Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos.

1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.

2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley.

Dichas previsiones deben ponerse en relación con la jurisprudencia del Tribunal Constitucional y del TJUE referida a la limitación del derecho

fundamental a la protección de datos personales, tal y como viene señalando de manera reiterada esta Agencia.

De acuerdo con la misma, el derecho a la protección de datos personales es un derecho fundamental, cuyo contenido consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso» (STC76/2019, de 22 de mayo, y STC 292/2000, de 30 de noviembre). Pero, además, estas sentencias señalaron igualmente la necesidad de que la injerencia esté prevista en una ley o norma de la Unión Europea, con respeto, en todo caso, al principio de proporcionalidad.

En concreto, el Tribunal Constitucional, en la STC 76/2019, de 22 de mayo, tras citar, entre otras, a su anterior STC 292/2000, de 30 de noviembre, señala:

- En segundo lugar, por mandato expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas ora incida directamente sobre su desarrollo (art. 81.1 CE), ora limite o condicione su ejercicio (art. 53.1 CE), precisa una habilitación legal (por todas, STC 49/1999, de 5 de abril, FJ 4). En la STC 49/1999, FJ 4, definimos la función constitucional de esa reserva de ley en los siguientes términos:

Esa reserva de ley a que, con carácter general, somete la Constitución española la regulación de los derechos fundamentales y libertades públicas reconocidos en su Título I, desempeña una doble función, a saber: de una parte, asegura que los derechos que la Constitución atribuye a los ciudadanos no se vean afectados por ninguna injerencia estatal no autorizada por sus representantes; y, de otra, en un Ordenamiento jurídico como el nuestro en el que los Jueces y Magistrados se hallan sometidos "únicamente al imperio de la Ley" y no existe, en puridad, la vinculación al precedente (SSTC 8/1981, 34/1995, 47/1995 y 96/1996) constituye, en definitiva, el único modo efectivo de garantizar las exigencias de seguridad jurídica en el ámbito de los derechos fundamentales y las libertades públicas. Por eso, en lo que a nuestro Ordenamiento se refiere, hemos caracterizado la seguridad jurídica como una suma de legalidad y certeza del Derecho (STC 27/1981, fundamento jurídico 10)."

Esta doble función de la reserva de ley se traduce en una doble exigencia: por un lado, la necesaria intervención de la ley para habilitar la injerencia; y, por otro lado, esa norma legal "ha de reunir todas

aquellas características indispensables como garantía de la seguridad jurídica”, esto es, “ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención” (STC 49/1999, FJ 4). En otras palabras, “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” (STC 292/2000, FJ 15).

Además, dicha ley deberá respetar en todo caso el principio de proporcionalidad, 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; STC 66/1995, de 8 de mayo, F. 5; STC 55/1996, de 28 de marzo, FF. 7, 8 y 9; STC 270/1996, de 16 de diciembre, F. 4.e; STC 37/1998, de 17 de febrero, F. 8; STC 186/2000, de 10 de julio, F. 6).”

La misma doctrina sostiene el Tribunal de Justicia de la Unión Europea (TJUE). Así, si el art. 8 de la Carta Europea de los Derechos Fundamentales reconoce el derecho de toda persona a la protección de los datos de carácter personal que le conciernan, el art. 52.1 reconoce que ese derecho no es ilimitado y permite la limitación del ejercicio de esos derechos y libertades reconocidos por la Carta, limitación que deberá ser establecida por la ley y respetar el contenido esencial de los mismos.

La STJUE de 6 de octubre de 2020, en los casos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net y otros, en su apartado 175, recuerda que:

En cuanto a la justificación de dicha injerencia, cabe precisar que el requisito, previsto en el artículo 52, apartado 1, de la Carta, de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que la permita debe definir ella misma el alcance de la limitación del ejercicio del derecho de

que se trate (véase, en este sentido, la sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 175 y jurisprudencia citada).

Igualmente, el apartado 65 de la Sentencia (STJUE) de la misma fecha 6 de octubre de 2020 (C-623/17), Privacy International contra Secretary of State for Foreign and Commonwealth Affairs y otros, con cita, como la anterior, de la sentencia Schrems 2, dice:

65 Cabe añadir que el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que permita la injerencia en dichos derechos debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate (sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 175 y jurisprudencia citada).

En definitiva, el apartado 175 de la STJUE de 16 de julio de 2020, C-311/2020, Schrems 2, dice:

Cabe añadir, sobre este último aspecto, que el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que permita la injerencia en dichos derechos debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate [dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 139 y jurisprudencia citada].

Es pues, la misma ley que establece la injerencia en el derecho fundamental la que ha de determinar las condiciones y garantías, esto es, el alcance y la limitación, que han de observarse en dichos tratamientos,

Y en dicha STJUE de 16 de julio de 2020, Schrems 2, se añade (y se reitera posteriormente en las citadas sentencias de 6 de octubre de 2020):

176 Finalmente, para cumplir el requisito de proporcionalidad según el cual las excepciones a la protección de los datos personales y las limitaciones de esa protección no deben exceder de lo estrictamente necesario, la normativa controvertida que conlleve la injerencia debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, de modo que las personas cuyos datos se hayan transferido dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso. En particular, dicha normativa deberá indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de

tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario. La necesidad de disponer de tales garantías reviste especial importancia cuando los datos personales se someten a un tratamiento automatizado [véase, en este sentido, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 140 y 141 y jurisprudencia citada].

Como ya mencionamos más arriba en este informe, la STC 76/2019, tan reiterada, dispone:

Esta doble función de la reserva de ley se traduce en una doble exigencia: por un lado, la necesaria intervención de la ley para habilitar la injerencia; y, por otro lado, esa norma legal «ha de reunir todas aquellas características indispensables como garantía de la seguridad jurídica», esto es, «ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención» (STC 49/1999, FJ 4). En otras palabras, «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» (STC 292/2000, FJ 15).

Más recientemente, la Sentencia del TJUE (Gran Sala) de 21 de junio de 2022, al pronunciarse respecto de la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, recuerdo su propia doctrina en los siguientes términos:

112 Hay que tener en cuenta que los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta no son derechos absolutos, sino que deben considerarse en relación con su función en la sociedad (Dictamen 1/15 (Acuerdo PNR UE-Canadá) de 26 de julio de 2017, EU:C:2017:592, apartado 136 -y jurisprudencia citada, y sentencia de 6 de octubre de 2020, Privacy International, C623/17-, EU:C:2020:790, apartado 63 y jurisprudencia citada).

113 Según la primera frase del apartado 1 del artículo 52 de la Carta, toda limitación del ejercicio de los derechos y libertades reconocidos por la Carta debe estar prevista por la ley y respetar la esencia de dichos derechos y libertades. En virtud de la segunda frase del apartado 1 del artículo 52 de la Carta, y sin perjuicio del principio de proporcionalidad, sólo pueden establecerse limitaciones a estos derechos y libertades si son necesarias y responden realmente a objetivos de interés general reconocidos por la Unión Europea o a la necesidad de proteger los derechos y libertades de los demás. A este respecto, el apartado 2 del artículo 8 de la Carta establece que los datos personales deben tratarse,

entre otras cosas, "con fines determinados y sobre la base del consentimiento del interesado o en virtud de otro fundamento legítimo previsto por la ley".

114 Debe añadirse que la exigencia de que toda limitación del ejercicio de los derechos fundamentales esté prevista por la ley implica que el acto que permite la injerencia en dichos derechos debe definir por sí mismo el alcance de la limitación del ejercicio del derecho de que se trate, teniendo en cuenta, por una parte, que esta exigencia no se opone a que la limitación de que se trate se formule en términos suficientemente abiertos para poder adaptarse a los distintos supuestos y seguir el ritmo de la evolución de las circunstancias (véase, en este sentido, la sentencia de 26 de abril de 2022, Polonia/Parlamento y Consejo, C401/19-, EU:C:2022:297, apartados 64 y 74 y la jurisprudencia citada) y, por otra parte, que el Tribunal de Justicia puede, en su caso, precisar, por vía interpretativa, el alcance efectivo de la limitación a la luz del propio tenor de la normativa de la UE en cuestión, así como de su régimen general y de los objetivos que persigue, interpretados a la luz de los derechos fundamentales garantizados por la Carta.

115 Por lo que respecta a la observancia del principio de proporcionalidad, la protección del derecho fundamental al respeto de la vida privada en el ámbito de la UE exige, según reiterada jurisprudencia del Tribunal de Justicia, que las excepciones y limitaciones a la protección de datos personales sólo se apliquen en la medida estrictamente necesaria. Además, un objetivo de interés general no puede perseguirse sin tener en cuenta que debe conciliarse con los derechos fundamentales afectados por la medida, ponderando adecuadamente el objetivo de interés general con los derechos en cuestión [Dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 140, y sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C140/20-, EU:C:2022:258, apartado 52 y jurisprudencia citada].

116 Más concretamente, la cuestión de si los Estados miembros pueden justificar una limitación de los derechos garantizados en los artículos 7 y 8 de la Carta debe apreciarse midiendo la gravedad de la injerencia que tal limitación supone y verificando que la importancia del objetivo de interés general perseguido por dicha limitación es proporcional a dicha gravedad (véanse, en este sentido, las sentencias de 2 de octubre de 2018, Ministerio Fiscal, C207/16-, EU:C:2018:788, apartado 55 y la jurisprudencia citada, y de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C140/20, EU:C:2022:258, apartado 53 y la jurisprudencia citada).

117 Para cumplir el requisito de proporcionalidad, la legislación en cuestión que implique la injerencia debe establecer normas claras y precisas que regulen el alcance y la aplicación de las medidas previstas e impongan unas garantías mínimas, de modo que las personas cuyos datos hayan sido transferidos dispongan de garantías suficientes para proteger eficazmente sus datos personales contra el riesgo de abuso. En particular, debe indicar en qué circunstancias y bajo qué condiciones puede adoptarse una medida que prevea el tratamiento de dichos datos, garantizando así que la injerencia se limite a lo estrictamente necesario. La necesidad de estas garantías es aún mayor cuando los datos personales son objeto de tratamiento automatizado. Estas consideraciones se aplican especialmente cuando los datos del PNR pueden revelar datos sensibles de los pasajeros (Dictamen 1/15 (Acuerdo PNR UE-Canadá) de 26 de julio de 2017, -EU:C:2017:592, apartado 141, y sentencia de 6 de octubre de 2020, La Quadrature du Net y otros, C511/18-, C512/18 -y C520/18-, EU:C:2020:791, apartado 132 y la jurisprudencia citada).

118 Así, la legislación que prevé la conservación de datos personales debe seguir satisfaciendo criterios objetivos que establezcan una conexión entre los datos que deben conservarse y el objetivo perseguido (véanse, en este sentido, el Dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 191 y la jurisprudencia citada, y las sentencias de 3 de octubre de 2019, A y otros, C70/18, EU:C:2019:823, apartado 63, y de 6 de octubre de 2020, La Quadrature du Net y otros, C511/18-, C512/18 -y C520/18-, EU:C:2020:791, apartado 133).

Por otro lado, de la regulación contenida en el anteproyecto se desprende que pueden ser objeto de tratamiento datos referidos a categorías especiales de datos personales, como pueden ser, entre otros, los datos de salud. En este caso, debe recordarse la prohibición general de tratamiento de dichos datos salvo que concurra alguna de las causas de levantamiento de la prohibición previstas en el artículo 9.2. del RGPD. En este caso, y con la misma salvedad referida al consentimiento a la que posteriormente nos referiremos, dicho tratamiento podría venir legitimado conforme a lo previsto en el artículo 9.2.g) del RGPD:

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

Asimismo, en función de la finalidad, puede concurrir la causa contemplada en la letra h) del propio precepto:

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

Añadiendo el citado apartado 3 lo siguiente:

3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

En estos casos que implican el tratamiento de las categorías especiales de datos personales, la imperiosa necesidad de recoger en la ley habilitante las correspondientes garantías es destacada por el Tribunal Constitucional en la ya citada sentencia 76/2019, en sus FJ 6 y 8:

c) La necesidad de disponer de garantías adecuadas es especialmente importante cuando el tratamiento afecta a categorías especiales de datos, también llamados datos sensibles, pues el uso de estos últimos es susceptible de comprometer más directamente la dignidad, la libertad y el libre desarrollo de la personalidad.

La exigencia de especial protección de esta categoría de datos está prevista en el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981 (instrumento de ratificación publicado en el «Boletín Oficial del Estado» núm. 274, de 15 de noviembre de 1985), cuyo artículo 6 establece lo siguiente: «Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. [...]» Esa exigencia ha sido igualmente afirmada por la Agencia Española de Protección de Datos. De acuerdo con el

preámbulo de su Circular 1/2019, esas garantías adecuadas y específicas para proteger los intereses y derechos fundamentales de los afectados «adquieren una especial relevancia tanto por la importancia de los datos personales objeto de tratamiento como por tratarse de tratamientos a gran escala de categorías especiales que entrañarán un alto riesgo para los derechos y libertades de las personas físicas difícilmente mitigable si no se toman medidas adecuadas». Asimismo, como ya se indicó en el fundamento jurídico 4 de esta sentencia, el Reglamento (UE) 2016/679 reitera la exigencia de que el legislador que regule el tratamiento de datos personales relativos a las opiniones políticas establezca dichas garantías adecuadas [artículo 9.2.g) y considerando 56].

Las garantías adecuadas deben velar por que el tratamiento de datos se realice en condiciones que aseguren la transparencia, la supervisión y la tutela judicial efectiva, y deben procurar que los datos no se recojan de forma desproporcionada y no se utilicen para fines distintos de los que justificaron su obtención. La naturaleza y el alcance de las garantías que resulten constitucionalmente exigibles en cada caso dependerán de tres factores esencialmente: el tipo de tratamiento de datos que se pretende llevar a cabo; la naturaleza de los datos; y la probabilidad y la gravedad de los riesgos de abuso y de utilización ilícita que, a su vez, están vinculadas al tipo de tratamiento y a la categoría de datos de que se trate. Así, no plantean los mismos problemas una recogida de datos con fines estadísticos que una recogida de datos con un fin concreto. Tampoco supone el mismo grado de injerencia la recopilación y el procesamiento de datos anónimos que la recopilación y el procesamiento de datos personales que se toman individualmente y no se anonimizan, como no es lo mismo el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, la salud, la vida sexual o la orientación sexual de una persona física, que el tratamiento de otro tipo de datos.

El nivel y la naturaleza de las garantías adecuadas no se pueden determinar de una vez para todas, pues, por un lado, deben revisarse y actualizarse cuando sea necesario y, por otro lado, el principio de proporcionalidad obliga a verificar si, con el desarrollo de la tecnología, aparecen posibilidades de tratamiento que resultan menos intrusivas o potencialmente menos peligrosas para los derechos fundamentales. (FJ.6)

[...]

(iv) Por último, debemos recordar que el Reglamento general de protección de datos establece las garantías mínimas, comunes o generales para el tratamiento de datos personales que no son especiales. En cambio, no establece por sí mismo el régimen jurídico

aplicable a los tratamientos de datos personales especiales, ni en el ámbito de los Estados miembros ni para el Derecho de la Unión. Por ende, tampoco fija las garantías que deben observar los diversos tratamientos posibles de datos sensibles, adecuadas a los riesgos de diversa probabilidad y gravedad que existan en cada caso; tratamientos y categorías especiales de datos que son, o pueden ser, muy diversos entre sí. El reglamento se limita a contemplar la posibilidad de que el legislador de la Unión Europea o el de los Estados miembros, cada uno en su ámbito de competencias, prevean y regulen tales tratamientos, y a indicar las pautas que deben observar en su regulación. Una de esas pautas es que el Derecho del Estado miembro establezca «medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado» [artículo 9.2.g) RGPD] y que «se ofrezcan garantías adecuadas» (considerando 56 RGPD). Es patente que ese establecimiento de medidas adecuadas y específicas solo puede ser expreso. Si la norma interna que regula el tratamiento de datos personales relativos a opiniones políticas, no prevé esas garantías adecuadas, sino que, todo lo más, se remite implícitamente a las garantías generales contenidas en el Reglamento general de protección de datos, no puede considerarse que haya llevado a cabo la tarea normativa que aquel le exige. (FJ.8)

Con el fin de dar adecuado cumplimiento a la normativa y jurisprudencia citada, esta Agencia viene recomendando repetidamente en sus informes que el prelegislador, en aquellos casos, como el presente, en que los tratamientos tienen como base jurídica el art. 6.1.c) o e) del RGPD (esto es, tratamientos cuya base es una obligación legal o una misión de interés público), y venga establecida por el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento y tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, como es el caso de las operaciones de tratamiento impuestas por el proyecto que se informa, o cuando el mismo implique el tratamiento de categorías especiales de datos personales, haga uso de la posibilidad que establece el art. 35.10 RGPD de modo que sea el propio órgano proponente de la disposición general, en el curso del procedimiento de creación de la disposición de la norma (ley, real decreto etc.) quien realice una evaluación de impacto relativa a la protección de datos (EIPD) como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica. Dicha EIPD habrá de incorporarse, como permite el art. 2.1, letra g), del Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo. Este precepto es, además, suficientemente expresivo de la voluntad del legislador de incluir en la MAIN, dentro del concepto “Otros impactos”, el análisis del “impacto que tendrá

para la ciudadanía y para la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma”.

g) Otros impactos: La memoria del análisis de impacto normativo incluirá cualquier otro extremo que pudiera ser relevante a criterio del órgano proponente, prestando especial atención a los impactos de carácter social y medioambiental, al impacto en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad y al impacto que tendrá para la ciudadanía y para la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma

Dicha EIPD no se ha llevado a cabo por el órgano proponente de la disposición general, sin que tampoco la MAIN contenga previsión alguna respecto del tratamiento de los datos de carácter personal. Su realización permitiría que los responsables o encargados del tratamiento no tendrían la obligación de realizar dicha evaluación de impacto de datos personales (EIPD) prescrita en el art. 35 RGPD (y que el Real Decreto del ENS ha considerado asimismo obligatoria) precisamente por haberse llevado ya a cabo en el seno del proceso de gestación de la norma de carácter general.

Esta Agencia recuerda, asimismo, que el citado Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) establece que la política de seguridad del sistema de información deberá examinar y tener en cuenta “los riesgos que se derivan del tratamiento de los datos personales” (art. 12.1.f)), así como que en caso de que los sistemas de información traten datos personales (como es el caso), en todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto en caso de resultar agravadas respecto de las previstas en el citado real decreto (art. 3.3).

En definitiva, esta AEPD recomienda que, con la participación del delegado de protección de datos (DPD), se lleven a cabo y se incorporen a la MAIN el análisis de riesgos (art. 24 RGPD) y la evaluación de impacto relativa a la protección de datos (art. 35 RGPD), lo que permitirá, a la vista de ello, al propio prelegislador, determinar no sólo las medidas de seguridad necesarias en los sistemas de información, sino las garantías específicas que se requieran para afrontar los riesgos derivados del tratamiento de los datos que el Anteproyecto de ley establece (ver art. 35.7.d) RGPD).

Por todo ello, una adecuada regulación conforme a la normativa de protección de datos personales requeriría la realización, con intervención de los DPD del ministerio proponente, de dichos análisis, con el fin de incorporar las garantías adecuadas, previa identificación de los correspondientes tratamientos de datos que se pretenden realizar, así como la tipología de los datos personales que pueden ser tratados, incluidos en su caso los correspondientes a las categorías especiales de datos del artículo 9 del RGPD o datos referidos a condenas e infracciones penales del artículo 10 del RGPD (a los que también se refiere el artículo 10 de la LOPDGDD) u otros datos especialmente sensibles, como los relativos a los indicadores de vulnerabilidad o de exclusión social.

IV

Sin perjuicio de lo anterior, atendiendo a las breves explicaciones dadas en la MAIN y al propio artículo 28 del texto, que hace referencia expresa a la finalidad estadística como justificación de la creación del Sistema de Información, en el único deberían tratarse datos previamente anonimizados, ya que para el cumplimiento de dicha finalidad no es necesario ni proporcional tratar datos de carácter personal, circunstancia que está expresamente prevista en el artículo 30 al referirse a los datos desagregados. Y tratándose en el Sistema datos anonimizados, no resulta de aplicación la normativa sobre protección de datos personales.

Sin embargo, el propio texto introduce previsiones específicas respecto de dichos datos, contrarias al principio de reserva de ley que rige en esta materia, al habilitar genéricamente al reglamento para permitir su tratamiento en el apartado 5 del artículo 30:

5. De acordarse en el seno de la Conferencia Sectorial de Servicios Sociales que el sistema de información incluya cualquier tipo de dato personal cuyo tratamiento esté inicialmente prohibido por Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas, se desarrollará en el reglamento del sistema de información las razones legítimas del levantamiento de dicha prohibición, en coherencia con los casos establecidos en el artículo 6 del Reglamento (UE) 2016/679.

Dicha previsión es contraria a la normativa de protección de datos personales en un doble sentido:

En primer término, porque sería contraria a los principios de limitación de la finalidad y minimización de datos, no resultando necesario ni proporcional el

tratamiento de datos personales para una finalidad exclusivamente estadística que puede llevarse a cabo previa disociación de los mismos.

A esta garantía se refiere específicamente el artículo 89.1. del RGPD:

Artículo 89 Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos

1. El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo.

[...]

En segundo lugar, porque la habilitación al desarrollo reglamentario para que pueda incluir el tratamiento de datos de carácter personal es contraria al principio de reserva de ley que rige en esta materia.

Por consiguiente, la regulación del Sistema de Información Estatal de Servicios Sociales, en cuanto que responde a una finalidad estadística, debe limitarse al tratamiento de datos desagregados, tal y como prevé el artículo 30.1. del proyecto, recogiendo expresamente que en ningún caso se incluirán en el sistema datos de carácter personal y suprimiendo cualquier referencia a los mismos o a la aplicación de la normativa de protección de datos personales, ya que una vez anonimizados pierden esa consideración, al no poder ser referidos a una persona física identificada o identificable. Asimismo, debe suprimirse la referencia al Ministerio competente como responsable del tratamiento de los datos, en cuanto que no existe dicho tratamiento.

Por lo tanto, debe recogerse como garantía específica la previa anonimización de los mismos, de tal forma que los datos se suministren por las Administraciones competentes de manera agregada, sin permitir la identificación de los afectados.

Por el contrario, si se pretendiera el tratamiento de datos de carácter personal en el Sistema de Información para otras finalidades, deberían identificarse las mismas y analizar su necesidad y proporcionalidad, así como el cumplimiento de todos los principios de protección de datos, realizando la preceptiva evaluación de impacto en los datos personales que permita justificar la procedencia de los mismos y las garantías específicas que deben recogerse, en todo caso, en el texto legal, sin que sea posible una remisión al posterior desarrollo reglamentario, y teniendo en cuenta el criterio de esta Agencia es contrario a la creación de bases de datos centralizadas, en la medida en que implican un mayor riesgo para los derechos y libertades de los afectados.

En este caso, tratándose de una modificación esencial del anteproyecto, el nuevo texto del mismo y de la MAIN, con las justificaciones oportunas y acompañado de la EIPD debería someterse a nuevo informe preceptivo de esta Agencia.

V

En cuanto al sistema interoperable de comunicación que permita el traslado automático de la información que sea necesaria para el acceso y disfrute de los servicios y prestaciones básicos en caso de movilidad territorial y que la Administración General del Estado deberá facilitar a las comunidades autónomas al que se refiere el artículo 19.3, pese al silencio de nuevo en el texto y la MAIN respecto de la finalidad del mismo, entiende esta Agencia que el mismo pretende una finalidad de gestión de los servicios sociales y, que por tanto, implica el tratamiento de datos de carácter personal, que deberá quedar limitado a los órganos con competencia legal en la materia, y que debe ponerse en relación con las referencias que el texto del anteproyecto contiene a la tarjeta social digital y a la historia social única, que define como el *“Expediente único, integrado y acumulativo, conformado por el documento o conjunto de documentos resultado de la intervención social realizada en el ámbito de los servicios sociales en la que se registran los datos personales, familiares, sanitarios, de vivienda, económicos, laborales, educativos y cualesquiera otros significativos de la situación social y familiar de la persona y/o familia, así como el diagnóstico, la intervención, la evolución de la situación y apoyos sociales que haya o esté recibiendo”*.

A este respecto, procede reiterar de nuevo la necesidad de que la MAIN incluya la correspondiente EIPD y que se recojan en el texto las garantías oportunas, en los términos previstos en la legislación y jurisprudencia ya citada.

Asimismo, debe tenerse en cuenta el criterio contrario de esta Agencia a la creación de bases de datos centralizadas al que anteriormente nos referíamos, tal y como indicamos en el ya citado Informe 25/2022:

Las principales objeciones que el texto remitido plantea desde la perspectiva de la protección del derecho fundamental a la protección de datos personales deriva de la forma en la que en el mismo se pretende articular el intercambio de información entre las autoridades competentes, que se pretende realizar a través de lo que denomina Sistema de información del Baremo de Valoración del Grado de Discapacidad, una de cuyas finalidades es garantizar la disponibilidad de la información y la comunicación recíproca entre las Administraciones competentes, para lo que se prevé, por un lado, la necesidad de garantizar la interoperabilidad entre los Sistemas de información de las Comunidades Autónomas y, por otro, la creación de una una base de datos de carácter personal, de la que sería responsable de su administración la Dirección General del Imserso, “en el que se determinará la información que se incorporará, su tratamiento, la comunicación recíproca y el intercambio de la misma entre las Administraciones competentes”, estableciéndose asimismo como forma de traslado de expedientes en el artículo 16 : “Para la necesaria coordinación entre las Administraciones competentes se habilitará su interconexión a través de la base de datos que habilite el Imserso, a los efectos de realizar traslados de expedientes”.

A este respecto, hay que partir necesariamente de la regulación legal de la colaboración entre Administraciones Públicas en los supuestos en que la misma implica la comunicación de datos personales, contenida en el artículo 155 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público:

Artículo 155. Transmisiones de datos entre Administraciones Públicas.

1. 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 y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y su normativa de desarrollo, cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad.

2. En ningún caso podrá procederse a un tratamiento ulterior de los datos para fines incompatibles con el fin para el cual se recogieron inicialmente los datos personales. De acuerdo con lo previsto en el artículo 5.1.b) del Reglamento (UE) 2016/679, no se considerará incompatible con los fines iniciales el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos.

3. Fuera del caso previsto en el apartado anterior y siempre que las leyes especiales aplicables a los respectivos tratamientos no prohíban expresamente el tratamiento ulterior de los datos para una finalidad distinta, cuando la Administración Pública cesionaria de los datos pretenda el tratamiento ulterior de los mismos para una finalidad que estime compatible con el fin inicial, deberá comunicarlo previamente a la Administración Pública cedente a los efectos de que esta pueda comprobar dicha compatibilidad. La Administración Pública cedente podrá, en el plazo de diez días oponerse motivadamente. Cuando la Administración cedente sea la Administración General del Estado podrá en este supuesto, excepcionalmente y de forma motivada, suspender la transmisión de datos por razones de seguridad nacional de forma cautelar por el tiempo estrictamente indispensable para su preservación. En tanto que la Administración Pública cedente no comunique su decisión a la cesionaria esta no podrá emplear los datos para la nueva finalidad pretendida.

Se exceptúan de lo dispuesto en el párrafo anterior los supuestos en que el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales esté previsto en una norma con rango de ley de conformidad con lo previsto en el artículo 23.1 del Reglamento (UE) 2016/679.

Asimismo, el artículo 28 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, al regular el derecho a no aportar documentos que ya se encuentren en poder de la Administración actuante o hayan sido elaborados por cualquier otra Administración, prevé como forma de comunicación el uso de las redes corporativas o la consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto.

Dichos preceptos no habilitan la creación de bases de datos centralizadas, tal y como se pretende en la norma remitida. Asimismo, el criterio de esta Agencia es contrario a la creación de dichas bases de datos, en la medida en que implican un mayor riesgo para los derechos y libertades de los afectados.

Asimismo, debe recordarse la doctrina del Tribunal Constitucional contraria a los tratamientos masivos de datos personales, recogida en la

Sentencia del Tribunal Constitucional en su sentencia 17/2013, de 31 de enero de 2013, en la que determinó la constitucionalidad del artículo 16.3 de la Ley de Bases de Régimen Local, referido a la comunicación de los datos del padrón entre Administraciones Públicas.

Tal y como ha sido interpretado por el TC en dicha sentencia (FJ 8), este precepto se refiere a la cesión no consentida de los datos relativos a la residencia o el domicilio a otras Administraciones públicas que así lo soliciten solamente en aquellos casos en los que, para el ejercicio de sus competencias, sean aquellos datos relevantes. En suma, esta petición, que no se refiere específicamente a la cesión de datos del padrón en lo concerniente a los datos de los extranjeros, tiene por finalidad poder disponer de los datos relativos a la residencia o el domicilio que constan en el padrón municipal, (...). De esta forma, de acuerdo con la Ley Orgánica de protección de datos, la finalidad inicial que justificó la recogida de los datos por parte de una Administración pública no impide el destino posterior de los datos para su uso en finalidades diferentes de aquellas que motivaron su recogida respetando, en todo caso, el principio de reserva de ley para establecer dicho cambio, (...) la Ley de bases de régimen local en su condición, además, de norma reguladora de un fichero como el padrón municipal puede prever cesiones de datos entre Administraciones públicas.

*(...) los datos cedidos han de ser **los estrictamente necesarios** para el cumplimiento de las funciones asignadas a los órganos administrativos de forma que deberá **motivarse** la petición de aquellos datos que resulten relevantes, pues es necesario distinguir entre el análisis y seguimiento de una situación individualizada relativa a un caso concreto y el suministro generalizado e indiscriminado de toda la información contenida en un registro personal. El precepto ha contemplado ambos extremos de manera que cualquier cesión de los datos del padrón debe fundamentarse en la necesidad por parte de la Administración cesionaria actuando en el ejercicio de sus competencias, de conocer, **en cada caso concreto**, el dato relativo al domicilio de la persona afectada, extremos que han de ser adecuadamente valorados por la cedente a fin de apreciar si los datos que se solicita son realmente necesarios, pertinentes y proporcionados, atendiendo a la*

competencia que pretende ejercer la Administración cesionaria (art. 4 in fine de la Ley 30/1992). Se trata así de una regla de por sí restringida a los datos relativos a la residencia y al domicilio en cada caso concreto, y a la que le resultarán de aplicación, de más está decirlo, el resto de principios y previsiones que conforman el contenido del derecho reconocidos en la legislación sobre protección de datos.

De lo anteriormente transcrito, y del resto de la fundamentación jurídica contenida en dicha sentencia resulta que el TC ha determinado que (i) habrá de evitarse el acceso indiscriminado y masivo a los datos personales (ii) el dato en cuestión solicitado habrá de ser pertinente y necesario (iii) para la finalidad establecida en el precepto (iv) la solicitud de acceso a los concretos datos personales habrá de motivarse y justificarse expresamente, (v) de manera que ello posibilite su control por el cedente (vi) y se evite un uso torticero de esa facultad con accesos masivos. Ello supone (vii) que ha de quedar garantizada la posibilidad de analizar si en cada caso concreto el acceso tenía amparo en lo establecido en la ley (art. 16.3 LBRL).

Por otro lado, la citada sentencia del Tribunal Constitucional 17/2013 analizaba, en su Fundamento Jurídico Noveno, un supuesto específico de acceso a los datos del padrón, por vía telemática, por la Dirección General de la Policía, para la exclusiva finalidad del ejercicio de las competencias establecidas en la Ley Orgánica de Derechos y Libertades de los Extranjeros en España y su Integración Social, sobre control y permanencia de extranjeros en España, y que se recoge en la disposición adicional séptima de la LBRL, introducida por el art. 3.5 de la Ley Orgánica 14/2003, de 20 de noviembre, en la que se señala lo siguiente:

“Ahora bien, dicha previsión legal ha de ser entendida de forma acorde con las exigencias de proporcionalidad que nuestra doctrina exige en la limitación de un derecho fundamental como es el aquí concernido, relativo la protección de datos de carácter personal. Eso significa que la cesión de datos que el acceso regulado por el precepto supone ha de venir rodeado de una serie de garantías específicas, garantías que, cumplimentadas por el órgano administrativo al que el precepto hace referencia, son, evidentemente, susceptibles de control. Entre ellas se encuentra la necesidad de motivar y justificar expresamente tanto la

concreta atribución de la condición de usuario para el acceso telemático a los datos del padrón que el precepto prevé, como los concretos accesos de que se trate, evitando –en cuanto que la exigible motivación de tales decisiones facilita su correspondiente control mediante los mecanismos previstos en el ordenamiento jurídico, en especial, a través del control jurisdiccional Contencioso-Administrativo– que se produzca tanto un uso torticero de dicha facultad como accesos indiscriminados o masivos. Límites al contenido del acceso que también resultan de determinadas previsiones de la legalidad ordinaria, las cuales han de ser aplicadas teniendo presente, en todo caso, la necesaria unidad del ordenamiento jurídico, tales como el art. 16.3 LBRL, que ya hemos examinado o, incluso, otras regulaciones específicas de la Ley Orgánica de protección de datos, en especial su art. 22.2. Resulta de ello que el acceso solamente será posible, en las condiciones antes dichas, cuando el concreto dato en cuestión resulte pertinente y necesario en relación con la finalidad que ha justificado el acceso, quedando garantizada la posibilidad de analizar si, en cada caso concreto, el acceso tenía amparo en lo establecido en la Ley pues, en caso contrario, no resultará posible su uso. Con tales garantías el acceso regulado en la disposición cuestionada resulta ser proporcionado en relación con la finalidad perseguida, ya que, en tanto que el dato resultante solo puede ser utilizado para la finalidad establecida en el precepto, ha de realizarse de forma puntual por quien se encuentre expresamente habilitado para ello y en relación a datos concretos cuya necesidad ha de ser también justificada de forma expresa y, por tanto, sometida a control, en los términos que acabamos de exponer.”

Por consiguiente, la creación de una base de datos centralizada en el Imserso carece de la necesaria habilitación legal, por lo que debe suprimirse del presente proyecto de real decreto.

Por otro lado, si se pretendiera su creación mediante una norma con rango de ley, la misma deberá respetar todos los requisitos exigidos por el RGPD y la doctrina jurisprudencial referenciada en el presente informe, justificándose adecuadamente su necesidad y proporcionalidad y, singularmente, la inexistencia de otras formas de colaboración menos invasivas que permitan la consecución del propósito perseguido con igual eficacia, así como la existencia de mayores beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto.

Asimismo, el anteproyecto de ley, que deberá someterse al preceptivo informe de esta Agencia, deberá ir acompañado de la Evaluación de impacto en la protección de datos que permita analizar adecuadamente los riesgos del tratamiento e identificar las garantías necesarias que deberán reflejarse en el texto legal.

Por lo tanto, procede analizar los riesgos que para los derechos y libertades de los afectados implica el tratamiento de sus datos personales e incluir en la norma las garantías oportunas, evitando la creación de una base de datos centralizada y el tratamiento masivo de datos personales.

Por ello, es al regular el sistema interoperable de comunicación al que se refiere el apartado 3 del artículo 19 del anteproyecto en el que deben incluirse, además de la finalidad del tratamiento, las referencias correspondientes a la aplicación de los principios contenidos en la normativa sobre protección de datos de carácter personal, singularmente los de limitación de la finalidad y minimización de datos; la posición que ostentan los diversos sujetos intervinientes conforme a lo ya manifestado por esta Agencia, correspondiendo la condición de responsables del tratamiento a los órganos de las Comunidades Autónomas y entidades locales con competencias en materia de servicios sociales y al Ministerio la de encargado del tratamiento; las categorías de datos personales que pueden ser objeto de tratamiento y cualesquiera otras garantías específicas, incluidas las oportunas medidas de seguridad, que resulten de la EIPD.

VI

Para concluir, en relación con las competencias que se atribuyen en el artículo 36 del anteproyecto a la Comisión Interministerial de Servicios Sociales, singularmente las referidas en las letras c) *Seguimiento y análisis de los datos generados por el Sistema de Información Estatal de Servicio Sociales* y h) *Establecimiento, en su caso, y seguimiento de los sistemas de intercambio de información relativa a las personas usuarias de servicios sociales entre distintos sistemas de información sectoriales*, debe tenerse en cuenta que el correcto ejercicio de las mismas no requiere del acceso a los datos de carácter personal, lo que debería recogerse como garantía específica respecto de los recogidos en los sistemas de intercambio de información relativa a las personas usuarias, ya que en el caso del Sistema de Información Estatal de Servicios Sociales dicha previsión debe haberse ya recogido en su regulación específica, tal y como hemos señalado anteriormente respecto de la necesidad de que los datos sean previamente anonimizados.