

El proyecto remitido tiene por objeto la creación y regulación de la Red Estatal de Vigilancia en Salud Pública y de sus Laboratorios Nacionales de Referencia para la Red Estatal de Vigilancia en Salud Pública.

Tal como señala su Exposición de Motivos, si bien la vigilancia epidemiológica en España tiene una larga tradición, habiéndose creado la Red Nacional de Vigilancia Epidemiológica para la enfermedades transmisibles mediante el Real Decreto 2210/1995, de 28 de diciembre, coordinada por el Ministerio de Sanidad, la pandemia de COVID-19 ha puesto de manifiesto la necesidad de mejorar los sistemas de salud y de forma específica la vigilancia en salud pública, tal y como se recoge en los distintos documentos y normas que se citan en la misma.

Asimismo, el Plan de Recuperación, Transformación y Resiliencia ha establecido, a través de su componente 18, las reformas e inversiones necesarias para la renovación y ampliación de las capacidades del Sistema Nacional de Salud (en adelante, SNS). Concretamente, la Reforma 2 (C18.R02) del sistema de salud pública se centra en la implementación de los tres instrumentos estratégicos y operativos previstos en la Ley 33/2011, de 4 de octubre: la Estrategia de Salud Pública, la Red Estatal de Vigilancia en Salud Pública y el Centro Estatal de Salud Pública.

De este modo, conforme se justifica en la Memoria de análisis de impacto normativo, *“En el contexto actual, debe desarrollarse una nueva Red Estatal de Vigilancia en Salud Pública, que se beneficie del desarrollo tecnológico para aumentar la capacidad de análisis, que fortalezca los sistemas ya existentes y a la que se incorporen, además de la vigilancia de las enfermedades transmisibles, otros sistemas y fuentes de información necesarios para extender la vigilancia a las enfermedades no transmisibles y problemas de salud; así como a sus determinantes, tal y como estaba previsto en la LGSP 33/2011, y que al mismo tiempo mejore la anticipación y respuesta necesidades futuras”*.

Asimismo, en la MAIN se explica la relación que tiene este proyecto con la creación de un sistema de información sobre el que ya se ha venido trabajando en el Ministerio de Sanidad desde 2021, así como con la creación de la Agencia Estatal de Salud Pública, entre cuyas funciones se encuentran

las definidas en este proyecto de real decreto para el organismo de coordinación de la Red de Vigilancia en Salud Pública.

Por otro lado, debe especificarse que, conforme al artículo 13 del proyecto, la Red Estatal de Vigilancia en Salud Pública estará integrada por los sistemas de vigilancia en salud pública, formando parte de la misma sin perjuicio de los que puedan crearse en el futuro:

- a) Sistema de Vigilancia de las Enfermedades No Transmisibles, que incluirá la vigilancia del cáncer.
- b) Sistema de Vigilancia de las Enfermedades Transmisibles, incluyendo las resistencias a los antimicrobianos y las infecciones relacionadas con la asistencia sanitaria.
- c) Sistema de Vigilancia en Salud Laboral
- d) Sistema de Vigilancia en Salud Ambiental.
- e) Sistema de Alerta Precoz y Respuesta Rápida.

No obstante, el proyecto únicamente desarrolla de forma específica el Sistema de Alerta Precoz y Respuesta Rápida, manteniendo la red nacional de vigilancia epidemiológica regulada por el Real Decreto 2210/1995, de 28 de diciembre en tanto no se regule el Sistema de Vigilancia de las Enfermedades Transmisibles (disposición adicional décima) y no desarrolla ningún otro de los sistemas de vigilancia en salud pública que se determinan en su artículo 13 (enfermedades no transmisibles, salud laboral y salud ambiental). A este respecto, el apartado 3 del artículo 13 prevé que *“El Gobierno regulará mediante real decreto, en lo que respecta a los sistemas de vigilancia previstos en los párrafos a) a d) del apartado 2, los fines; los eventos objeto de vigilancia; la información a obtener; el mecanismo, forma y periodicidad de recogida de datos; el circuito de comunicación y los mecanismos de coordinación específicos cuando se requiera la coordinación entre varias administraciones, organismos y entidades, así como cualquier otro aspecto que se considere necesario”*.

Entre los aspectos que necesariamente se habrán de contener en los correspondientes reales decretos serán los referidos a la protección de datos de carácter personal, debiendo someterse los correspondientes proyectos al informe preceptivo de esta Agencia.

## I

El proyecto de real decreto crea la Red Estatal de Vigilancia en Salud Pública, integrada por los sistemas de vigilancia en salud pública anteriormente señalados, en los que se procederá a la recogida, análisis, interpretación y difusión de la información procedente de los eventos objeto de vigilancia (artículo 5.2.).

Conforme al artículo 3.b. del mismo, la información de interés para la vigilancia en salud pública se define como *“cualquier dato o información de naturaleza clínica, sanitaria, personal, social, estadística o de otra naturaleza, tanto individuales como poblacionales o ambientales, necesario para la vigilancia en salud pública, incluidos los destinados a identificar de forma inequívoca a las personas cuando así se precise por motivos de salud pública”*.

Por consiguiente, en la medida en que sea objeto de tratamiento cualquier información sobre una persona física identificada o identificable nos encontraremos ante un tratamiento de datos de carácter personal sujeto a las previsiones del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, RGPD) y de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD).

En el presente caso, debe partirse de la naturaleza reglamentaria del proyecto informado y de la vigencia, en relación con las limitaciones al derecho fundamental de protección de datos personales, del principio de reserva de ley exigido por el artículo 53.1 de la Constitución y el artículo 8 de la LOPDGDD, que conforme a reiterada jurisprudencia del Tribunal Constitucional requiere, 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 este sentido, la importante sentencia 292/2000 de 30 de noviembre señala, en su Fundamento Jurídico 14, se pronuncia respecto del alcance de las normas reglamentarias en los siguientes términos:

*14. Pese a la importancia que para garantizar el ejercicio del derecho fundamental poseen los derechos del interesado a ser informado y a consentir la cesión de sus datos personales, como antes se ha declarado, sin embargo, es suficiente según el art. 21.1 LOPD que la comunicación de tales datos entre Administraciones Públicas, para el ejercicio de competencias diferentes o que versen sobre materias distintas, sea autorizada por una norma reglamentaria. Al respecto, ya hemos dicho [STC [127/1994](#), FJ 5, con remisión a la STC [83/1984](#), FJ 4,*

y [99/1987](#), FJ 3 a)] que incluso en los ámbitos reservados por la Constitución a la regulación por Ley no es imposible una intervención auxiliar o complementaria del Reglamento, pero siempre que estas remisiones restrinjan efectivamente el ejercicio de esa potestad reglamentaria a un complemento de la regulación legal que sea indispensable por motivos técnicos o para optimizar el cumplimiento de las finalidades propuestas por la Constitución o por la propia Ley. De tal modo que esa remisión no conlleve una renuncia del legislador a su facultad para establecer los límites a los derechos fundamentales, transfiriendo esta facultad al titular de la potestad reglamentaria, sin fijar ni siquiera cuáles son los objetivos que la reglamentación ha de perseguir, pues, en tal caso, el legislador no haría sino "deferir a la normación del Gobierno el objeto mismo reservado" (STC [227/1993](#), de 9 de julio, FJ 4, recogiendo la expresión de la STC [77/1985](#), de 27 de junio, FJ 14).

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

Por consiguiente, antes de entrar en el contenido concreto del proyecto, procede analizar las normas con rango de ley que regulan la materia objeto de desarrollo por el mismo.

A este respecto, debe partirse de las previsiones contenidas en la Ley 14/1986, de 25 de abril, General de Sanidad, cuyo artículo 8 apartado 1 señala que "Se considera como actividad fundamental del sistema sanitario la realización de los estudios epidemiológicos necesarios para orientar con mayor eficacia la prevención de los riesgos para la salud, así como la planificación y evaluación sanitaria, debiendo tener como base un sistema organizado de información sanitaria, vigilancia y acción epidemiológica" estableciendo en su

artículo 23, primero del Capítulo V del Título I dedicado a la intervención pública en relación con la salud individual colectiva, que *“Para la consecución de los objetivos que se desarrollan en el presente capítulo, las Administraciones Sanitarias, de acuerdo con sus competencias, crearán los Registros y elaborarán los análisis de información necesarios para el conocimiento de las distintas situaciones de las que puedan derivarse acciones de intervención de la autoridad sanitaria”*.

Asimismo, la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, además de establecer acciones de coordinación y cooperación de las administraciones públicas sanitarias, define en el capítulo V el «Sistema de Información Sanitaria del Sistema Nacional de Salud», cuyos objetivos son, entre otros, responder a las necesidades de información de las autoridades sanitarias para favorecer el desarrollo de políticas y la toma de decisiones, y a la ciudadanía para facilitar la toma de decisiones sobre su estilo de vida, prácticas de autocuidado y utilización de los servicios sanitarios. Tal y como señala su artículo 53.6, *“La cesión de los datos, incluidos aquellos de carácter personal necesarios para el sistema de información sanitaria, estará sujeta a la legislación en materia de protección de datos de carácter personal y a las condiciones acordadas en el Consejo Interterritorial del Sistema Nacional de Salud”*.

Dichas previsiones generales se desarrollan por la Ley 33/2011, de 4 de octubre, General de Salud Pública, que dedica el Capítulo I del Título II a la vigilancia de la salud pública, estableciendo su concepto y ámbitos en el artículo 12 y las autoridades competentes y la creación, por vía reglamentaria de la Red de Vigilancia en Salud Pública en el artículo 13:

*Artículo 12. De la vigilancia en salud pública.*

- 1. La vigilancia en salud pública es el conjunto de actividades destinadas a recoger, analizar, interpretar y difundir información relacionada con el estado de la salud de la población y los factores que la condicionan, con el objeto de fundamentar las actuaciones de salud pública.*
- 2. Sin perjuicio de las competencias que correspondan a otras autoridades, la vigilancia de salud pública tomará en cuenta, al menos, los siguientes factores:*
  - 1.º Los condicionantes sociales y las desigualdades que incidan en la salud con mediciones en el nivel individual y en el poblacional.*
  - 2.º Los riesgos ambientales y sus efectos en la salud, incluida la presencia de los agentes contaminantes en el medio ambiente y en las personas, así como el impacto potencial en la salud de la exposición a emisiones electromagnéticas.*
  - 3.º La seguridad alimentaria, incluyendo los riesgos alimentarios.*
  - 4.º Los riesgos relacionados con el trabajo y sus efectos en la salud.*
  - 5.º Las enfermedades no transmisibles.*
  - 6.º Las enfermedades transmisibles, incluyendo las zoonosis y las enfermedades emergentes.*



*7.º Los problemas de salud relacionados con el tránsito internacional de viajeros y bienes.*

*8.º Las lesiones y la violencia.*

*9.º Otros problemas para la salud pública de los que se tenga constancia.*

*3. Asimismo, la vigilancia en salud pública requiere contar con unos sistemas de alerta precoz y respuesta rápida para la detección y evaluación de incidentes, riesgos, síndromes, enfermedades y otras situaciones que pueden suponer una amenaza para la salud de la población.*

*4. Las comunidades autónomas, las ciudades de Ceuta y Melilla y las Entidades locales asegurarán en el ámbito de sus competencias que los respectivos sistemas de vigilancia en salud pública cumplen en todo momento con las previsiones de esta ley. Asimismo, habrán de proporcionar la información que establezca la normativa nacional e internacional, con la periodicidad y desagregación que en cada caso se determine.*

#### *Artículo 13. Articulación de la vigilancia en salud pública.*

*1. Corresponde a la Administración General del Estado, a las comunidades autónomas, a las ciudades de Ceuta y Melilla y a la Administración local, en el ámbito de sus competencias, la organización y gestión de la vigilancia en salud pública.*

*2. Corresponde al Consejo Interterritorial del Sistema Nacional de Salud, a través de la Comisión de Salud Pública, asegurar la cohesión y calidad en la gestión de los sistemas de vigilancia en salud pública.*

*3. Con el fin de coordinar los diferentes sistemas de vigilancia se creará la Red de Vigilancia en Salud Pública, que incluirá entre sus sistemas el de alerta precoz y respuesta rápida. Este sistema tendrá un funcionamiento continuo e ininterrumpido las veinticuatro horas del día. La configuración y funcionamiento de la Red de Vigilancia en salud pública serán determinados reglamentariamente.*

Por otro lado, son numerosos los preceptos de la ley en los que se establece un deber de colaboración en el ámbito de la vigilancia en salud pública, como son, entre otros, además del transcrito artículo 41, el artículo 8, referido al deber de colaboración de los ciudadanos, el artículo 23 sobre la colaboración entre los servicios asistenciales y los de salud pública o el artículo 24 respecto de la colaboración de otros centros y establecimientos sanitarios con la salud pública.

Asimismo, la citada Ley 33/2011, de 4 de octubre, contiene previsiones específicas en relación con el tratamiento de datos de carácter personal en el

Capítulo IX, referido al Sistema de Información en Salud Pública, destacando las previsiones de los artículos 41 y 43:

*Artículo 41. Organización de los sistemas de información.*

*1. Las autoridades sanitarias con el fin de asegurar la mejor tutela de la salud de la población podrán requerir, en los términos establecidos en este artículo, a los servicios y profesionales sanitarios informes, protocolos u otros documentos con fines de información sanitaria.*

*2. Las Administraciones sanitarias no precisarán obtener el consentimiento de las personas afectadas para el tratamiento de datos personales, relacionados con la salud, así como su cesión a otras Administraciones públicas sanitarias, cuando ello sea estrictamente necesario para la tutela de la salud de la población.*

*3. A los efectos indicados en los dos apartados anteriores, las personas públicas o privadas cederán a la autoridad sanitaria, cuando así se las requiera, los datos de carácter personal que resulten imprescindibles para la toma de decisiones en salud pública, de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*

*En cualquier caso, el acceso a las historias clínicas por razones epidemiológicas y de salud pública se someterá a lo dispuesto en el apartado 3 del artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en materia de Información y Documentación Clínica.*

*Artículo 43. Seguridad de la información.*

*1. En todos los niveles del sistema de información en salud pública se adoptarán las medidas necesarias para garantizar la seguridad de los datos.*

*2. Los trabajadores de centros y servicios públicos y privados y quienes por razón de su actividad tengan acceso a los datos del sistema de información están obligadas a mantener secreto.*

En cuanto al acceso a las historias clínicas por razones epidemiológicas y de salud pública, el apartado 3 del artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en materia de Información y Documentación Clínica, al cual se remite el artículo 41.3 citado, dispone que:

*3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en*

*la legislación vigente en materia de protección de datos personales, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clinicoasistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.*

*Se exceptúan los supuestos de investigación previstos en el apartado 2 de la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.*

*Asimismo se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clinicoasistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.*

*Cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, de 4 de octubre, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos.*

Por otro lado, debe tenerse en cuenta, asimismo, la normativa internacional que incide en esta materia y se cita en la propia Exposición de Motivos del proyecto, como el Reglamento Sanitario Internacional de 2005, el cual contiene previsiones específicas en materia de protección de datos personales en su artículo 45:

*Artículo 45 Tratamiento de los datos personales*

*1. La información sanitaria que los Estados Partes obtengan o reciban en cumplimiento del presente Reglamento de otro Estado Parte o de la OMS y que se refiera a personas identificadas o identificables será considerada confidencial y tratada de forma anónima según estipule la legislación nacional.*

*2. Sin perjuicio de las disposiciones del párrafo 1, los Estados Partes podrán dar a conocer y tratar datos personales cuando sea esencial para evaluar y manejar un riesgo para la salud pública, pero los Estados*



*Partes, de conformidad con la legislación nacional, y la OMS se asegurarán de que los datos personales sean:*

- a) tratados de manera justa y con arreglo a la ley, y evitando todo procesamiento adicional incompatible con esa finalidad;*
- b) adecuados, pertinentes y no excesivos en relación con esa finalidad;*  
42 45
- c) exactos y, cuando sea preciso, actualizados; deberán adoptarse todas las medidas razonables necesarias para garantizar que los datos inexactos o incompletos sean eliminados o rectificados; y*
- d) no se conserven más tiempo del necesario.*

*3. A petición, la OMS proporcionará en lo posible a una persona sus propios datos personales a los que se refiere este artículo de manera inteligible, sin retrasos ni gastos excesivos y, cuando sea necesario, permitirá su corrección.*

Asimismo, el Reglamento (UE) 2022/2371 del Parlamento Europeo y del Consejo de 23 de noviembre de 2022 sobre las amenazas transfronterizas graves para la salud y por el que se deroga la Decisión n.º 1082/2013/UE incluye previsiones específicas en relación con el tratamiento de datos personales, que queda sujeto a la normativa sobre protección de datos personales, destacando que el mismo debe limitarse a lo estrictamente necesario y, siempre que sea posible, dichos datos deben anonimizarse, si bien contempla la posibilidad de tratar datos personales en el Sistema de Alerta Precoz y Respuesta cuando sea necesario para el rastreo de contactos (Considerando 39), debiendo delegarse en la Comisión poderes para adoptar actos con arreglo al artículo 290 del TFUE por lo que respecta a, entre otras cuestiones, una lista de categorías de datos personales que podrían intercambiarse a efectos del rastreo de contactos (Considerando 46), incluyendo previsiones específicas en los artículo 27 y 28:

#### *Artículo 27*

##### *Protección de datos personales*

*1. El presente Reglamento se entenderá sin perjuicio de las obligaciones de los Estados miembros en lo relativo al tratamiento de datos personales que efectúen de conformidad con el Reglamento (UE) 2016/679 y la Directiva 2002/58/CE y las obligaciones de las instituciones, órganos y organismos de la Unión en lo relativo al tratamiento de datos personales que efectúen de conformidad con el Reglamento (UE) 2018/1725, en el desempeño de sus funciones.*

*2. La Comisión y, cuando proceda, otras instituciones, órganos y organismos de la Unión no tratarán datos personales, excepto en aquellos casos en que ello sea estrictamente necesario para el cumplimiento de su misión. Los datos de carácter personal se anonimizarán cuando proceda, de tal modo que el interesado no sea identificable.*

## Artículo 28

*Protección de los datos personales con respecto a la función de mensajería selectiva del SAPR*

1. El SAPR incluirá una función de mensajería selectiva que permita comunicar los datos personales, incluidos los datos de contacto y los datos relativos a la salud, únicamente a las autoridades nacionales competentes implicadas en las medidas de rastreo de contactos y en los procedimientos de evacuación médica. Esa función de mensajería selectiva se concebirá y utilizará de manera que quede garantizada la seguridad y la legalidad del tratamiento de datos personales y que conecte con los sistemas de rastreo de contactos a escala de la Unión.

2. Cuando las autoridades nacionales competentes que apliquen las medidas de rastreo de contactos o los procedimientos de evacuación médica comuniquen, a través del SAPR, datos personales necesarios a efectos de dicho rastreo con arreglo al artículo 19, apartado 3, utilizarán la función de mensajería selectiva a que se refiere el apartado 1 del presente artículo y comunicarán los datos únicamente a los demás Estados miembros que participen en tales medidas de rastreo de contactos o de evacuación médica.

3. Cuando comuniquen los datos indicados en el apartado 2, las autoridades nacionales competentes harán referencia a la alerta notificada previamente a través del SAPR.

4. La función de mensajería selectiva se utilizará únicamente a efectos de rastreo de contactos y de evacuación médica. Solo permitirá a las autoridades nacionales competentes recibir los datos que les hayan sido enviados por otras autoridades nacionales competentes. El ECDC solo accederá a los datos necesarios para garantizar el funcionamiento adecuado de la función de mensajería selectiva. Los mensajes que contengan datos personales se borrarán automáticamente de la función de mensajería selectiva a más tardar catorce días después de su envío.

5. Cuando sea necesario a efectos del rastreo de contactos, los datos personales también podrán intercambiarse mediante tecnologías de rastreo de contactos. Las autoridades nacionales competentes no conservarán los datos de contacto ni los datos relativos a la salud recibidos a través de la función de mensajería selectiva durante un período superior al período de conservación aplicable en el contexto de sus actividades nacionales de rastreo de contactos.

6. La Comisión adoptará actos delegados de conformidad con el artículo 31 para completar el presente Reglamento mediante el establecimiento de:

a) los requisitos detallados que sean necesarios para garantizar que el funcionamiento del SAPR y el tratamiento de datos cumplen lo dispuesto en el Reglamento (UE) 2016/679 y en el Reglamento (UE)

*2018/1725, incluidas las respectivas responsabilidades de las autoridades nacionales competentes y del ECDC, y*

*b) una lista de las categorías de datos personales que puedan intercambiarse a efectos de la coordinación de las medidas de rastreo de contactos.*

*7. La Comisión, mediante actos de ejecución, adoptará:*

*A) a) los procedimientos para la interconexión del SAPR con los sistemas de rastreo de contactos a escala de la Unión e internacional, y*

*b) las modalidades de tratamiento de las tecnologías de rastreo de contactos y su interoperabilidad, así como los casos y las condiciones en que se puede conceder a terceros países acceso a la interoperabilidad del rastreo de contactos y las modalidades prácticas de dicho acceso, de plena conformidad con el Reglamento (UE) 2016/679 y la jurisprudencia aplicable del Tribunal de Justicia de la Unión Europea.*

*Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 29, apartado 2.*

Atendiendo a la regulación contenida en la normativa legal citada, los tratamientos de datos personales contemplados en el proyecto de real decreto quedarían legitimados, con carácter general, conforme a lo previsto en la letra e) del artículo 6.1 del RGPD: “el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento”. En cuanto a los que se puedan realizar por las administraciones públicas, instituciones, entidades y organismos del sector público, así como las personas físicas o jurídicas del sector privado a las que se refiere el artículo 12 del proyecto, en cumplimiento de las obligaciones de colaboración contempladas en la Ley 33/2011, de 4 de octubre, la base jurídica sería la determinada por la letra c) del citado artículo 6.1 del RGPD: “el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento”. En ambos casos se cumpliría, además con el principio constitucional de reserva de ley que recuerda el artículo 8 de la LOPDGDD.

En los supuestos en que sea necesario proceder al tratamiento de categorías especiales de datos, como pueden ser los datos de salud, sería necesario que, con carácter previo, concurra alguna de las causas que permiten levantar la prohibición de su tratamiento, conforme a lo previsto en el artículo 9 del RGPD.

Singularmente, en relación con los datos de salud, entiende esta Agencia que sería de aplicación la contemplada en la letra i) del artículo 9.2. del RGPD:

*i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles*

*de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,*

Dicho precepto exige el establecimiento de medidas específicas y adecuadas, debiendo traerse a colación la doctrina de nuestro Tribunal Constitucional contenida en la Sentencia 76/2019, de 22 de mayo respecto de la norma en la que deben recogerse dichas garantías (F.J.8):

*(...) La previsión de las garantías adecuadas no puede deferirse a un momento posterior a la regulación legal del tratamiento de datos personales de que se trate. Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado. (...). Según reiterada doctrina constitucional, la reserva de ley no se limita a exigir que una ley habilite la medida restrictiva de derechos fundamentales, sino que también es preciso, conforme tanto a exigencias denominadas –unas veces– de predeterminación normativa y –otras– de calidad de la ley como al respeto al contenido esencial del derecho, que en esa regulación el legislador, que viene obligado de forma primaria a ponderar los derechos o intereses en pugna, predetermine los supuestos, las condiciones y las garantías en que procede la adopción de medidas restrictivas de derechos fundamentales. Ese mandato de predeterminación respecto de elementos esenciales, vinculados también en último término al juicio de proporcionalidad de la limitación del derecho fundamental, no puede quedar deferido a un ulterior desarrollo legal o reglamentario, ni tampoco se puede dejar en manos de los propios particulares. (...)*

A este respecto, tal y como hemos visto anteriormente, en nuestro ordenamiento jurídico ya se contienen garantías específicas respecto del tratamiento de datos de carácter personal por razones de salud pública, incluidos los datos de salud imprescindibles, como pueden ser las contenidas en los artículos 41 y 43 de la Ley 33/2011, de 4 de octubre, General de Salud Pública y en el artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en materia de Información y Documentación Clínica.

De este modo, en relación con los tratamientos de datos de salud y el acceso a las historias clínicas, el proyecto de real decreto debe respetar, en todo caso, dichas garantías, sin perjuicio de que pueda introducir otras

garantías adicionales para facilitar el cumplimiento de los principios de protección de datos recogidos en el artículo 5 del RGPD:

*1. Los datos personales serán:*

*a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);*

*b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);*

*c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);*

*d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);*

*e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);*

*f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).*

*2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).*

## II

Partiendo de lo anterior, procede analizar las previsiones contenidas en el proyecto de real decreto respecto de los tratamientos de datos de carácter personal.



A este respecto, se contienen previsiones específicas en el artículo 10.1, referido al informe de gestión de la Red que debe elaborar el órgano de coordinación de la Red cada dos años, el cual *“incorporará una valoración sintética sobre la protección de datos personales en el marco de las actividades de la Red”*; en el artículo 11.1, que regula la evaluación independiente y con periodicidad quinquenal de la Red, que deberá incluir en el informe de la evaluación un *“análisis de riesgo y medidas de cumplimiento en protección de datos en las propuestas de mejora del sistema”*, contemplando, asimismo, la realización de una evaluación de cada uno de los sistemas de vigilancia cada cinco años; el artículo 19, que al regular la integración de la información dispone en su apartado 1 que *“En la Red se integrará la información necesaria para la vigilancia en salud pública, teniendo en consideración lo previsto en el Esquema Nacional de Seguridad y el Esquema Nacional de Interoperabilidad y sus normas técnicas de desarrollo y en la normativa de Protección de Datos Personales, así como de las directrices, estándares y normas de interoperabilidad aprobadas en la Comisión de Salud Digital”*, estableciendo en su apartado 3 garantías del principio de minimización y limitación de la finalidad al señalar que *“El Comité de Gestión de la Red velará por que no existan redundancias ni duplicidades innecesarias en la captura de datos y por la integración necesaria de los datos y de la información derivada de los distintos elementos objeto de vigilancia. Asimismo, velará por que los datos recogidos sean los estrictamente necesarios para satisfacer las necesidades de la Red y su tratamiento responda a las finalidades que recoge este real decreto”*; el artículo 20, referido al intercambio de información en los sistemas de vigilancia cuyo apartado 1 incluye previsiones específicas de seguridad y trazabilidad, disponiendo que *“Los sistemas de vigilancia se dotarán de plataformas digitales, que a nivel estatal gestionará el órgano de coordinación de la Red, con acceso regulado y seguro a las partes que participen en la vigilancia, para gestionar el intercambio y almacenaje de la información generada por la actividad de vigilancia, que garantice la interoperabilidad necesaria, la seguridad y la trazabilidad de los datos”*.

Asimismo, siguiendo el criterio de esta Agencia, la MAIN ha incluido en el análisis el impacto en materia de protección de datos personales, (apartado 10) acompañado de una descripción de los tratamientos que formarán parte del Sistema de Alerta Precoz y Respuesta Rápida, y se ha recogido en el proyecto una disposición adicional primera en la que se abordan los aspectos de la protección de datos de carácter personal en los siguientes términos:

*Disposición adicional primera. Protección de datos de carácter personal.*

*1. Los tratamientos de datos personales regulados en este real decreto se llevarán a cabo conforme a 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.

2. La prestación de servicios para los fines de la Red se realizará con las garantías del artículo 28 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

3. Los responsables de los tratamientos de la Red serán el Ministerio de Sanidad y las comunidades autónomas y las ciudades de Ceuta y Melilla, en el ámbito de sus respectivas competencias, que garantizarán la aplicación de las medidas de seguridad preceptivas que resulten del correspondiente análisis de riesgos, teniendo en cuenta que los tratamientos afectan a categorías especiales de datos y que dichos tratamientos serán realizados por administraciones públicas obligadas al cumplimiento del Esquema Nacional de Seguridad.

4. Se prevé que los aspectos relacionados con la información a recoger y tratar se fijen en los reales decretos que desarrollan cada sistema de vigilancia.

Así mismo, se prevé que el Comité de Gestión de la Red vele por que los datos recogidos sean los estrictamente necesarios para satisfacer las necesidades de la red y su tratamiento responda a las finalidades contempladas en el presente real decreto.

Para garantizar las exigencias de actualización, completitud y exactitud de los datos se prevé expresamente que la Red integre los sistemas de información con el fin de disponer de datos actualizados completos y permanentes, garantizando, además, que no existan redundancias ni duplicidades en la captura de los datos.

5. Los informes a los que se refiere el artículo 10 no incluirán información sobre datos personales ni información que permita la identificación de una persona.

6. Para garantizar la adecuada interoperabilidad será necesario utilizar los identificadores personales que ya constan en el conjunto mínimo de datos de los informes clínicos en el SNS aprobados por el Real Decreto 1093/2010, de 3 de septiembre. Estos identificadores son el nombre y apellidos, el código SNS, el Código de Identificación Personal (CIP) de la comunidad autónoma, el Documento Nacional de Identidad, Número de Identificación de Extranjeros, Número de Identificación Fiscal y pasaporte.

7. Las administraciones sanitarias con función de vigilancia en salud pública no precisarán obtener el consentimiento de las personas afectadas para el tratamiento de datos personales, relacionados con la salud, así como su cesión a otras administraciones públicas sanitarias, cuando ello sea necesario por razones de interés público en el ámbito de la salud pública o en el ejercicio de poderes públicos y en cumplimiento de obligaciones legales, conforme al artículo 9.2 y al artículo 6.1.c) y e) del Reglamento (UE) 2016/679 del Parlamento

*Europeo y del Consejo, de 27 de abril de 2016 y al artículo 41 de la Ley 33/2011, de 4 de octubre. En cualquier caso, el acceso a las historias clínicas por razones epidemiológicas y de salud pública que realizan las administraciones sanitarias con función de vigilancia en salud pública se someterá a lo dispuesto en el artículo 16.3 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en materia de Información y Documentación Clínica, de acuerdo con la disposición final tercera de la Ley 33/2011, de 4 de octubre. Para el cumplimiento de las funciones de vigilancia se garantizará un acceso general a las historias clínicas y no solo de forma individualizada al personal autorizado en vigilancia en salud pública ya que estas funciones son consideradas como actividad fundamental del sistema sanitario de acuerdo a lo establecido en el artículo 8.1 de la Ley 14/1986, de 25 de abril.*

*8. Todas las personas que tengan acceso a los datos generados como consecuencia de la puesta en marcha de este real decreto están sometidos al deber de secreto. De acuerdo con el artículo 16.3 de la Ley 41/2002, de 14 de noviembre, el acceso a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública que realizan las administraciones sanitarias con función de vigilancia en salud pública habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la administración que solicitase el acceso a los datos. En virtud de lo establecido en este apartado será de aplicación la excepción al deber de información a los interesados en los términos previstos en el artículo 14.5.d) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.*

*9. Los datos recogidos por la Red podrán cederse a terceras partes siempre que se garantice la protección de la confidencialidad y la privacidad. La cesión de datos a terceras partes deberá responder a las finalidades que establece este real decreto.*

*Este uso está de acuerdo con lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre.*

*10. El Comité de Gestión de la Red elaborará el procedimiento de acceso a los datos recogidos por la Red y el tratamiento de los mismos conforme a la normativa de Protección de Datos*

*11. Los datos recogidos en la Red, estarán disponibles de forma abierta e interactiva para su acceso por los interesados. La información se facilitará excluyendo datos personales. Este acceso podrá efectuarse dentro de los límites fijados por la normativa en materia de derecho de acceso a la información pública, la de protección de datos de carácter personal, así como –en su caso- las derivadas de las garantías para unidades informantes sobre confidencialidad y secreto estadístico. Los responsables de los tratamientos de la Red, definidos en el punto 2 de*

*esta disposición adicional primera, valorarán aquella información que no podrá ser objeto de difusión abierta para los interesados, a los efectos de cumplir con la citada normativa.*

*12. El intercambio de datos con otros países en amenazas transfronterizas graves para la salud se regirá por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y por el Reglamento (UE) 2022/2371 del Parlamento Europeo y del Consejo, de 23 de noviembre de 2022, sobre las amenazas transfronterizas graves para la salud y por el que se deroga la Decisión nº 1082/2013/UE y de acuerdo a lo establecido en el Reglamento sanitario internacional (2005) de la Organización Mundial de la Salud.*

Esta Agencia valora muy positivamente tanto la inclusión del análisis del impacto en la protección de datos personales como la citada disposición adicional, si bien deben realizarse una serie de consideraciones sustanciales.

En primer término, tal y como viene señalando esta Agencia, 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, realice un análisis de riesgos y, en su caso, 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 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.

En el presente caso, teniendo en cuenta que se pretende el tratamiento de datos de salud que pueden afectar a numerosas personas, y que incluye no solo las enfermedades transmisibles sino también de manera novedosa, tal y como se señalará posteriormente, las enfermedades no transmisibles, y que se va a realizar una integración en la Red de todos los sistemas de vigilancia, de modo que se realizará la integración necesaria de los datos y de la información derivada de los distintos elementos objeto de vigilancia, atendiendo al alto riesgo de dichos tratamientos debería haberse adjuntado la Evaluación de impacto en la protección de datos como anexo a la MAIN, conforme a lo previsto en el artículo 35.10 del RGPD, que permita identificar adecuadamente los riesgos derivados de dichos tratamientos e incorporar en la norma las garantías oportunas. Para la elaboración de dicha Evaluación de impacto, podría haber servido como punto de partida la preceptiva evaluación de impacto que debe haberse realizado para el desarrollo del sistema de información, en el cual el Ministerio de Sanidad viene trabajando desde 2021, tal y como se señala en la MAIN.

Por consiguiente, debería elaborarse por el Ministerio de Sanidad, con la asistencia de su delegado de protección de datos, una Evaluación de impacto en la protección de datos que permita incorporar, en su caso, garantías adicionales a las previstas en la norma y a las que nos referiremos a continuación.

Para la elaboración de dicha evaluación, además de lo ya señalado respecto de la EIPD que debe haberse realizado dentro de los trabajos de desarrollo del sistema de información, conforme al principio de privacidad desde el diseño (artículo 25 del RGPD), debe tenerse en cuenta las indicaciones recogidas en las “Orientaciones para la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo”, recientemente publicadas por esta Agencia (<https://www.aepd.es/es/documento/orientaciones-evaluacion-impacto-desarrollo-normativo.pdf>).

En segundo lugar, en relación con el contenido de la disposición adicional primera, se realizan las siguientes observaciones:

1.- Los responsables del tratamiento deben garantizar el cumplimiento de toda la normativa de protección de datos personales y no solo la aplicación de medidas de seguridad, debiendo analizar los riesgos que el tratamiento tenga para los derechos y libertades de las personas físicas (artículo 24 del RGPD). Particularmente, al tratarse de tratamientos de alto riesgo, al poder implicar un tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, deberá realizarse la correspondiente evaluación de impacto en la protección de datos (artículo 35 del RGPD).

Asimismo, deberán garantizar la aplicación de las medidas técnicas y organizativas que resulten de la correspondiente evaluación de impacto en la protección de datos, en los términos previstos en el artículo 3 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

2.- En relación con la información a recoger y tratar, se prevé que se fije en los reales decretos que desarrollan cada sistema de vigilancia, y que será el Comité de Gestión de la Red el que velará por el cumplimiento de los principios de minimización de datos y limitación de la finalidad.

No obstante, debería especificarse que será cada uno de los reales decretos los que identifiquen las categorías de datos personales que podrán ser objeto de tratamiento, atendiendo a las especificidades de cada uno de ellos y garantizando, cuando se trate de datos de salud y siempre que su tratamiento no sea estrictamente necesario atendiendo a la concreta finalidad pretendida, la previa anonimización o, en su caso, seudonimización, de los



datos, así como recogiendo el carácter excepcional del tratamiento de los datos identificativos cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población ya que, como se ha señalado al principio del presente informe, se trata de garantías específicamente recogidas en la normativa legal, nacional e internacional, que habilita estos tratamientos, sin que dichas garantías se puedan restringir mediante real decreto.

Además, debe tenerse en cuenta la doctrina del Tribunal Constitucional contraria al tratamiento masivo de datos personales por las Administraciones Públicas, recogida con claridad en su Sentencia 17/2013 de 31 de enero de 2013, en sus Fundamentos Jurídicos 7 y 8.

Señala el FJ7, referido al acceso por parte de los órganos competentes en materia de extranjería a los datos obrantes en poder de otros órganos administrativos:

*En cuanto al segundo párrafo de la disposición adicional impugnada, el mismo autoriza a los órganos de la Administración estatal, competentes en el ámbito de los procedimientos administrativos que se tramiten en el ámbito que regula la Ley Orgánica de derechos y libertades de los extranjeros y solamente en el ejercicio de las competencias que tienen atribuidas, para acceder a los ficheros en los que obren datos necesarios para su actuación de la Agencia Estatal de Administración Tributaria, la Tesorería General de la Seguridad Social y el Instituto Nacional de Estadística, este último en lo relativo al padrón municipal de habitantes, lo cual ha de realizarse de acuerdo con la legislación sobre protección de datos sin que sea preciso el consentimiento del interesado. Al respecto, conviene hacer notar que la mención del precepto a los procedimientos administrativos tramitados en el ámbito de la Ley Orgánica de derechos y libertades de los extranjeros no puede entenderse sino haciendo referencia a la tramitación de un determinado expediente en el que resulta necesaria la constancia de determinado dato que ya obra en poder de otro órgano de la Administración General del Estado, tratándose así de un acceso específico en cada caso ajustado a los datos que resulten precisos para la tramitación de un expediente determinado y no de un acceso masivo o indiscriminado. La finalidad de esa cesión no es otra que comunicar el contenido de ficheros con datos tributarios, de Seguridad Social o de residencia, datos que, en cualquier caso, son ya previamente conocidos por la Administración General del Estado, atendiendo a la necesidad de que la misma disponga de la información oportuna para la gestión de procedimientos en materia de extranjería que son también de su competencia. Por ello, en la medida en que han de tratarse de datos relacionados con un concreto procedimiento y que ya obran en poder de la Administración pública, no puede considerarse vulnerado el art. 18.4 CE. En todo caso, como ya hemos señalado, tal acceso solamente puede producirse cuando ese dato resulte necesario o pertinente en*

*relación con la tramitación de un concreto expediente, lo que permite analizar o determinar en cada caso la conformidad del acceso con lo establecido en el régimen legal que le resulta de aplicación. Así, rectamente interpretada en los términos antes expuestos, resulta que esa cesión de datos que el acceso previsto supone ha de realizarse de acuerdo con lo que al respecto disponga la Ley Orgánica de protección de datos lo que determina, no solamente la aplicación de lo que la misma dispone en materia de información al interesado respecto de la cesión de datos (art. 5.4 LOPD), sino también que la cesión, establecida en una norma legal [art.11.2 a) LOPD], se produce para el cumplimiento de finalidades legítimas del órgano cedente y del cesionario (art. 4.1 LOPD), finalidades que, desde el punto de vista material, no resultan ser incompatibles entre sí (art. 4.2 LOPD), sino que, por el contrario, los datos son comunicados para el cumplimiento de fines directamente relacionados con las funciones legítimas de cedente y cesionario que contribuyen a garantizar un bien de relevancia constitucional: dar cumplimiento a lo dispuesto en la ley, en este caso la de extranjería (arts. 10.1 y 13.1 CE).*

Asimismo, en su FJ 8, interpreta el artículo 16.3 de la Ley de Bases de Régimen Local para determinar la constitucionalidad del mismo. 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.

Por consiguiente, no cabe un acceso masivo e indiscriminado a datos personales, y por lo tanto, en cambio, cuando exista la posibilidad de cesión establecida en una ley, como ocurre en el presente caso, dicho acceso deberá ser siempre “específico en cada caso ajustado a los datos que resulten precisos para la tramitación de un expediente determinado y no de un acceso masivo e indiscriminado”; “tal acceso sólo podría producirse cuando ese dato resulte necesario o pertinente en relación con la tramitación de un concreto expediente, lo que permite analizar o determinar en cada caso la conformidad del acceso con lo establecido en el régimen General que le resulte de aplicación.” (STC 19/2013, FJ 7º).

Estas previsiones, que alcanzan a todos los sistemas contemplados en el proyecto, tiene especial relevancia al incluirse entre los mismos el Sistema de Vigilancia de las Enfermedades No Transmisibles, que incluirá la vigilancia del cáncer, así como otras que se citan en la MAIN (salud mental, diabetes, enfermedades cardiovasculares, entre otras) que afectan a un elevado número de personas.

Teniendo en cuenta que la Red va a integrar todos los sistemas de información, deben adoptarse todas las garantías necesarias para evitar el tratamiento masivo e indiscriminado de datos personales referidos a la salud de las personas.

Asimismo, debe precisarse respecto de la interoperabilidad, que el uso de los identificadores personales solo procederá cuando sea estrictamente necesario, debiendo adoptarse las medidas técnicas oportunas que eviten el uso indebido de los mismos.

4. Por las mismas razones señaladas en el apartado anterior, debe suprimirse el último párrafo del apartado 7, en el que se señala que *“Para el cumplimiento de las funciones de vigilancia se garantizará un acceso general a las historias clínicas y no solo de forma individualizada al personal autorizado en vigilancia en salud pública ya que estas funciones son consideradas como actividad fundamental del sistema sanitario de acuerdo a lo establecido en el artículo 8.1 de la Ley 14/1986, de 25 de abril”*.

Sin perjuicio de la consideración como actividad fundamental del sistema sanitario, debe atenderse a las garantías específicas establecidas legalmente para compatibilizar dicha actividad con la protección del derecho fundamental a la protección de datos personales, sin que las mismas se puedan desconocer por vía reglamentaria, tal y como se ha indicado. Y, en este sentido, el acceso a las historias clínicas es objeto de una regulación específica en el artículo 16 de la Ley 41/2002, de 14 de noviembre, que no contempla dicho acceso generalizado, sino particularizado y motivado.

5. Las referencias al deber de información deberían contenerse en un apartado específico. Sin perjuicio de que resulte de aplicación la excepción del artículo 14.5.d), debería garantizarse que se informa al afectado en el momento de recabar los datos del mismo, conforme a lo previsto en el artículo 13, que dichos datos podrán ser comunicados a la Red Estatal de Vigilancia en Salud Pública.

6.- En el apartado 9 se contempla la posible cesión de los datos a terceras partes en los siguientes términos: “9. Los datos recogidos por la Red podrán cederse a terceras partes siempre que se garantice la protección de la confidencialidad y la privacidad. La cesión de datos a terceras partes deberá responder a las finalidades que establece este real decreto. Este uso está de acuerdo con lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre”.

A este respecto, la única previsión que respecto de dicha comunicación a terceros se contiene en el proyecto de real decreto es la atribución de competencias en el artículo 7.1.d) al Ministerio de Sanidad, a través del órgano de coordinación de la Red para *Establecer el procedimiento que establezca el acceso a los datos recogidos por la Red a terceras partes*.

Sin embargo, no se identifica en el proyecto quiénes pueden ser esas terceras partes, ni las razones que justificarían las comunicaciones a las mismas de los datos personales que puedan ser objeto de tratamiento en la Red. Tampoco de la normativa legal examinada resultaría la necesidad de comunicar datos personales a terceros, más allá de la finalidad específica contemplada en el artículo 6.e) del proyecto referida a *“Apoyar el desarrollo de planes genéricos y específicos de preparación y respuesta frente a posibles eventos de importancia en salud pública y de acciones de respuesta ante la aparición de alertas y emergencias en salud pública”* cuya ejecución no requiere el tratamiento de datos de carácter personal. Por lo tanto, debería recogerse que dicha comunicación se realizará previa disociación de los datos de carácter personal, en forma anónima y desagregada.

En el caso de que se prevean otros destinatarios, deberían identificarse las categorías de destinatarios así como que la comunicación se realizará previa anonimización o, en su caso, seudonimización, de los datos, recogiendo el carácter excepcional del tratamiento de los datos identificativos cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población.

7.- El apartado 10 prevé que “El Comité de Gestión de la Red elaborará el procedimiento de acceso a los datos recogidos por la Red y el tratamiento de los mismos conforme a la normativa de Protección de Datos”. Esta previsión, que no incluye el acceso por terceras partes al que anteriormente nos hemos referido, que es competencia del órgano de coordinación de la Red, parece ir referida al propio funcionamiento de cada sistema de vigilancia y de la Red en su conjunto, por lo que debería incluirse dentro de las competencias que al mismo se atribuyen en el artículo 9.1., así como que lo hará previa la realización de una evaluación de protección de datos personales, conforme al artículo 35 del RGPD.

Por otro lado, debería revisarse la MAIN para verificar que los datos personales cuyo tratamiento se prevé en el Sistema de Alerta Precoz y Respuesta Rápida así como los destinatarios se corresponde con las consideraciones anteriores, e incluir en la disposición adicional, tal y como se ha señalado anteriormente, las categorías de datos personales que podrán ser objeto de tratamiento en este sistema y las categorías de destinatarios, al ser el único que se regula por el proyecto de real decreto.

Por último, debe tenerse en cuenta que el objeto del proyecto remitido se verá afectado, una vez que se proceda a su aprobación, por la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios, ya que el artículo 34.1a) incluye, entre los fines para los que pueden tratarse datos sanitarios electrónicos para uso secundario, *“las actividades de interés público en el ámbito de la salud pública y la salud laboral, como la protección contra las amenazas transfronterizas graves para la salud, la vigilancia de la salud pública o la garantía de unos niveles elevados*



*de calidad y seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios". A este respecto, la propuesta recoge una serie de garantías específicas dirigidas a garantizar la protección de datos de carácter personal, que deberían tenerse en cuenta, como son las relativas a la prohibición del uso secundario de datos sanitarios electrónicos (artículo 35), las funciones de los organismos de acceso a los datos sanitarios (artículo 37) la minimización de datos y limitación de la finalidad (artículo 44), las solicitudes de acceso a los datos (artículo 45) o el entorno de tratamiento seguro (artículo 50).*

Asimismo, en relación con el desarrollo de espacios comunes de datos al amparo del Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos o DGA), esta Agencia ha publicado recientemente el documento "Aproximación a los espacios de datos desde la perspectiva del RGPD" (<https://www.aepd.es/es/documento/aproximacion-espacios-datos-rgpd.pdf>), con recomendaciones que pueden ser de utilidad en el presente caso para el adecuado cumplimiento del RGPD.