Resolución 803/2020

S/REF: 001-049456

N/REF: R/0803/2020; 100-004453

Fecha: La de firma

Reclamante: [redacted]

Dirección [redacted]

Administración/Organismo: Ministerio de Ciencia e Innovación

Información solicitada: Aplicación SIVIES

Sentido de la resolución: Desestimatoria

I. ANTECEDENTES

1. Según se desprende de la documentación obrante en el expediente, el reclamante solicitó al MINISTERIO DE CIENCIA E INNOVACIÓN, al amparo de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno[1] (en adelante LTAIBG), con fecha 28 de octubre de 2020, la siguiente información:

   Solicito la siguiente información sobre la base de datos y aplicación SiViEs:

   - La documentación del software del sistema SiViEs con todos los documentos que tenga. Incluyendo todos los tipos de documentación que haya, como, por ejemplo: documentación para los usuarios, para los desarrolladores, sobre las pruebas del software -pruebas unitarias-, registro de actualizaciones del software, documentación del diseño y arquitectura del sistema, documentación del código fuente...

[1] https://www.boe.es/buscar/doc.php?id=BOE-A-2013-12887

[redacted]

- Documentación de la estructura de la base de datos de SiViEs, que según los documentos públicos, https://administracionelectronica.gob.es/pae_Home/dam/jcr:35d6af28-9efc-4ae0-81a8-c8ae00cbb52f/48eficiencia.pdf, está implementada en SQL Server. Solicito también que se me indique si es así o hay partes implementadas en otros lenguajes. Solicito también que se incluya el mapa de la base de datos y el detalle de todas y cada una de las tablas que contiene la base de datos y especificando qué representan los registros que contienen cada una de ellas, si son casos diagnosticados de una enfermedad, por ejemplo, y el número total de registros que contienen y cuántos campos distintos hay en cada tabla y cuáles son. Por ejemplo: existe la tabla con tal nombre, donde se incluyen registros para todos y cada uno de los casos de covid, en total hay tantos registros, y para cada uno hay los campos de fecha de diagnóstico y sexo del paciente.

- Detalle de con qué software está creado SiViEs y con cuál software y sistema de gestión de base de datos se gestiona.

Toda la información solicitada es de indudable interés y carácter público, más en un momento como el actual en el que vivimos una pandemia sanitaria debido al coronavirus y la aplicación que se está utilizando en España para gestionar la información de los casos de esta enfermedad es precisamente SiViEs.

Recuerdo, además, la existencia del derecho de acceso de forma parcial. En el caso de que se me deniegue o no entregue parte de la información solicitada, esto no es óbice para no entregar el resto de lo pedido.

2. Mediante Resolución de 16 de noviembre de 2020, el MINISTERIO DE CIENCIA E INNOVACIÓN contestó al solicitante lo siguiente:

3º. Con fecha de 29 de octubre, la UIT MCIN remite dicha solicitud a la Secretaría General de Investigación y, una vez analizada, en virtud de lo dispuesto el artículo 14.1.k de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, deniega el acceso a la información solicitada, considerando que la difusión de dicha información supone un perjuicio para la garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión, por los motivos que a continuación se indican:

a) En primer lugar el solicitante ha tenido acceso a una parte de la información que solicita, y que es pública, sobre la base de datos SIVIEs a través de la dirección web:

https://administracionelectronica.gob.es/pae_Home/dam/jcr:35d6af28-9efc-4ae0-81a8-c8ae00cbb52f/48eficiencia.pdf

[redacted]

El solicitante, en síntesis, requiere "La documentación del software del sistema SiViEs con todos los documentos que tenga" "mapa de la base de datos y el detalle de todas y cada una de las tablas que contiene la base de datos y especificando que representan los registros que contienen cada una de ellas, si son casos diagnosticados de una enfermedad …/…" es decir, solicita toda la información de la que disponga el Instituto de Salud Carlos III sobre la aplicación SIVIEs.

b) La información solicitada se refiere a la aplicación SiViEs, Sistema de Vigilancia de España, responsable de recoger datos epidemiológicos de las enfermedades de declaración obligatoria, tales como cólera, VIH SIDA, lepra, hepatitis, otras y, recientemente COVID 19, asimismo recoge los datos de brotes y las alertas sanitarias; recientemente la alerta producida por la expansión de la enfermedad COVID19. Concretamente, esta función está explicitada expresamente en la legislación vigente, en la Orden SND/404/2020, de 11 de mayo, de medidas de vigilancia epidemiológica de la infección por SARS-CoV-2 durante la fase de transición hacia una nueva normalidad.

Mediante Real Decreto 2210/1995, de 28 de diciembre, se crea la red nacional de vigilancia epidemiológica (RENAVE), con el objeto de permitir la recogida y el análisis de la información epidemiológica con la finalidad de poder detectar problemas, valorar los cambios en el tiempo y en el espacio, contribuir a la aplicación de medidas de control individual y colectivo de los problemas que supongan un riesgo para la salud de incidencia e interés nacional o internacional y difundir la información a sus niveles operativos competentes. Con el objeto de que, mediante la vigilancia epidemiológica, las Administraciones sanitarias dispongan de la información necesaria para la toma de decisiones.

En el momento de creación de la RENAVE el Instituto de Salud Carlos III (ISCIII) estaba adscrito al Ministerio de Sanidad, manteniendo en la actualidad una doble dependencia funcional del Ministerio de Ciencia e Innovación y del Ministerio de Sanidad, en particular, el ISCIII depende funcionalmente del Ministerio de Sanidad para la realización de aquellas actividades que desarrolle en materia de salud, de planificación y asistencia sanitaria y, en coordinación con el Ministerio de Ciencia e Innovación, de aquellas otras de investigación aplicada cuando tengan traslación al Sistema Nacional de Salud.

Por tanto, en el caso de la RENAVE y de la aplicación SIVIEs, el ISCIII depende del Ministerio de Sanidad. El Centro Nacional de Epidemiología/Instituto de Salud Carlos III gestiona la RENAVE pero los datos son de las Comunidades Autónomas y del Ministerio de Sanidad.

[redacted]

La Red nacional de vigilancia epidemiológica se encuentra al servicio del Sistema Nacional de Salud. El análisis de la información que las Comunidades Autónomas incluyen en la aplicación no la realiza SIVIEs, es el Ministerio de Sanidad y las autoridades competentes las que acceden a la aplicación y realizan los análisis oportunos.

c) El solicitante pretende el acceso a las especificaciones técnicas de la aplicación SIVIEs, en las que se incluyen todos aquellos requisitos de seguridad para proteger la información frente a ataques y a vulneraciones. La difusión de esta información posibilitaría el ataque al sistema y el acceso a toda la información que contiene SIVIEs, es decir, a todos los procesos de vigilancia epidemiológica.

d) El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, Anexo II, dispone que es obligación de la Administración, desde el nivel más bajo de protección de sus aplicaciones, aplicar las medidas de seguridad en el marco operacional que permitan prevenir "ataques que puedan revelar información del sistema sin llegar a acceder al mismo" (4.2.6) y garantizar "la seguridad del sistema cuando accedan remotamente usuarios u otras entidades, lo que implicará proteger tanto el acceso en sí mismo […] como el canal de acceso remoto" (4.2.7).

e) La Orden SND/404/2020, de 11 de mayo, dispone que, la información individualizada de casos confirmados de CVID19, se enviará al Ministerio de Sanidad a través de la herramienta de vigilancia SiViEs que gestiona el Centro Nacional de Epidemiología del Instituto de Salud Carlos

III. En su artículo 9 establece que el tratamiento de la información de carácter personal que se realice como consecuencia del desarrollo y aplicación de esta orden se hará de acuerdo 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, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y en lo establecido en los artículos ocho.1 y veintitrés de la Ley 14/1986, de 25 de abril, General de Sanidad. …/…

El tratamiento tiene por finalidad el seguimiento y vigilancia epidemiológica del COVID-19 para prevenir y evitar situaciones excepcionales de especial gravedad, atendiendo a razones de interés público esencial en el ámbito específico de la salud pública, y para la protección de intereses vitales de los afectados y de otras personas físicas al amparo de lo

[redacted]

establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

El responsable del tratamiento será el Ministerio de Sanidad, que garantizará 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.

f) Sobre la información solicitada recaen las consideraciones del artículo 43, Seguridad de la Información, de la Ley 33/2011, de 4 de octubre, General de Salud Pública, que establece la obligación de guardar secreto en relación con los Sistemas de Información del Sistema Nacional Código de Salud e insta, muy concretamente en su punto 1, a que "En todos los niveles del sistema de información en salud pública se adoptarán las medidas necesarias para garantizar la seguridad de los datos", estas medidas serían imposibles de garantizar de revelarse la información solicitada; otrosí, el punto 2 subraya el carácter secreto en los siguientes términos: "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".

g) En el momento actual, la aplicación SIVIEs podría considerarse una infraestructura estratégica a los efectos de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, que en su artículo 2.d) define a estas como "las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales"; sobre SIVIEs descansa una parte importante del control de la pandemia provocada por la enfermedad COVID19, así queda establecido en la Orden SND/404/2020, de 11 de mayo, de medidas de vigilancia epidemiológica de la infección por SARS-CoV-2 durante la fase de transición hacia una nueva normalidad, por tanto se trata de un sistema sobre el que descansa el funcionamiento de un servicio esencial.

h) Por último, la legislación española ya prevé la protección especial de aplicaciones destinadas a la lucha contra la COVID-19, así en la Resolución de 30 de abril de 2020, de la Secretaría General de Administración Digital, por la que se publica el Convenio entre la Secretaría de Estado de Digitalización e Inteligencia Artificial y Telefónica Digital España, SLU, para la operación de la Aplicación ASISTENCIACOVID19 en el contexto de la situación de crisis sanitaria ocasionada por el COVID-19, Cláusula Decimonovena, Deber de secreto, la norma dispone: "Ambas partes se comprometen a guardar la máxima reserva y secreto

[redacted]

sobre la información calificada como confidencial facilitada por una, a la otra, con motivo de la colaboración en las actividades objeto de este Convenio." Dicha aplicación es, de acuerdo con su Cláusula segunda, Características de la aplicación, meramente asistencial y de apoyo al ciudadano particular; con mayor razón debe imperar este deber de secreto sobre la aplicación objeto de la solicitud, SiViEs, cuyo impacto alcanza a toda la población de España y su función es la de gestionar y controlar la evolución epidemiológica de las enfermedades de declaración obligatoria, incluida la de la pandemia que sufre España como consecuencia de la expansión del virus SARS-COV-2.

3. Ante la citada respuesta, mediante escrito de entrada el 19 de noviembre de 2020, el interesado presentó, al amparo de lo dispuesto en el artículo 24[2] de la LTAIBG, una reclamación ante el Consejo de Transparencia y Buen Gobierno, con el siguiente contenido:

   El ministerio me deniega lo solicitado alegando por un lado que ya he accedido a parte de ello aquí:

   https://administracionelectronica.gob.es/pae_Home/dam/jcr:35d6af28-9efc-4ae0-81a8-c8ae00cbb52f/48eficiencia.pdf

   Una publicación académica que hacen miembros del ISCIII hace años y que yo mismo les indico en mi petición. No cubre en ningún caso, por lo tanto, lo que estoy solicitando ni sirve, como es obvio, para dar por satisfecho el derecho al acceso.

   Por otro lado, el ministerio argumenta que por motivos de seguridad no me pueden dar acceso a lo solicitado. Pero no realizan una ponderación ni alegan por el límite concreto que deniegan la información.

   El artículo 14.2 de la Ley 19/2013 determina que "la aplicación de los límites será justificada y proporcionada a su objeto y finalidad de protección y atenderá a las circunstancias del caso concreto, especialmente a la concurrencia de un interés público o privado superior que justifique el acceso". En este sentido, el criterio interpretativo CI/002/2015 del CTBG afirma que "los límites no operan ni automáticamente a favor de la denegación ni absolutamente en relación a los contenidos", para lo cual "deberá analizarse si la estimación de la petición de información supone un perjuicio /test del daño) concreto, definido y evaluable". En el presente caso, se ha omitido cualquier razonamiento que justifique la aplicación del límite y de hecho ni siquiera se ha cita el límite. Estableciendo

[2] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&tn=1&p=20181206#a24

[redacted]

que los límites, aunque no citados, sí operan automáticamente a favor de la denegación, circunstancia que va contra el criterio del CTBG.

El Preámbulo de la Ley 19/2013 señala que "los límites previstos se aplicarán atendiendo a un test de daño (del interés que se salvaguarda con el límite) y de interés público en la divulgación (que en el caso concreto no prevalezca el interés público en la divulgación de la información) y de forma proporcionada y limitada por su objeto y finalidad". Asimismo, el CTBG, en su criterio interpretativo CI/002/2015 advierte de que la aplicación de los límites "no podrá afectar o ser relevante para un determinado ámbito material, porque de lo contrario se estaría excluyendo un bloque completo de información", lo cual sucede en este caso.

Que haya parte de la información solicitada que pueda perjudicar a la seguridad del Estado no es óbice para no entregar absolutamente nada de toda la documentación solicitada. De hecho, no han justificado qué partes de la información solicitada podrían vulnerar la seguridad y por qué y la petición de información ya explicaba además la existencia del derecho de acceso a la información parcial pidiendo que si se denegaba parte de la información, se entregara el resto.

No justifican de qué forma puede afectar a la seguridad ya que la estructura interna del sistema que se ha solicitado para saber cómo se almacena y procesa la información no deja al aire vulnerabilidades. Se trata de una red cerrada que no es accesible más que por los responsables de salud pública de cada comunidad y, por lo tanto, que la gente pueda conocer como está estructurada o formada tampoco les permitiría acceder a ella y, por lo tanto, vulnerarla.

Conocer qué softwares se utilizan para gestionarla o cuáles se usaron para crearla o conocer el mapa de la base de datos, por ejemplo, en ningún caso supone una vulneración, ya que con esa información la gente seguiría sin poder acceder a ella. Pero se trata de rendición de cuentas, ya que la ciudadanía tiene derecho a conocer cómo se ha hecho, cómo se gestiona y de qué forma está estructurada y qué datos se almacenan.

De hecho, cabe tener en cuenta que para otras aplicaciones de la Administración se ha liberado incluso el código, como es el caso de Radar COVID. De hecho, eso ha servido para que la ciudadanía detecte fallos de seguridad de la aplicación y la Administración haya podido arreglarlos antes de recibir un ataque por esos errores. La liberación y el acceso público a este tipo de información permite la rendición de cuentas y el conocimiento colectivo. Una ciudadanía bien informada con acceso a toda esa información ayuda a que la Administración se haga más eficaz y mejore su trabajo.

[redacted]

El ministerio además alega con un real decreto que menciona que la Administración debe proteger la seguridad de la aplicación de ataques que puedan revelar información. Proteger su seguridad no supone que no deba entregar información a la ciudadanía sobre esa aplicación a través del derecho de acceso. Más cuando no se está pidiendo información del contenido, sino simplemente conocer cómo está realizada y cómo está estructurada y gestionada. Si se quisieran conocer datos concretos que se contienen en ella, podría tener sentido esta denegación, pero no ante la presente solicitud. Lo mismo que cuando alegan datos personales. No se está pidiendo información sobre ningún caso de coronavirus y, por lo tanto, ningún dato personal, sino simplemente información sobre la herramienta que debe ser pública: la ciudadanía tiene derecho a conocer cómo se están gestionando y de qué forma los datos de los casos de coronavirus ante una situación tan importante y grave como la que estamos viviendo.

Por último, el ministerio también hace mención que lo solicitado pertenece al Ministerio de Sanidad y no al de Ciencia. Esto en ningún caso sirve tampoco para denegar lo solicitado. La petición se dirigía al Instituto de Salud Carlos III que depende de ambos. Era tan fácil como que se hubiera resuelto desde el propio ISC III o que se hubiera derivado la solicitud a Sanidad. En procedimientos anteriores este solicitante ha pedido información sobre SiViEs al Ministerio de Sanidad y este la ha derivado a Ciencia, que ha sido el departamento que se ha encargado de resolver siempre las peticiones de información sobre el SiViEs. De todos modos, como menciono, simplemente se debería haber hecho una derivación.

El criterio interpretativo CI/007/2015 del Consejo de Transparencia y Buen Gobierno establece que cuando "la información se encuentre en poder de varias unidades informantes que resultan responsables de su custodia pero su autor esté claramente definido (…) tampoco se trataría de un caso de reelaboración, operando el artículo 19.4 de la Ley 19/2013 que establece que: "Cuando la información objeto de la solicitud, aun obrando en poder del sujeto al que se dirige, haya sido elaborada o generada en su integridad o parte principal por otro, se le remitirá la solicitud a éste para que decida sobre el acceso".

Por todo ello, solicito que se estime mi reclamación y se inste a la Administración a entregarme lo que había solicitado.

Recuerdo también que antes de resolver solicito una copia del expediente completo, incluidas las alegaciones de la administración, para que yo como reclamante pueda alegar lo que considere oportuno.

[redacted]

4. Con fecha 20 de noviembre de 2020, el Consejo de Transparencia y Buen Gobierno remitió el expediente al MINISTERIO DE CIENCIA E INNOVACIÓN, al objeto de que se pudieran hacer las alegaciones que se considerasen oportunas. La respuesta a la solicitud de alegaciones tuvo entrada el 15 de diciembre de 2020 y en la misma, además de reiterar el contenido de su resolución, se indica lo siguiente:

   2º.En segundo lugar, el reclamante ha solicitado en cinco ocasiones anteriores, utilizando diferentes variables en cada petición pero con el mismo fondo, el acceso a todos los datos incluidos en la aplicación SIVIEs , sobre casos COVID19 notificados.

   A continuación, se enumeran los expedientes de las solicitudes y su tramitación:

   I. Nº de expediente 001-042325, de fecha 9 de abril de 2020, se dicta resolución del Secretario General de Investigación de fecha 13 de mayo de 2020 por la que se concede parcialmente el acceso a la información solicitada; el solicitante presenta reclamación ante el Consejo de Transparencia y Buen Gobierno con nº 100-003665 y fecha 1 de junio de 2020, el Secretario General de Investigación presenta alegaciones y el CTBG dicta la Resolución 246/2020 que estima parcialmente la reclamación.

   II. Nº de expediente 001-043416, de fecha 1 de junio de 2020; resolución del Secretario General de Investigación de fecha 24 de junio de 2020 que, motivadamente, deniega el acceso a la información solicitada de acuerdo con los establecido en el artículo 15.1 de la Ley 19/2013; el solicitante presenta reclamación ante el Consejo de Transparencia y Buen Gobierno con nº 100-003923 y fecha 23 de julio de 2020; se presentan alegaciones y el CTBG dicta la Resolución 422/2020 que desestima la reclamación.

   lll.Nº de expediente 001-044876, de fecha 27 de julio de 2020, en la que, entre otros datos recogidos en la aplicación SIVIEs, solicita información sobre personal sanitario infectado por COVID19; en este caso el ISCIII indica a la UIT del MICINN que las peticiones de información que afecten a personal sanitario deben ser enviadas al centro de Coordinación de Alertas y Emergencias Sanitarias del Ministerio de Sanidad. El ISCIII desconoce el resultado de la tramitación de esta petición.

   IV. Nº de expediente 001-047990, que, de forma motivada, en virtud de lo dispuesto en el artículo 18.1.e) de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, se inadmite a trámite, considerándola manifiestamente repetitiva; el solicitante presenta reclamación ante el Consejo de Transparencia y Buen Gobierno con nº 100-004324 y fecha 28 de octubre de 2020; el

[redacted]

Secretario General de Investigación presenta las alegaciones pertinentes; a fecha de elaboración de las presentes el CTBG no ha dictado resolución.

V. Nº de expediente 001-049456, el interesado solicita información técnica sobre la aplicación SIVIEs; en virtud de lo dispuesto en el artículo el artículo 14.1.k de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, se inadmite la solicitud; el solicitante presenta reclamación ante el CTBG objeto de las presentes alegaciones.

Esta introducción en relación con las solicitudes de acceso a la información presentadas por [redacted] *y los resultados de su tramitación en cada caso, indica el interés manifiesto del solicitante en acceder a los datos contenidos en la aplicación SIVIEs.*

(…)

6º. Ante esta reclamación se alega lo siguiente:

La información solicitada se refiere a la aplicación SiViEs, Sistema de Vigilancia de España, responsable de recoger datos epidemiológicos de las enfermedades de declaración obligatoria, tales como cólera, VIH SIDA, lepra, hepatitis, otras y, recientemente, COVID 19, asimismo recoge los datos de brotes y las alertas sanitarias; recientemente, la alerta producida por la expansión de la enfermedad COVID19.

Concretamente esta función está explicitada expresamente en la Orden SND/404/2020, de 11 de mayo, de medidas de vigilancia epidemiológica de la infección por SARS-CoV-2 durante la fase de transición hacia una nueva normalidad.

Por tanto, toda la información incluida en SIVIEs es altamente sensible, tanto desde el punto de vista de la salvaguarda sanitaria como desde la protección de los datos personales incorporados a la aplicación informática.

(…)

La denegación de la información viene motivada, como queda recogido en la resolución de 16 de noviembre de 2020, en los límites derivados de la obligación de la Administración de salvaguardar dicha información en obligado cumplimiento y aplicación de diferentes normas vigentes, como así queda recogido en la resolución objeto de reclamación: Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad; Orden SND/404/2020, de 11 de mayo, en relación con lo dispuesto en el Reglamento europeo de protección de datos, en la Ley Orgánica 3/2018, de 5 de diciembre, de

[redacted]

Protección de Datos Personales y garantía de los derechos digitales, y en lo establecido en los artículos ocho.1 y veintitrés de la Ley 14/1986, de 25 de abril, General de Sanidad, Ley 33/2011, de 4 de octubre, General de Salud Pública, que establece la obligación de guardar secreto en relación con los Sistemas de Información del Sistema Nacional de Salud, etc.

(…)

Ante esta afirmación se alega que la app Radar COVID no recoge ningún dato personal ni de geolocalización, por tanto, el acceso a la misma no podrá permitir la vulneración de derechos personales, ni de datos sanitarios protegidos legalmente. Situación completamente distinta de lo que sucedería en el caso de acceso no autorizado a la aplicación SIVIEs por la información altamente protegida y sensible que contiene: datos epidemiológicos de las enfermedades de declaración obligatoria - tales como cólera, VIH SIDA, lepra, hepatitis, COVID 19 - datos de brotes y las alertas sanitarias.

No obstante, valorada la reclamación y en respuesta a lo planteado por el reclamante: "Conocer qué softwares se utilizan para gestionarla o cuáles se usaron para crearla o conocer el mapa de la base de datos, por ejemplo, en ningún caso supone una vulneración, ya que con esa información la gente seguiría sin poder acceder a ella", mediante las presentes alegaciones, el Instituto de Salud Carlos III facilita la siguiente información:

DESCRIPCIÓN DEL SISTEMA INFORMÁTICO SiViEs

SiViEs, técnicamente es una aplicación Web diseñada basándose en un modelo típico de tres capas (datos, negocio y presentación). Es un portal de acceso restringido que cumple las necesidades de recogida de datos, tratamiento, transformación, consulta/análisis de la información epidemiológica, gestión y administración de la configuración del sistema, generación de documentación automática y administración de seguridad y permisos.

SiViEs contempla las diferentes formas de presentación de la enfermedad (casos individuales, casos agregados, brotes) y las diferentes definiciones de un caso de una enfermedad (sospechoso, probable, confirmado) y sus diferentes fuentes de información. Suministra apoyo científico-técnico a RENAVE (Red Nacional de Vigilancia Epidemiológica), estandarizando y facilitando la gestión de enfermedades, integrando las múltiples fuentes de información y estableciendo un sistema de soporte a la detección y seguimiento de incidencias. La plataforma también debe posibilitar la elaboración de estudios sobre la información recogida en aras de la investigación y permite la participación de actores como las CCAA y otros entes a través de un sistema completo de gestión de perfiles y servicios Web para la completa automatización.

[redacted]

SiViEs facilita la comunicación con otros Organismos nacionales e internacionales mediante la transformación y envío de datos en origen.

MÓDULOS QUE CONFIGURAN EL SISTEMA SiViEs

***Módulo de Configuración de Fichas**: permite elaborar los cuestionarios (fichas) con las preguntas (campos) de cada enfermedad o tipo de brote, agrupándolas de forma visual dentro de bloques de información asociada.*

***Módulo de Configuración de Tablas**; permite crear tablas en la propia Base de Datos definiendo las columnas con su tipo de datos y sus atributos. En estas tablas se pueden insertar filas para almacenar la información vinculada al dominio de las respuestas a las preguntas de un cuestionario sobre una enfermedad (lista de valores). Además, se pueden agregar nuevas enfermedades y fuentes de datos.*

***Módulo de Entrada**: permite la declaración de brotes, casos individualizados o casos agregados, bien de forma automática, a través de ficheros en formato texto CSV o en formato XML (servicio que se expone mediante servicios web), o bien de forma manual a través de la incorporación directa de la información a través de formularios.*

***Módulo de Documentación y Ayuda**: permite autogenerar un documento (metadatos) en el que los declarantes tengan toda la información necesaria (características de los campos de cada ficha de cada enfermedad, tipo de brote, etc.) para realizar la declaración.*

***Módulo de Salida**: permite la generación de consultas dinámicas, informes, gráficas y mapas sobre los datos almacenados.*

***Módulo de Gestión de Dup**licados: permite detectar si un mismo caso puede haber sido informado por varias CCAA, dado que un ciudadano puede ser atendido en varios territorios, para descartarlo del sistema.*

***Módulo de Transformación de Datos**: permite llevar a cabo transformaciones de fichas a otras fichas distintas de modo que sea posible realizar mapeos de los formatos nacionales a los requeridos por Organismos internacionales.*

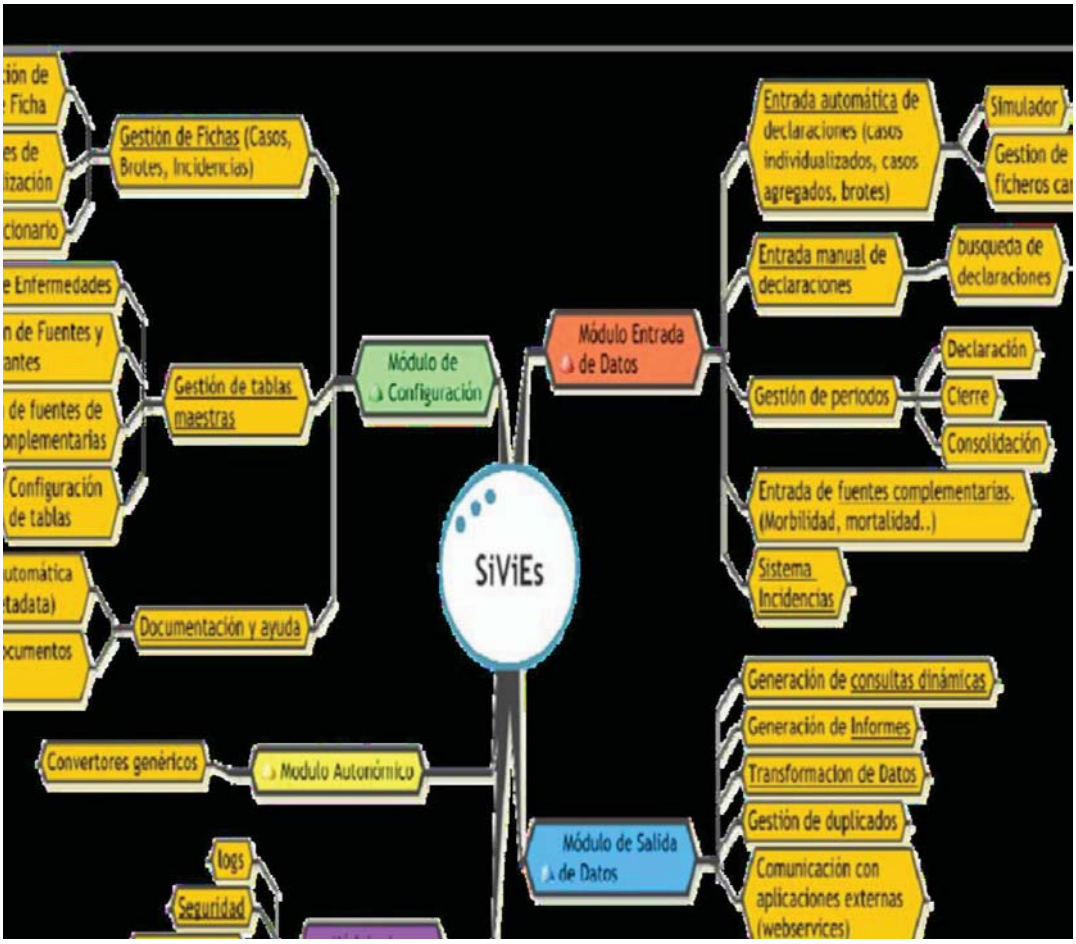
***Módulo de Gestión de Incidencias**: permite que los actores introduzcan incidencias epidemiológicas (información relativa a un riesgo para la salud y/o de utilidad para el seguimiento de una enfermedad/infección o síndrome). El módulo dispone de un sistema de mensajería electrónica para notificar a los usuarios implicados.*

[redacted]

***Módulo de Gestión de Seguridad/Perfiles**: permite controlar los permisos de acceso a la aplicación que se pueden realizar, bien mediante autenticación basada en usuario/contraseña contra directorio activo o bien mediante certificado digital. El nivel de granularidad del perfilado es muy fina.*

En el sistema, todas las conexiones se realizan cifradas hacia servidores configurados en instalaciones que cumplen las normativas. El sistema está concebido para soportar alta disponibilidad, de forma que si se instala en varios servidores es capaz de seguir operando en caso de fallo.

Gráfico con la descripción de los componentes básicos del sistema



PLATAFORMA TECNOLÓGICA

[redacted]

Las tecnologías utilizadas son: .Net; Asp.net para las páginas Web, Wcf (Workflow classes foundation) para el control de flujos de procesos, SQL Server 2012 como gestor de Base de Datos, Integration Services como herramienta de transformación de datos y Team Server para control de gestión de la configuración y trabajo en equipo. Se usa Windows Server 2012 como software base para los servidores de datos y aplicaciones.

PROCESO DE TRATAMIENTO EN SIVIEs

Diariamente, las CCAA y las Ciudades Autónomas de Ceuta y Melilla preparan un fichero, en el formato establecido, con la información de los pacientes que van a remitir al sistema informático SiViEs. El fichero lo cargan en el sistema SiViEs, bien a través de la opción prevista en el sistema para recibir ficheros o bien a través del envío máquina a máquina utilizando servicios web.

Los ficheros recibidos en SiViEs se validan previamente, verificando que cumplen las reglas correctas para su recepción (fechas válidas y coherentes, campos obligatorios de cumplimentación). Si algún registro del fichero no cumple con la validación establecida el fichero se rechaza en su totalidad. SiViEs permite al usuario identificar si el fichero se ha aceptado o rechazado y las causas por las cuales ha sido rechazado.

Una vez corregido el fichero se realiza el mismo procedimiento de carga descrito.

Aceptado el fichero se procesan los registros para almacenar en SiViEs la información recibida. El sistema a través de los informes y consultas establecidas facilita la información almacenada a los usuarios autorizados.

5. El 16 de diciembre de 2021, en aplicación del art. 82 de la Ley 39/2015, de 1 de octubre[3], del Procedimiento Administrativo Común de las Administraciones Públicas, se dio Audiencia al reclamante para que formulase las alegaciones que estimara pertinentes. Mediante escrito de entrada el 31 de diciembre, el reclamante realizó las siguientes alegaciones:

   Agradezco la información que me han facilitado en fase de alegaciones, admitiendo así que depende de ellos lo solicitado, que es de utilidad para satisfacer mi petición pero que no lo hace al completo. No me informan ni sobre los softwares y lenguajes concretos usados para cada parte, ni me aportan lo siguiente:

[3] https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565&p=20181206&tn=1#a82

[redacted]

- La documentación del software del sistema SiViEs con todos los documentos que tenga. Incluyendo todos los tipos de documentación que haya, como, por ejemplo: documentación para los usuarios, para los desarrolladores, sobre las pruebas del software -pruebas unitarias-, registro de actualizaciones del software, documentación del diseño y arquitectura del sistema, documentación del código fuente...

- Documentación de la estructura de la base de datos de SiViEs, que según los documentos públicos, https://administracionelectronica.gob.es/pae_Home/dam/jcr:35d6af28-9efc-4ae0-81a 8-c8ae00cbb52f/48eficiencia.pdf, está implementada en SQL Server. Solicito también que se me indique si es así o hay partes implementadas en otros lenguajes. Solicito también que se incluya el mapa de la base de datos y el detalle de todas y cada una de las tablas que contiene la base de datos y especificando qué representan los registros que contienen cada una de ellas, si son casos diagnosticados de una enfermedad, por ejemplo, y el número total de registros que contienen y cuántos campos distintos hay en cada tabla y cuáles son. Por ejemplo: existe la tabla con tal nombre, donde se incluyen registros para todos y cada uno de los casos de covid, en total hay tantos registros, y para cada uno hay los campos de fecha de diagnóstico y sexo del paciente.

No quiero acceder a los datos de SiViEs en esta ocasión únicamente conocer cómo está estructurado es información de indudable interés público y no vulneraría ninguno de los puntos que el ministerio dice que vulneraría conocer los datos que contiene. Simplemente sería entregar la documentación sobre la base de datos y el detalle de las tablas que contiene, que no me lo han dado aún en alegaciones, y que supondría una indudable rendición de cuentas. La ciudadanía tiene derecho a conocer qué tablas contiene este sistema tan importante en la actual crisis pandémica y conocer qué datos almacenan exactamente. No pido los datos de nadie ni de ningún caso, sólo conocer qué datos se tienen sobre cada caso, es decir, la estructura de las tablas y el sistema. No supondría ninguna vulneración ni se me estaría entregando ningún dato de ninguna persona.

Pido, por lo tanto, que se siga adelante con la reclamación y se estime para que el ministerio deba entregarme lo que he solicitado. Haber pedido en otras ocasiones cosas relacionadas con SiViEs, como la información pedida no era la misma, no se trata de una petición abusiva ni repetitiva. Estoy en mi derecho como ciudadano a pedir distintas informaciones sobre la misma temática.

II. FUNDAMENTOS JURÍDICOS

[redacted]

1. De conformidad con lo dispuesto en el artículo 24 de la LTAIBG[4], en conexión con el artículo 8 del Real Decreto 919/2014, de 31 de octubre, por el que se aprueba el Estatuto del Consejo de Transparencia y Buen Gobierno[5], el Presidente de este Organismo es competente para resolver las reclamaciones que, que con carácter potestativo y previo a su eventual impugnación en vía contencioso-administrativa, se presenten frente a las resoluciones expresas o presuntas recaídas en materia de acceso a la información.

2. La LTAIBG, en su artículo 12[6], reconoce el derecho de todas las personas a acceder a la información pública, entendiendo por tal según dispone su artículo 13 "*los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones*".

   De este modo, la Ley delimita el ámbito material del derecho a partir de un concepto amplio de información, que abarca tanto documentos como contenidos específicos y que se extiende a todo tipo de "formato o soporte", a la vez que acota su alcance exigiendo la concurrencia de dos requisitos vinculados con la naturaleza "publica" de las informaciones: (a) que se encuentren "en poder" de alguno de los sujetos obligados por la ley, y (b) que hayan sido elaboradas u obtenidas "en el ejercicio de sus funciones".

3. Respecto al fondo del asunto cabe recordar que el objeto de la solicitud de información se centra en obtener:

   - La *documentación del software del sistema SiViEs con todos los documentos que tenga* (…) *por ejemplo: documentación para los usuarios, para los desarrolladores, sobre las pruebas del software -pruebas unitarias-, registro de actualizaciones del software, documentación del diseño y arquitectura del sistema, documentación del código fuente …*

   - *Documentación de la estructura de la base de datos de SiViEs*, si *está implementada en SQL Server (…) si es así o hay partes implementadas en otros lenguajes*.

   - *El mapa de la base de datos y el detalle de todas y cada una de las tablas que contiene la base de datos y especificando qué representan los registros que contienen cada una de ellas, si son casos diagnosticados de una enfermedad, por ejemplo, y el número total de registros que contienen y cuántos campos distintos hay en cada tabla y cuáles son.*

[4] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&p=20181206&tn=1#a24
[5] https://www.boe.es/buscar/act.php?id=BOE-A-2014-11410&tn=1&p=20141105#a8
[6] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&tn=1&p=20181206#a12

[redacted]

- *Detalle de con qué software está creado SiViEs y con cuál software y sistema de gestión de base de datos se gestiona.*

Por su parte, la Administración ha denegado la información al considerar de aplicación el límite previsto en el artículo 14.1 k), que dispone que *el derecho de acceso podrá ser limitado cuando acceder a la información suponga un perjuicio para: La garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión*.

Sostiene la Administración en apoyo de su denegación que *La difusión de esta información posibilitaría el ataque al sistema y el acceso a toda la información que contiene SIVIEs, es decir, a todos los procesos de vigilancia epidemiológica*, y *la Administración de salvaguardar dicha información en obligado cumplimiento y aplicación de diferentes normas vigentes*:

- *El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, Anexo II, dispone que es obligación de la Administración, desde el nivel más bajo de protección de sus aplicaciones, aplicar las medidas de seguridad en el marco operacional que permitan prevenir "ataques que puedan revelar información del sistema sin llegar a acceder al mismo" (4.2.6) y garantizar "la seguridad del sistema cuando accedan remotamente usuarios u otras entidades, lo que implicará proteger tanto el acceso en sí mismo […] como el canal de acceso remoto" (4.2.7).*

- *Orden SND/404/2020, de 11 de mayo,* (…) *el tratamiento de la información de carácter personal que se realice como consecuencia del desarrollo y aplicación de esta orden se hará de acuerdo 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,* en este caso *afectan a categorías especiales de datos.*

- El artículo 43 de la Ley 33/2011, de 4 de octubre, General de Salud Pública, que establece *la obligación de guardar secreto en relación con los Sistemas de Información del Sistema Nacional Código de Salud e insta, muy concretamente en su punto 1, a que "En todos los niveles del sistema de información en salud pública se adoptarán las medidas necesarias para garantizar la seguridad de los datos",* y *estas medidas serían imposibles de garantizar de revelarse la información solicitada*

- *La Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, que en su artículo 2.d) define a estas como "las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa*

[redacted]

el funcionamiento de los servicios esenciales"; sobre SIVIEs descansa una parte importante del control de la pandemia provocada por la enfermedad COVID19, así queda establecido en la Orden SND/404/2020, de 11 de mayo, de medidas de vigilancia epidemiológica de la infección por SARS-CoV-2 durante la fase de transición hacia una nueva normalidad, por tanto se trata de un sistema sobre el que descansa el funcionamiento de un servicio esencial, y *podría considerarse una infraestructura estratégica* .

4. A este respecto, debemos comenzar señalando que la aplicación de los límites contemplados en la LTAIBG debe ser acorde con el Criterio Interpretativo CI/002/2015[7], de 24 de junio, de este Consejo de Transparencia, elaborado en función de las competencias otorgadas por su artículo 38.2 a), Criterio en el que se indica que:

   "Los límites a que se refiere el artículo 14 de la LTAIBG, a diferencia de los relativos a la protección de los datos de carácter personal, no se aplican directamente, sino que de acuerdo con la literalidad del texto del número 1 del mismo, "podrán" ser aplicados.

   De esta manera, los límites no operan ni automáticamente a favor de la denegación ni absolutamente en relación a los contenidos.

   La invocación de motivos de interés público para limitar el acceso a la información deberá estar ligada con la protección concreta de un interés racional y legítimo.

   En este sentido su aplicación no será en ningún caso automática: antes al contrario ***deberá analizarse si la estimación de la petición de información supone un perjuicio (test del daño) concreto, definido y evaluable****. Este, además no podrá afectar o ser relevante para un determinado ámbito material, porque de lo contrario se estaría excluyendo un bloque completo de información.*

   Del mismo modo, ***es necesaria una aplicación justificada y proporcional atendiendo a la circunstancia del caso concreto*** *y siempre que no exista un interés que justifique la publicidad o el acceso (test del interés público)."*

   Asimismo, deben tenerse en cuenta los pronunciamientos adoptados por los Tribunales de Justicia respecto de la aplicación de esos límites, entre los que destacan los siguientes:

   Sentencia nº 60/2016, de 18 de mayo de 2016, del Juzgado Central de lo Contencioso-Administrativo nº 6 de Madrid, dictada en el PO 57/2015[8]: "(…) *Este derecho solamente se*

[7] https //www.consejodetransparencia.es/ct_Home/Actividad/criterios.html
[8] https //www.consejodetransparencia.es/ct_Home/Actividad/recursos_jurisprudencia/Recursos_AGE/2015/4_RTVE_2.html

[redacted]

verá limitado en aquellos casos en que así sea necesario por la propia naturaleza de la información –derivado de lo dispuesto en la Constitución Española– o por su entrada en conflicto con otros intereses protegidos. En todo caso, los límites previstos se aplicarán atendiendo a un test de daño (del interés que se salvaguarda con el límite) y de interés público en la divulgación (que en el caso concreto no prevalezca el interés público en la divulgación de la información) y de forma proporcionada y limitada por su objeto y finalidad". "*La ley consagra la* ***prevalencia del derecho subjetivo a obtener la información y correlativamente el deber de entregarla****, salvo que concurran causas justificadas que limiten tal derecho, a las que se refiere el art. 14. Tales causas constituyen conceptos jurídicos indeterminados cuya relevancia y trascendencia deben ser concretadas en cada caso, ponderando los intereses en conflicto, como la norma indica, de tal modo que frente a los actos típicamente discrecionales*, (…).

En la Sentencia de 7 de noviembre de 2016, dictada en el Recurso de Apelación presentado frente a la Sentencia de instancia indicada previamente, la Audiencia Nacional expresamente señaló que "***Y si concurre alguno de los límites del art. 14 reseñado deberá de acreditarlo"***

Sentencia nº 46/2019, de 22 de junio de 2019, del Juzgado Central de lo Contencioso-Administrativo nº 2 de Madrid, dictada en el PO 38/2016[9]: "*El derecho de acceso a la información es un derecho fundamental reconocido a nivel internacional como tal, debido a la naturaleza representativa de los gobiernos democráticos; es un derecho esencial para promover la transparencia de las instituciones públicas y para fomentar la participación ciudadana en la toma de decisiones. "*

Sentencia nº 98/2017, de 22 de junio de 2017, del Juzgado Central de lo Contencioso-Administrativo nº 11 de Madrid, dictada en el PO 49/2016[10]: "*La ley consagra pues la prevalencia del derecho subjetivo a obtener la información y correlativamente el deber de entregarla, salvo que concurran causas justificadas que limiten tal derecho, a las que se refiere el art. 14, causas que constituyen conceptos jurídicos indeterminados cuya relevancia y trascendencia han de ser concretadas en cada caso, ponderando los intereses en conflicto (…)".*

5. Dicho esto, debemos partir del hecho, como explica la Administración, de que *la información solicitada se refiere a la aplicación SiViEs, Sistema de Vigilancia de España, responsable de recoger datos epidemiológicos de las enfermedades de declaración obligatoria, tales como*

[9] https://www.consejodetransparencia.es/ct_Home/Actividad/recursos_jurisprudencia/Recursos_AGE/2018/100_MInterior_7.html
[10] https //www consejodetransparencia.es/ct_Home/Actividad/recursos_jurisprudencia/Recursos_AGE/2016/18_MFomento_1_Renfe1_pliegos.html

[redacted]

cólera, VIH SIDA, lepra, hepatitis, otras y, recientemente, COVID 19, asimismo recoge los datos de brotes y las alertas sanitarias; recientemente, la alerta producida por la expansión de la enfermedad COVID19.

Por tanto, como indica también la Administración *toda la información incluida en SIVIEs es altamente sensible, tanto desde el punto de vista de la salvaguarda sanitaria como desde la protección de los datos personales incorporados a la aplicación informática*.

Recordemos que la red nacional de vigilancia epidemiológica (RENAVE) se crea *con el objeto de permitir la recogida y el análisis de la información epidemiológica con la finalidad de poder detectar problemas, valorar los cambios en el tiempo y en el espacio, contribuir a la aplicación de medidas de control individual y colectivo de los problemas que supongan un riesgo para la salud de incidencia e interés nacional o internacional y difundir la información a sus niveles operativos competentes, así como,* para que, *mediante la vigilancia epidemiológica, las Administraciones sanitarias dispongan de la información necesaria para la toma de decisiones*.

Teniendo en cuenta lo anterior, a juicio de este Consejo de Transparencia y Buen Gobierno, como alega la Administración, *la aplicación SIVIEs podría considerarse una infraestructura estratégica a los efectos de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, que en su artículo 2.d) define a estas como "las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales*".

Como ya se ha expuesto, sobre SIVIEs descansa una parte importante del control de la pandemia provocada por la enfermedad COVID19, así queda establecido en la Orden SND/404/2020, de 11 de mayo, de medidas de vigilancia epidemiológica de la infección por SARS-CoV-2 durante la fase de transición hacia una nueva normalidad, por tanto se trata de un sistema sobre el que descansa el funcionamiento de un servicio esencial.

Por lo que, facilitar la documentación del (i) *software del sistema SiViEs (por ejemplo, los desarrolladores, sobre las pruebas del software -pruebas unitarias-, registro de actualizaciones del software, documentación del diseño y arquitectura del sistema, documentación del código fuente*), de (ii) *la estructura de la base de datos*, y (iii) *el detalle de con qué software está creado SiViEs y con cuál software y sistema de gestión de base de datos se gestiona* podría vulnerar la protección, obligatoria, de la aplicación SIVIEs.

Aunque se partiera del hecho que apunta el reclamante en relación a que *la estructura interna del sistema que se ha solicitado para saber cómo se almacena y procesa la*

[redacted]

información no deja al aire vulnerabilidades, o a que, que *la gente pueda conocer como está estructurada o formada tampoco les permitiría acceder a ella,* entiende este Consejo de Transparencia y Buen Gobierno que sí puede facilitar el poder vulnerar la aplicación y los datos sensibles que guarda, en definitiva, facilitaría poder "atacar" la aplicación.

Aunque, como indica el reclamante, no se están solicitando los datos de carácter personal especialmente protegidos que se contienen en la base de datos - *cólera, VIH SIDA, lepra, hepatitis, otras y, recientemente, COVID 19-*, facilitar la información y documentación técnica que se reclama pondría en peligro la protección de estos datos. Como señala el mencionado Criterio supondría un perjuicio (test del daño) concreto, definido y evaluable, no hipotético, sin que exista un interés superior que lo justifique.

Hay que recordar en este punto, que a la vista de la reclamación la Administración aclara que la *app Radar COVID no recoge ningún dato personal ni de geolocalización, por tanto, el acceso a la misma no podrá permitir la vulneración de derechos personales, ni de datos sanitarios protegidos legalmente*.

A ello, cabe añadir, que no solo se pondría en peligro la protección de los citados datos sino también la finalidad con la que recogen los datos de *poder detectar problemas, valorar los cambios en el tiempo y en el espacio, contribuir a la aplicación de medidas de control individual y colectivo de los problemas que supongan un riesgo para la salud de incidencia e interés nacional o internacional y difundir la información a sus niveles operativos competentes, así como, para que, mediante la vigilancia epidemiológica, las Administraciones sanitarias dispongan de la información necesaria para la toma de decisiones.*

En este sentido, consideramos que el perjuicio al límite previsto en el artículo 14.1 k) de la LTAIBG, alegado por la Administración, así como el perjuicio para la seguridad pública y a la protección de datos, es real y no meramente hipotético sin que, a nuestro juicio, haya sido aportado al expediente justificación de la existencia de un interés superior que permita desplazar la aplicación del límite aludido.

En consecuencia, entendemos que la presente reclamación ha de ser desestimada.

III. RESOLUCIÓN

En atención a los Antecedentes y Fundamentos Jurídicos descritos, procede **DESESTIMAR** la reclamación presentada por [redacted], con entrada el 19 de noviembre de 2020, contra la resolución de 16 de noviembre de 2020 del MINISTERIO DE CIENCIA E INNOVACIÓN.

[redacted]

De acuerdo con el artículo 23, número 1[11], de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno, la Reclamación prevista en el artículo 24 de la misma tiene la consideración de sustitutiva de los recursos administrativos, de conformidad con lo dispuesto en el artículo 112.2 de la Ley 39/2015, de 1 de octubre[12], de Procedimiento Administrativo Común de las Administraciones Públicas.

Contra la presente Resolución, que pone fin a la vía administrativa, se podrá interponer Recurso Contencioso-Administrativo, en el plazo de dos meses, ante los Juzgados Centrales de lo Contencioso-Administrativo de Madrid, de conformidad con lo previsto en el artículo 9.1 c) de la Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso-Administrativa[13].

EL PRESIDENTE DEL CTBG

Fdo: José Luis Rodríguez Álvarez

[11] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&tn=1&p=20181206#a23
[12] https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565&p=20151002&tn=1#a112
[13] https://www.boe.es/buscar/act.php?id=BOE-A-1998-16718&tn=1&p=20181206#a9

[redacted]