- **Expediente N.º: PS/00222/2021**

- RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos (en lo sucesivo, AEPD) y en base a los siguientes

ANTECEDENTES

PRIMERO: Con fecha 21 de mayo de 2020 la directora de la AEPD, siguiendo el mismo criterio utilizado ante cualquier noticia publicada en los medios de comunicación que afectase al tratamiento de datos de salud por parte de las Administraciones Públicas, y, ante las noticias aparecidas en medios de comunicación relativas al proyecto del Gobierno de España acerca de la implantación de una aplicación (o App) de rastreo de posibles infectados de COVID-19, encargado a la SECRETARIA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL (en lo sucesivo, la SEDIA), del MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL (en adelante, el METD), que usará una interfaz de programación de aplicaciones (en adelante, API) de Google y Apple, un protocolo para ser interoperable entre países, que se lanzará como piloto en Canarias a comienzos de junio, conectándose a los sistemas informáticos sanitarios de las Comunidades Autónomas, insta a la Subdirección General de Inspección de Datos (en lo sucesivo, SGID) a que inicie las actuaciones previas de investigación a las que se refiere el artículo 67 de la Ley Orgánica 3/2018, de 6 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), con relación a las actuaciones realizadas por la SEDIA, por si de tales hechos se desprendieran indicios de infracción en el ámbito competencial de la AEPD.

SEGUNDO: ***A.A.A.*** (en adelante, la parte reclamante uno) con fecha 7 de septiembre de 2020 interpone una reclamación ante la AEPD contra la SEDIA.

En particular, basa su reclamación en las siguientes circunstancias:

"1. Investigar si la aplicación RadarCovid cumple con los principios de licitud, lealtad, transparencia y responsabilidad proactiva del RGPD (Art. 5), de conformidad con las directrices del EDPB (Art. 70 RGPD), en la medida en que:

(a) SGAD no ha publicado el contenido de la EIPD, a pesar de la "encarecida" recomendación del EDPB, así como confirmar si SGAD ha elaborado la EIPD y, en su caso, planteado la Consulta previa a la AEPD antes de efectuar el tratamiento de datos personales (Art. 35 y 36 RGPD);

(b) SGAD no ha publicado el código fuente, tal y como requiere el EDPB en sus directrices;

(c) SGAD no ha definido en la Política de privacidad las funciones y responsabilidades de las autoridades sanitarias de las CC.AA. que han completado los procesos técnicos necesarios para integrar la aplicación en sus sistemas sanitarios (Art. 13 y 14 RGPD);

(d) SGAD no ha especificado de forma suficientemente clara las distintas finali-

dades del tratamiento y sus respectivas bases legitimadoras, en atención a lo dispuesto en el apartado "5. ¿Para qué y por qué utilizamos tus datos?" y "10. ¿Cuál es la legitimación para el tratamiento de tus datos?" de la Política de privacidad (Art. 13 y 14 RGPD); y

(e) SGAD no ha especificado los plazos de conservación de los datos para fines de investigación científica o histórica o fines estadísticos en la Política de privacidad (Art. 9.2j y 89.1 RGPD).

2. Ordenar a SGAD que las operaciones de tratamiento en el marco de Radar-Covid se ajusten al RGPD y las directrices del EDPB; y

3. Sancionar a SGAD con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el RGPD o las directrices del EDPB."

Sobre dicha reclamación recayó resolución de ADMISIÓN A TRÁMITE de fecha 5 de octubre de 2020, en el expediente con núm. de referencia E/07823/2020.

Con fecha 24 de enero de 2021, la parte reclamante uno, amplía su reclamación y traslada a la AEPD unas alegaciones complementarias basadas en las siguientes circunstancias:

"1. Incorporar dichas ALEGACIONES COMPLEMENTARIAS a la investigación que está llevando a cabo la AEPD por una posible vulneración de la normativa en materia de protección de datos;

PRIMERO: Publicación tardía e incompleta del código fuente
SEGUNDO: Modificación del responsable del tratamiento
TERCERO: Brecha de seguridad
CUARTO: Comunicaciones de datos al "EU interoperability gateway"
QUINTO. Modificación de la Política de Privacidad de RadarCOVID

2. Hacer extensiva la reclamación a los nuevos responsables del tratamiento de la aplicación RadarCOVID identificados en la misma (i.e. Ministerio de Sanidad y Consejerías de Sanidad de las correspondientes Comunidades y Ciudades Autonómicas) por ostentar éstos la legitimación pasiva en el presente procedimiento;

3. En su caso, ordenar a los responsables o encargados del tratamiento de RadarCOVID que las operaciones de tratamiento se ajusten a las disposiciones del RGPD, cuando proceda, de una determinada manera y dentro de un plazo especificado, de conformidad con las expresas directrices e interpretaciones efectuadas por el EDPB sobre la materia; y

4. En su caso, sancionar a todo responsable o encargado del tratamiento de RadarCOVID con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el RGPD, de conformidad con las expresas directrices e interpretaciones efectuadas por el EDPB sobre la materia."

TERCERO: ***B.B.B.*** junto a diez profesores más (en adelante, la parte reclamante dos), con fecha 1 de octubre de 2020, interpone una reclamación ante la AEPD, con el siguiente tenor:

"Por la presente le informamos de una brecha de seguridad en la App Radar COVID, reportada a la SEDIA e Indra S.A, el 16 de septiembre del 2020. Le adjuntamos el reporte técnico así como la valoración jurídica en la nota legal que enviamos a la Vicepresidenta Nadia Calviño y a la Secretaria de Estado Carme Artigas este lunes 28 de septiembre".

Sobre dicha reclamación recayó resolución de ADMISIÓN A TRÁMITE de fecha 5 de octubre de 2020, en el expediente con núm. de referencia E/07905/2020.

CUARTO: ***C.C.C.*** (en adelante, la parte reclamante tres) con fecha 5 de octubre de 2020, interpone una reclamación ante la AEPD.

En particular, informa de cómo una decisión de diseño en la aplicación de rastreo de contactos Radar COVID pone en riesgo la privacidad de sus usuarios.

*"En concreto, el riesgo proviene de que solo los usuarios positivos de COVID suben las claves TEK (claves con el resultado de un test) al servidor de radar-covid-backend-dp3t-server (https://radarcovid.covid19.gob.es , con IP ***IP.1, ***IP.2, ***IP.3, ***IP.4 accesible a través de CloudFront CDN). Por lo tanto, cada vez que se observa una subida de la clave desde un teléfono al endpoint ' /v1/gaen/expuesto ' de este servidor, se puede inferir que el propietario del teléfono es COVID-positivo. La encriptación entre la aplicación y el servidor no ayuda a encubrir esa información: incluso si el endpoint y el contenido de la subida no son observables, la longitud de los mensajes revelará una subida de la clave TEK al servidor."*

Sobre dicha reclamación recayó resolución de ADMISIÓN A TRÁMITE de fecha 16 de octubre de 2020, en el expediente con núm. de referencia E/08295/2020.

QUINTO: RIGHTS INTERNATIONAL SPAIN (en adelante, la parte reclamante cuatro) con fecha 26 de febrero de 2021 interpone una reclamación ante la AEPD.

En particular, basa su reclamación en las siguientes circunstancias:

"- Tras tener conocimiento de la tramitación, por parte de esta Agencia, de un procedimiento de oficio que investiga la aplicación de rastreo de contactos Radar COVID, y habiendo detectado una serie de potenciales riesgos para la privacidad e incumplimiento de las directrices aplicables, la asociación RIGHTS INTERNATIONAL SPAIN presenta un escrito para su incorporación al procedimiento, en el cual se denuncian irregularidades con respecto a la publicación del código de la aplicación.

- En este sentido, se llama la atención sobre el hecho de que, a pesar de poder ser descargada la aplicación en diversas Comunidades Autónomas (incluso se liberó una versión para un proyecto piloto), el código no se publicó hasta el 9 de septiembre de 2020, y el mismo difería del que tuvo la aplicación en su versión inicial. Además, hasta la fecha, no se ha publicado el histórico de desarrollo de la app, es decir, el historial con todos los datos y pasos que se han dado desde el principio de su desarrollo.

- En relación con el piloto, la asociación critica que, al no encontrarse publicado el código fuente, se desconoce su alcance concreto, aunque las descargas no se encontraban geolocalizadas, y, por tanto, la app podía ser descargada e instalada

desde cualquier zona geográfica. Los índices utilizados para cuantificar el éxito de la acción iban más allá del territorio delimitado para las pruebas, pudiendo afectar a usuarios no informados o conscientes del uso de información de sus terminales

- La asociación considera que la mencionada ausencia de transparencia provocó un retraso en la detección de una brecha de datos personales en la app, ya que, como luego se descubrió, únicamente enviaba información al servidor en caso de detectar un positivo.

- Finalmente, la asociación llama la atención sobre algunas deficiencias relativas al documento de Evaluación de Impacto, el cual se publicó recientemente, en enero de 2021, a pesar de que la aplicación estuvo disponible ya en junio de 2020. Según su control de cambios, la versión publicada es la de noviembre de 2020, no indicando nada al respecto de las versiones anteriores, los cambios realizados, y los riesgos que puedan haber sido detectados con posterioridad a la evaluación inicial. Cuestionan la utilidad de una evaluación de impacto presentada y elaborada de esta manera."

Sobre dicha reclamación recayó resolución de ADMISIÓN A TRÁMITE de fecha 12 de marzo de 2021, en el expediente con núm. de referencia E/02649/2021.

SEXTO: En el marco de las actuaciones previas de investigación se practicaron cinco requerimientos de información dirigidos a la SEDIA, en distintas fechas:

Requerimiento	Código Seguro de Verificación	Fecha requerimiento	Fecha notificación requerimiento
Primero	***CSV.1**	26/05/2020	07/06/2020
Segundo	***CSV.2**	18/08/2020	29/08/2020
Tercero	***CSV.3**	18/09/2020	29/09/2020
Cuarto	***CSV.4**	02/10/2020	13/10/2020
Quinto	***CSV.5**	26/10/2020	06/11/2020

En el primer requerimiento, de fecha 26 de mayo de 2020, se solicitaba la siguiente información:

(…)

Respecto a los tratamientos

1.- Información sobre las finalidades concretas de la app y de los tratamientos de datos personales previstos en el marco de la citada app.

2.- Información sobre las tipologías de datos personales que pudieran ser recabados de los usuarios por estos tratamientos, especificando concretamente los datos de salud, datos de ubicación e identificativos, en cuestión. Indicar el carácter obligatorio o voluntario de facilitarlos. Periodo de conservación previsto para cada uno de los datos o tipos de datos anteriormente citados.

3.- Sobre los datos de ubicación que se recaben, información sobre los trata-

mientos posteriores previstos con dichos datos y sus finalidades. Adicionalmente, información sobre los procesos de anonimización y/o seudonimización aplicados.

4.- Detalle de la previsión de uso de la app en términos de obligatoriedad y de alcance:

4.1.- Información sobre la obligatoriedad de uso de la App.

4.2.- Información sobre la compatibilidad de la App con las distintas versiones de los sistemas operativos (ANDROID e IOS).

4.3.- Soluciones contempladas para los usuarios de sistemas incompatibles y otros sistemas operativos (Windows Mobile, etc…).

4.4.- Medidas previstas para su utilización por parte de menores de edad y garantías.

5.- Terceras entidades previstas intervinientes en los tratamientos, públicas y privadas. Identificación de éstas y copia de los contratos/acuerdos suscritos por la SEDIA y las sucesivas subcontrataciones.

6.- Información sobre las cesiones previstas e identificación de las categorías de destinatarios y marco legitimador en el que se van a realizar

7.- Información sobre el cumplimiento de los principios de protección de datos, principalmente del principio de proporcionalidad, limitación de finalidad, así como del de minimización de los datos recabados, según las finalidades previstas. Copia de los informes que reflejen los estudios realizados en su caso.

Respecto al almacenamiento y seguridad de los datos

8.- Descripción de las bases de datos o ficheros que intervienen en el proceso, tanto en los terminales móviles como en los servicios centrales y comunidades autónomas.

Estructura de registro y descripción de los contenidos. Descripción de los metadatos, IP, puerto, IMEI, Identificación del dispositivo, etc… así como la finalidad para la que se hace uso de estos datos.

Información sobre si los datos relativos a las pruebas diagnósticas son incluidos en estas bases de datos y son asociados a los usuarios de las aplicaciones.

Información sobre la localización de los servidores de recogida de información y las entidades a cargo de la gestión de dichos servidores.

9.- Copia del análisis de riesgos sobre los derechos y libertades de los usuarios de la app realizado sobre el posible tratamiento de datos y la evaluación de impacto relativa a protección de datos a realizar sobre esta iniciativa.

10.- Descripción de las medidas técnicas y organizativas implementadas que garanticen la seguridad de los datos personales, tanto de la parte cliente descargada por los usuarios como de la información tratada en la parte del servidor, incluyendo, al menos, la gestión de usuarios, control de acceso, ficheros de registro de acceso (logs), copia de seguridad y procedimiento de gestión de brechas de seguridad. Información sobre si los datos se almacenan cifrados y, en su caso, tipo de cifrado.

11.- Copia del análisis y gestión de riesgos de seguridad en el contexto del

Esquema Nacional de Seguridad.

Respecto a la App y APIs de Google y Apple

12.- Copia de la Política de Privacidad de la app. Copia de cualquier otra evaluación de los tratamientos de datos previstos en la app realizada por su parte hasta la fecha, si la hubiere. 12.- Fecha de puesta en funcionamiento prevista para la mencionada app.

13.- Copia de la documentación técnica tanto de la app como de las APIs utilizadas en el desarrollo de ésta que incluya información sobre la estructura de datos y procesos.

14.- Información sobre si dicha aplicación y las interfaces (API) son de código abierto y si dichas APIs han sido sometidas a una auditoría por una tercera entidad independiente nacional o internacional y resultado de ella.

15.- Información sobre los recursos de los dispositivos móviles a los que accede la app y la finalidad de cada acceso. Información que se facilita al usuario sobre estos accesos.

16.- Información sobre los recursos de los dispositivos móviles a los que acceden las APIs y la finalidad de cada acceso. Información que se facilita al usuario sobre estos accesos.

17.- Descripción del procedimiento de rastreo y alerta incluyendo:

- Descripción del procedimiento de rastreo. Procedimiento de generación de identificadores, frecuencia de cambio, ubicaciones en las que se almacenan y periodo de conservación de estos en cada ubicación.

- Descripción detallada del procedimiento de comunicación a los usuarios que han estado próximos a un usuario al que se ha constatado la infección, detallando la información que se le comunica.

- Autoridades y/o terceros a los que se facilitan los identificadores.

- Descripción del procedimiento mediante el que se comunica un positivo contagiado de COVID-19. Quién lo introduce en el circuito. Descripción del procedimiento que garantiza que es un positivo constatado por las autoridades sanitarias y no un falso positivo.

Respecto a las transmisiones de datos

18.- Descripción de las transmisiones de datos especificando las redes, protocolos y cifrado.

19.- Descripción de las tramas de datos que se transmiten, estructura y contenido. Descripción de los metadatos, IP, puerto, IMEI, Identificación del dispositivo, ubicación, etc… así como la finalidad para la que se hace uso de estos datos y cuáles de ellos son registrados en los ficheros.

La suspensión de plazos administrativos prevista en la Disposición adicional tercera del Real Decreto 463/2020, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19, en su apartado 4 establece: "Sin perjuicio de lo dispuesto en los apartados anteriores, desde la entrada en vigor del presente real decreto, las entidades del sector público podrán acordar motivadamente la continuación de aquellos

procedimientos administrativos que vengan referidos a situaciones estrechamente vinculadas a los hechos justificativos del estado de alarma, o que sean indispensables para la protección del interés general o para el funcionamiento básico de los servicios".

Atendiendo a la naturaleza especialmente sensible de los datos en cuestión, esta Agencia considera que se trata de un supuesto de urgencia inaplazable, en el que resulta necesario salvaguardar el derecho fundamental a la protección de los datos personales, por lo que se desvirtuaría su carácter urgente si se viera afectado por la suspensión de plazos decretada (…).

En el segundo requerimiento, de fecha 18 de agosto de 2020, se solicitaba la siguiente información:

(…)

1.- Actualización de la información y documentación aportada relativa al sistema RADAR COVID que pudiera haber cambiado con respecto a la versión piloto.

2.- Copia de los contratos de servicios que presta Amazon Web Services (AWS).

3.- Información sobre el rol que desempeña la Secretaría de Estado de Digitalización e Inteligencia Artificial, así como el Ministerio de Sanidad en la gestión del sistema RADAR COVID, y en su caso, copia de los contratos o convenios suscritos entre ambos.

4.- Respecto a los tratamientos realizados por la Comunidades Autónomas:

• Información sobre el rol que desempeñan las Comunidades Autónomas en la gestión del sistema RADAR COVID, y en su caso, copia de los contratos o convenios suscritos.

• Descripción de los tratamientos que realizan.

• Descripción detallada del procedimiento establecido para la comunicación de los identificadores positivos de COVID 19. Copia de los protocolos y documentación al respecto.

• Descripción del sistema de información utilizado por las CCAA para la gestión de los códigos de diagnóstico.

• Descripción de las medidas de seguridad de este sistema, incluyendo la gestión de usuarios y contraseñas (procedimiento de altas y bajas) y tipo de cifrado de las comunicaciones.

5.- Respecto al almacenamiento y seguridad de los datos

5.1.-Descripción de las bases de datos del back-end:

Estructura de la base de datos, descripción de las tablas y de cada uno de los campos.

Copia impresa de un registro completo de cada tabla incluyendo la descripción de los contenidos de los campos.

Información sobre si los datos se almacenan cifrados y, en su caso, tipo de cifrado.

5.2.- Copia del análisis de riesgos sobre los derechos y libertades de los usuarios de la app realizado sobre los posibles tratamientos de datos de carácter personal y la evaluación de impacto relativa a protección de datos a realizar sobre esta iniciativa.

5.3.- Descripción de las medidas técnicas y organizativas implementadas que garanticen la seguridad de los datos personales, incluyendo la gestión de usuarios, control de acceso, ficheros de registro de acceso (logs), copia de seguridad y procedimiento de gestión de brechas de seguridad.

5.4- Copia del análisis y gestión de riesgos de seguridad en el contexto del Esquema Nacional de Seguridad.

6.- Descripción del procedimiento de interoperabilidad con otras Apps desarrolladas con la misma finalidad por terceros países.

6.1.- Datos que se comparten o se tienen previsto compartir de los usuarios.

6.2.- Descripción del procedimiento establecido para compartir dichos datos.

6.3.- Descripción del procedimiento de recopilación de datos de identificadores de usuarios de otras Apps.

6.4.- Descripción del procedimiento de comunicación a usuarios de otras Apps de que han estado en contacto con usuarios positivos. (…)

En el tercer requerimiento, de fecha 18 de septiembre de 2020, se solicitaba la siguiente información:

(…)

1.- Finalidades para las que se utilizan librerías de software Firebase de Google tras concluir la fase piloto, y en particular las que utilizan el servicio Google analytics, según se desprende del código de la app recientemente hecho público en hithub.com (En las líneas 198-199:// Recommended: Add the Firebase SDK for Google Analytics. implementation 'com.google.firebase:firebase-analytics-ktx:17.5.0').(…)

En el cuarto requerimiento, de fecha 2 de octubre de 2020, se solicitaba la siguiente información:

Ha tenido entrada en esta Agencia un escrito en el que se reporta una incidencia de seguridad detectada en relación con la app Radar COVID que se expone literalmente:

"*sólo los usuarios positivos de COVID suben las claves TEK (claves con el resultado de un test) al servidor de radar-covid-backend-dp3t-server, https:// radarcovid.covid19.gob.es/ (con IP: ***IP.1, ***IP.2, ***IP.3, ***IP.4 accesible a través de CloudFront CDN). Por lo tanto, cada vez que se observa una subida de la clave desde un teléfono al endpoint de este servidor '/v1/gaen/expuesto', se puede inferir que el propietario del teléfono es COVIDpositivo. La encriptación entre la aplicación y el servidor no ayuda a encubrir esa información: incluso si el endpoint y el contenido de la subida no son observables, la longitud de los mensajes revelará una subida de la clave TEK al servidor.*

La comunicación puede ser observada por diversas entidades. Por ejemplo,

el proveedor de telecomunicaciones (si la conexión se hace a través de GSM); el proveedor de servicios de Internet si la conexión se hace a través de Internet; o cualquier persona con acceso a la misma red (WiFi o Ethernet) que el usuario. En el caso de la appRadar COVID, en la que las subidas se hacen utilizando el endpoint de Cloudfront que se utiliza para la descarga de las claves TEKs, Amazon también tiene la capacidad de observar las direcciones IP de los usuarios de Radar COVID y asociarlas al hecho de que esos usuarios comunican un test de COVID positivo.

Las direcciones IP observables constituyen datos personales ya que "contienen información concerniente a personas físicas 'identificadas o identificables'" (ya lo entendió así la Sentencia de la Sala Tercera del Tribunal Supremo, Secc. 6, de 23 de Octubre 2014, ECLI: ES:TS:2014:3896, interpretando la antigua LOPD). Pero, además del hecho de comunicar la dirección IP, habida cuenta de que, como se muestra en el informe técnico, sólo los usuarios positivos de COVID suben las claves al servidor de radar-covid-backend-dp3t-server, esa IP queda asociada a los datos de claves TEK subidos, que corresponden siempre a la comunicación de un test positivo de COVID.

De este modo, el funcionamiento de la app permite vincular de modo inequívoco una IP con el hecho de que su titular está subiendo un test positivo de COVID. Así pues, sin que el usuario sea consciente de ello, la app hace posible que terceros conozcan que el titular de una IP está infectado por el virus, lo que implica la comunicación de un dato sensible, al tratarse de un dato de salud (dato especialmente protegido conforme al art. 9 RGPD). Mientras que el tratamiento de la dirección IP es necesario para el funcionamiento de la aplicación, la posibilidad de asociar la IP con la subida de un test positivo no lo es."

En uso de las facultades conferidas por el artículo 58.1 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 (en adelante, RGPD), y el Art. 67 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se solicita que en el plazo de diez días hábiles, nos informen si tienen cocimiento de este hecho y, en su caso, las medidas adoptadas para su resolución.

En el quinto y último requerimiento, de fecha 26 de octubre de 2020, se solicitaba la siguiente información:

(…)

1.- Número de identificadores que se han visto afectados por la vulnerabilidad.

2. Descripción detallada de las acciones realizadas para su resolución incluyendo fecha de las medidas adoptadas y fecha de su implantación.

3.- Información respecto de si tiene conocimiento de la utilización por terceros de los datos expuestos.

4.- Protocolo de comunicaciones utilizado entre la app y el backend y descripción detallada del tipo de cifrado utilizado. (…)

SÉPTIMO: A la vista de las alegaciones aportadas por la SEDIA en respuesta a los requerimientos practicados, la SGID emitió un informe de actuaciones previas de investigación en el marco del expediente con número de referencia E/03936/2020, de fecha 26 de febrero de 2021, en virtud de los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el artículo 67 de la LOPDGDD, con el siguiente tenor:

"**ANTECEDENTES**

Con fecha de 21 de mayo de 2020 la Directora de la Agencia Española de Protección de Datos acuerda iniciar las presentes actuaciones de investigación en relación con las noticias aparecidas en medios de comunicación sobre el proyecto del Gobierno de implantación de una app de rastreo por bluetooth de posibles infectados de COVID-19.

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se han realizado investigaciones a las siguientes entidades:

Ministerio de Asuntos Económicos y Transformación Digital - SEDIA- Secretaría de Estado de Digitalización e Inteligencia Artificial- con NIF S2833002E con domicilio en Calle Poeta Joan Maragall 41 - 28071 Madrid.

Ministerio de Sanidad -SGSDII- Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud con domicilio en PASEO DEL PRADO, 18-20 - 28071 Madrid.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Con fechas de 26/5, 17/8, 18/9, 2/10 y 26/10 de 2020, se notificó por la Inspección de Datos sendos requerimientos de información a la Secretaría de Estado de Digitalización e Inteligencia Artificial solicitando diversa información y documentación en relación con la aplicación móvil (app) que permitirá el rastreo de contactos por Bluetooth con objeto de la detección precoz de posibles contagiados por la COVID-19 (RADAR COVID). Con fechas 5/6, 18/6, 3/7, 21/7, 28/7, 1/9, 22/9, 23/9, 9/10, 15/10, 27/10, 30/10 y 5/11 de 2020 se recibieron respectivos escritos de respuesta completando los requerimientos de información efectuados.

De la información y documentación aportada se desprende lo siguiente:

1.1.- Con fecha 9 de octubre de 2020 se firmó el "*Acuerdo entre el Ministerio de Asuntos Económicos y Transformación Digital (Secretaría de Estado de Digitalización e Inteligencia Artificial) y el Ministerio de Sanidad acerca de la aplicación "RADAR COVID".*", cuyo objeto es:

a) Delegar en la Secretaría General de Administración Digital (en adelante, SGAD) del Ministerio de Asuntos Económicos y Transformación Digital, todas las competencias de diseño, desarrollo, implantación y evolución de la aplicación "RADAR COVID" que correspondan a la Dirección General de Salud Digital y Sistemas de Información para el Sistema Nacional de Salud en virtud de lo previsto en el artículo 8.2.a) del Real Decreto 735/2020, de

4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio de Sanidad, la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud. La Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud ha aprobado previamente la delegación de todas estas competencias en la SGAD de acuerdo con lo previsto en el artículo 9.1 de la Ley 40/2015, de 1 de octubre.

b) Delegar en la SGAD la competencia del Ministro de Sanidad para suscribir con las comunidades y ciudades autónomas los convenios de colaboración para la adhesión de estas al uso de la aplicación "RADAR COVID", de acuerdo con lo previsto en el Capítulo VI del Título Preliminar de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. sin perjuicio del apoyo que para facilitar su tramitación le prestará la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud.

La parte expositiva del Convenio recoge en el sexto punto lo siguiente:

"Sexto.- Que, desde el mes de mayo de 2020, la SGAD ha venido desarrollando, con el conocimiento y la conformidad del Ministerio de Sanidad, una aplicación para la trazabilidad de contactos en relación con la pandemia ocasionada por la COVID-19 denominada "RADAR COVID". Durante el mes de julio de 2020, con la conformidad de la Dirección General de Salud Pública, Calidad e Innovación del Ministerio de Sanidad, la SGAD llevó a cabo con éxito el proyecto piloto de la misma, cuyo éxito garantiza la viabilidad de la solución propuesta para el rastreo de contactos estrechos."

1.2 El representante de la SGAD manifiesta, en escrito de fecha 1/9/2020, respecto al sistema RADAR COVID que el Ministerio de Sanidad tiene la condición de responsable del tratamiento, y cada Comunidad Autónoma será responsable de tratamiento de los datos de su ámbito respectivo, mientras que la Secretaría General de Administración Digital (Secretaría de Estado de Digitalización e Inteligencia Artificial) tiene la condición de encargado del tratamiento.

1.3.- El sistema "RADAR COVID" lo constituye:

- Una app para dispositivos móviles denominada "RADAR COVID" que recoge identificadores de proximidad de usuarios de esta y utiliza la interfaz de programación de aplicaciones (API) desarrollada por Google y Apple.
- Un servicio Web que se pone a disposición de los gobiernos de las Comunidades Autónomas (CCAA) para distribuir los códigos que permiten a los usuarios de la app que han dado positivo en un test COVID-19, enviar los identificadores de proximidad de los últimos 14 días conservados en el terminal móvil al servidor.
- Además, los servicios de salud de las CCAA han de establecer los procesos y procedimientos necesarios para facilitar a los usuarios que han dado positivo en la prueba de COVID-19 un código de seguridad que es la llave para subir al servidor los identificadores de proximidad que conservan en los dispositivos móviles.

Las dos primeras han sido desarrolladas por el Gobierno de España con la finalidad de ayudar a evitar la propagación de la COVID-19 identificando los po-

sibles contactos que una persona que resulte infectada haya podido tener en los últimos 14 días y la tercera es responsabilidad del Servicio de Salud de cada CCAA.

1.4.- Con fecha 15 de junio de 2020 se acordó por el Secretario General de la Administración Digital la contratación de los servicios para la trazabilidad de contactos con relación a la pandemia ocasionada por la COVID 19 a Indra Tecnologías de la Información S.L. (en adelante INDRA). Según consta en el objeto del contrato recogido en el "Pliego de condiciones para el diseño, desarrollo, piloto y evaluación de un sistema que permita el rastreo de contactos en relación con la pandemia ocasionada por la covid-19" de fecha 12 de junio de 2020, el proyecto de implantación tendría tres fases: fase pre-piloto, fase piloto y fase post-piloto.

1.5.- El Gobierno lanzó el proyecto piloto el 29 de junio y finalizó el 29 de julio de 2020 en la isla de La Gomera en coordinación con el Gobierno de Canarias, con el Gobierno del Cabildo de La Gomera y con el Ayuntamiento de San Sebastián de La Gomera, así como con el Servicio Canario de la Salud.

Posteriormente se han ido incorporando al proyecto las Comunidades Autónomas en fase de pruebas hasta la firma del convenio a suscribir con cada una de ellas, en las siguientes fechas: Andalucía, Aragón, Cantabria y Extremadura el 19 de agosto, Canarias y Castilla y León el 20 de agosto, Baleares el 24 de agosto, Murcia el 25 de agosto, Madrid y Navarra el 1 de septiembre, La Rioja el 3 de septiembre, Asturias el 4 de septiembre, Com. Valenciana el 8 de septiembre, Melilla y Galicia el 14 de septiembre, Castilla-la Mancha el 18 de septiembre, País Vasco el 21 de septiembre, Ceuta el 24 de septiembre de 2020.

La implantación y utilización en pruebas en todo el territorio nacional de la aplicación está amparada por un Acuerdo del Consejo interterritorial del Sistema Nacional de Salud adoptado en fecha 19 de agosto de 2020, con la secuencia temporal que acuerden con la SEDIA.

Respecto de los principios de proporcionalidad, limitación de finalidad, así como de minimización de los datos recabados según las finalidades previstas.

1.6.- Manifiestan que la principal finalidad de la aplicación es permitir alertar a las personas que han estado en contacto con alguien infectado por la COVID-19 e informarles de las medidas que conviene adoptar después, como someterse a auto cuarentena o a pruebas diagnósticas, o proporcionar asesoramiento sobre qué hacer en caso de experimentar algún síntoma. Esto es, pues, útil tanto para los ciudadanos como para las autoridades sanitarias públicas. También puede desempeñar un papel importante en la gestión de las medidas de confinamiento durante las posibles situaciones de desescalada.

1.7.- Manifiestan que se recaban exclusivamente los datos que se requieren para las finalidades indicadas.

No se lleva a cabo el almacenamiento ni el momento exacto ni el lugar de contacto, sin embargo, consideran útil almacenar el día del contacto para saber si se produjo cuando la persona experimentaba síntomas (o cuarenta y ocho horas antes) y definir con mayor precisión el mensaje de seguimiento en el que se ofrezcan consejos relacionados, por ejemplo, con la duración de la auto

cuarentena.

1.8.- Respecto a si la medida es necesaria, en el sentido de que no exista otra más moderada para la consecución de tal propósito con igual eficacia, manifiestan:

"Es muy importante considerar la utilidad real, la necesidad y efectividad de esta Aplicación, así como su impacto en el sistema social más amplio, incluidos los derechos fundamentales y libertades, considerando que estas aplicaciones sientan un precedente para el uso futuro de tecnologías invasivas similares, incluso después de la crisis COVID-19.

La situación de emergencia no puede suponer una suspensión del derecho fundamental a la protección de datos personales. Pero, al mismo tiempo, la normativa de protección de datos no puede utilizarse para obstaculizar o limitar la efectividad de las medidas que adopten las autoridades competentes, especialmente las sanitarias, en la lucha contra la epidemia, ya que en ella se prevén soluciones que permiten compatibilizar el uso lícito de los datos personales con las medidas necesarias para garantizar eficazmente el bien común.

Los fundamentos que legitiman/hacen posible dichos tratamientos son la necesidad de atender las misiones realizadas en interés público, así como la de garantizar los intereses vitales de los propios afectados o de terceras personas, en virtud de lo expuesto en el Considerando 46 del RGPD, donde se reconoce que en situaciones excepcionales, como una epidemia, la base jurídica de los tratamientos puede ser múltiple, basada tanto en el interés público, como en el interés vital del interesado u otra persona física.

El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano.

Por tanto, si procedemos a realizar un juicio de necesidad, es decir, determinar si el tratamiento es necesario, en el sentido de que no existe otra alternativa menos invasiva para la privacidad para conseguir este propósito con la misma eficacia o con una eficacia razonable, conviene apuntar que la legislación sectorial en materia sanitaria no cuenta en la actualidad con instrumentos suficientemente precisos que permitieran afrontar una situación como la de crisis sanitaria en la que el país aún se encuentra inmerso.

En este sentido, se han aprobados medidas específicas, como es el desarrollo de una aplicación como la que se está evaluando, que refuerzan los instrumentos de coordinación y cooperación en materia de salud pública a la vista de las características globales de la epidemia."

1.9.- Respecto a la proporcionalidad, añaden:

"En este caso, el beneficio tendrá que medirse en función de una menor pro-

pagación de la infección en términos globales, con la posibilidad de recuperar la libertad de acción, y una protección de la salud de los individuos. Los datos de salud tienen un alto valor, por lo que hay que prevenir que, aprovechando la incertidumbre que provoca una situación de emergencia, se produzcan abusos por parte de terceros que conduzcan a situaciones de pérdida de libertades, discriminación u otros daños en la situación personal de los ciudadanos.

Se trata por tanto de realizar una valoración de los beneficios que este tratamiento promete aportar en la lucha frente a la pandemia y de los costes en la privacidad de los individuos que pueden acarrear.

En cuanto a los posibles perjuicios o amenazas que puede suponer una aplicación como esta para la privacidad habrá que tener en cuenta cómo se ha realizado la aplicación que estamos evaluando y de cuáles son sus objetivos. Estas amenazas pueden aparecer por la urgencia en ofrecer soluciones en funcionamiento que relajen los controles y requisitos para proteger los datos de los ciudadanos. Por ejemplo, se pueden encontrar posibles amenazas a la privacidad en la implementación de esta. Por otra parte, no hay que olvidar que una app o una web es solamente un interfaz para mostrar y llevar datos a un servidor.

Las principales amenazas a la privacidad de este tipo de soluciones vienen de la realización de mapas de relaciones entre personas, reidentificación por localización implícita, de la fragilidad de los protocolos a la hora construir "tarjetas" casi anónimas, y de dispersar las señales de los contagios de forma que no se identifique en ningún caso la identidad de los contagiados. Debe tenerse en cuenta que el tratamiento de la información no solo afecta al usuario de la aplicación sino también la de todos los terceros con los que ha estado en contacto, por lo que este tratamiento ha de cumplir los principios de protección de datos.

Hay estudios sobre la robustez de los protocolos de criptografía y anonimización (ver documento anexo 12. DP3T - Data Protection and Security), y siempre existe una posibilidad de que aplicando suficiente tiempo y capacidad de cómputo puedan romperse y asociar los apodos anónimos con números de teléfono y personas. Desde el punto de vista de la privacidad, cuanto más cálculo se haga en la parte de servidor, menos control tienen los usuarios, por lo que las soluciones centralizadas siempre parecen menos respetuosas con la privacidad que las distribuidas. La posibilidad de que, debido a la acumulación de los datos de forma centralizada, se produjese un abuso en una empresa poco ética, se ampliarán los propósitos del tratamiento o se fuera víctima de un ciberataque constituye otra de las mayores amenazas de este tipo de soluciones.

En cuanto los beneficios que puede representar este tipo de tratamiento, es importante traer a colación, el análisis realizado por la propia AEPD sobre si el uso de estos datos representa en la crisis de la pandemia un beneficio importante, determinando que el éxito de este tipo de soluciones se basa en muchos factores que no dependen de la tecnología. En primer lugar, es necesaria la implicación de un elevado número de usuarios, algunos estudios hablan de al menos el 60% de una población que, teniendo en cuenta a los niños y los ancianos, suponen casi todos los usuarios de móvil. Por otro lado, depende de que se realice una declaración responsable de la situación personal de

infección, preferiblemente supervisada por un profesional para evitar estrategias de desinformación. Finalmente, es necesario disponer de acceso a test, no solo para todos los usuarios, sino para poder actualizar la información periódicamente y para que aquellos que sean notificados de haber estado en contacto con un infectado puedan realizar la prueba con prontitud.

No obstante, y siempre bajo un uso respetuoso con la privacidad de los usuarios, se pueden deducir los siguientes beneficios:

Beneficios para los interesados

.- Las personas que hayan estado muy cerca de alguien que resulte ser un portador confirmado del virus serán informadas al respecto, a fin de romper las cadenas de transmisión lo antes posible.

Asimismo, se les informará de las medidas que conviene adoptar después, como someterse a autocuarentena o a pruebas diagnósticas, o proporcionar asesoramiento sobre qué hacer en caso de experimentar tal o cual síntoma.

.- La instalación de la aplicación en el dispositivo es voluntaria, sin consecuencia negativa alguna para quien decida no descargar o no usar la aplicación.

.- El usuario mantiene el control sus datos personales.

.- El uso de la Aplicación no requiere un seguimiento de la ubicación de los usuarios a título individual; en su lugar, se utilizan datos de proximidad

.- La información recogida se aloja en el equipo terminal del usuario y solo se recoge la información pertinente cuando sea absolutamente necesario.

Beneficios para la Administración

.- Las personas que hayan estado muy cerca de alguien que resulte ser un portador confirmado del virus serán informadas al respecto, a fin de romper las cadenas de transmisión lo antes posible.

.- Tecnología sencilla.

.- La normativa de protección de datos personales contiene una regulación para el uso de casos como lo es el tratamiento que se lleva a cabo con esta Aplicación, que compatibiliza y pondera los intereses y derechos en liza para el bien común.

.- Desempeña un papel importante en la gestión de las medidas de confinamiento durante las posibles situaciones de desescalada.

.- No es necesario que una autoridad almacene información de contacto real.

.- Su repercusión puede reforzarse mediante una estrategia que favorezca la ampliación de las pruebas a las personas que presenten síntomas leves.

Alternativas al tratamiento y por qué no se han elegido:

Como conclusión, cabe señalar que esta Aplicación no puede sustituir, sino meramente complementar, el rastreo manual de contactos realizado por personal sanitario cualificado, que puede determinar si los contactos estrechos pueden o no dar lugar a una transmisión del virus.

Esta labor de rastreo es compleja, principalmente porque exige a los profesionales sanitarios disponer de información rápida y fiable de los contactos de los

pacientes, por lo que se puede concluir que el uso de esta Aplicación cumple con los principios de idoneidad ya que el tratamiento evaluado consigue los objetivos propuestos y el juicio de necesidad ya que, actualmente, no existe otra alternativa menos invasiva para la privacidad para conseguir este propósito con la misma eficacia o con una eficacia razonable.

La aplicación se constituye como una herramienta complementaria de las técnicas tradicionales de rastreo de contactos (en particular, de las entrevistas con personas infectadas), es decir, forma parte de un programa de salud pública de mayor alcance y el objetivo es que sea utilizada exclusivamente hasta el momento en que las técnicas de localización manual de contactos puedan gestionar por sí solas el volumen de nuevas infecciones."

Respecto a las finalidades concretas de la app y los tratamientos de datos personales:

1.10.- Manifiestan que los objetivos perseguidos con esta aplicación de alerta de contagios son los siguientes:

- Preservar la salud pública sin renunciar a la privacidad de los ciudadanos.
- Ir un paso por delante de la COVID-19, alertando de forma proactiva a personas en riesgo de estar incubando el virus.
- Minimizar el impacto económico de la COVID-19, al controlar la pandemia sin medidas drásticas y facilitando el movimiento de personas.

La principal funcionalidad de la aplicación es permitir alertar a las personas que han estado en contacto con alguien infectado por la COVID-19 e informarles de las medidas que conviene adoptar después, como someterse a auto cuarentena o a pruebas diagnósticas. La finalidad última es que las personas que hayan estado muy cerca de alguien que resulte ser un portador confirmado del virus sean informadas al respecto, a fin de romper las cadenas de transmisión lo antes posible.

1.11.- La aplicación móvil implementa una versión de alerta de contactos ("contact tracing") de acuerdo con el protocolo "Decentralized Privacy-Preserving Proximity Tracing" (DP-3T), haciendo uso del API desarrollado conjuntamente por Apple y Google de este protocolo, mediante el conocido como API "Exposure Notification". La app no geolocaliza al usuario ni permite el rastreo de su ubicación, sino que se basa en el intercambio de identificadores pseudoaleatorios, anónimos y efímeros entre el dispositivo del usuario y otros teléfonos móviles próximos, todo ello vía Bluetooth de baja energía. La app tampoco requiere del proceso de identificación o login, ni solicita ningún dato personal.

De acuerdo con este protocolo, cuando una persona da positivo en el test de COVID-19 y decida compartir este dato, únicamente se envían al servidor los pseudocódigos anónimos que él ha emitido y no los que ha detectado de otros móviles cercanos, a diferencia del modelo centralizado que envía todos. Por lo tanto, el cotejo y análisis de datos se lleva a cabo en el móvil de cada usuario y no en el servidor.

Respecto a las tipologías de datos recabados de los usuarios

1.12.- La aplicación no requiere registro y no solicita al usuario ningún dato de carácter personal, solamente se almacenan en el equipo terminal del usuario

los códigos pseudo-aleatorios o Identificador de proximidad, que son datos generados mediante el intercambio de señales de Bluetooth de baja energía (BLE) entre dispositivos dentro de una distancia relevante desde el punto de vista epidemiológico y durante un tiempo relevante también desde el punto de vista epidemiológico.

La app no recoge datos de ubicación.

Estos identificadores de proximidad se comunican únicamente cuando se haya confirmado que un usuario en cuestión está infectado de COVID-19 y a condición de que la persona opte por que así se haga. Estos datos de proximidad son generados a través de las APIs de Google y Apple sin referenciar a ningún dato de usuario ni de dispositivo.

Respecto al periodo de conservación previsto para los datos:

1.13.- Los datos de proximidad se suprimirán cuando dejen de ser necesarios para alertar a las personas y como máximo tras un período de un mes (período de incubación más el margen).

Los datos se almacenan en el dispositivo del usuario, y solo aquellos que hayan sido comunicados por los usuarios y que sean necesarios para cumplir la finalidad se cargan en el servidor central de validación de positivos a disposición de las autoridades sanitarias cuando se haya elegido tal opción (es decir, solo se cargarían los datos en el servidor de «contactos estrechos» de una persona que hubiera dado positivo a la infección de COVID-19).

La aplicación no solicita datos personales y los datos de claves infectadas almacenados en el servidor, se conservarán durante el tiempo que dure la crisis de la COVID-19.

Respecto a la previsión de uso de la app en términos de obligatoriedad y de alcance

1.14.- La descarga de la app es voluntaria, el usuario puede apagar el Bluetooth y desinstalarla en todo momento.

La app estará disponible en dispositivos con sistema operativo iOS, a partir de la versión 13.5, y Android, a partir de la versión 6.0 y posteriores, lo que se estima que cubre el 99% de los teléfonos móviles inteligentes, según la cuota de mercado publicada por revistas especializadas.

La app advierte que los menores de 18 años no podrán usar los servicios disponibles a través de la App sin la previa autorización de sus padres, tutores o representantes legales, quienes serán los únicos responsables de todos los actos realizados a través de la App por los menores a su cargo.

Respecto al procedimiento de rastreo y alerta:

1.15.- El procedimiento de generación de identificadores sigue la implementación del protocolo DP-3T en el API “Exposure Notification” de Apple y Google. Los identificadores efímeros se rotan cada 10-20 minutos, y se descartan al cabo de 14 días.

1.16.- Las alertas de notificación solo presentan información sobre: el tiempo de exposición, la fecha en que ocurrió y el nivel de severidad, en una escala de alto y bajo. Se presenta como una notificación en la aplicación, que puede

ser consultada en todo momento a través del histórico de notificaciones.

En ningún momento se ofrecen datos personales sobre la persona con la que se mantuvo contacto.

1.17.- El procedimiento mediante el que se comunica un positivo contagiado de COVID-19 es el siguiente:

1.- El paciente realiza un test a través de su Servicio Público de Salud.

2.- Si el resultado del test es positivo, desde el servicio de salud se informa de la detección de un positivo y se solicita una clave única de un solo uso.

3.- Se genera un código de confirmación de positivo que se comunica al responsable sanitario autorizado.

4.- Cuando el paciente recibe el resultado positivo en el test de Covid-19, se le proporciona el código de confirmación de un solo uso, que puede introducir en su App.

5.- Con el consentimiento del paciente, su teléfono envía el código de confirmación de un solo uso, que es verificado por el servidor, y se carga el histórico de los últimos 14 días de claves Bluetooth en el servidor central.

Respecto a los tratamientos realizados por la Comunidades Autónomas:

1.18.- Las CCAA, como responsables del tratamiento en su respectivo ámbito, tienen la responsabilidad de entregar un código (PIN de 12 dígitos) a los pacientes que resultan positivos en prueba PCR para COVID19 y que tienen la app RADAR COVID instalada en su dispositivo móvil. En este sentido, desde el sistema de gestión de alertas centralizado se ha habilitado un servicio Web a partir del que se pone a disposición de las CCAA un conjunto de códigos positivos. A partir de ahí, cada CCAA debe definir un procedimiento de custodia y distribución de esos códigos positivos a los pacientes diagnosticados con COVID19 garantizando la custodia de esos códigos y su distribución atendiendo al procedimiento definido en cada CCAA en virtud de sus competencias en el ámbito sanitario.

1.19.- El envío de identificadores positivos entre el servidor central y las CCAA no usa certificados, sino pares de claves (pública-privada) que se generan en las CCAA. Las CCAA incluyen en la petición un token JWT (procedimiento que permite el proceso de autenticación entre un proveedor de identidad y un proveedor de servicio a través de una URL, que generan firmado con su clave privada).

Desde el servidor central se valida la firma del token JWT de la petición con la clave pública que previamente han compartido.

Adicionalmente, se incluye en la respuesta un campo que contiene la firma en base64 de la concatenación de todos los códigos facilitados y se utiliza para generar dicha firma la clave privada del servidor. Las CCAA validan esa firma con clave pública del servidor, que está incluida en el documento de integración, para garantizar que no ha habido alteración de los códigos facilitados.

La entrega de claves públicas se hace de manera privada entre la CCAA y el prestatario del servicio y se definirá un procedimiento ad-hoc en el caso de que una clave pública de una CCAA se haya podido ver comprometida ya que

una vez que se identifique que una clave en una CCAA ha sido comprometida, se puede dar de baja del sistema o reemplazarla por otra. Por el mismo motivo, no hay un procedimiento de revocación de códigos, pero igualmente podrían eliminarse o hacer que caduquen.

Respecto de las terceras entidades intervinientes en los tratamientos:

1.20.- Indra Tecnologías de la Información S.L:

El "P*liego de condiciones para el diseño, desarrollo, piloto y evaluación de un sistema que permita el rastreo de contactos en relación con la pandemia ocasionada por la covid-19",* aceptado por INDRA, recoge en el objeto del contrato las necesidades a cubrir y entre otras, las siguientes cláusulas:

"5.4. Infraestructura en la nube (cloud).

Se precisará que los desarrollos del Backend se realicen en una infraestructura en la nube en modo de autogestión, para facilitar la agilidad en el desarrollo de la solución.

No obstante, lo anterior, tanto el almacenamiento como cualquier actividad de tratamiento de datos se ubicarán en el territorio de la Unión Europea, ya sean éstos provistos y gestionados por la empresa adjudicataria o por sus contratistas y colaboradores, y se alojarán en servidores y/o centros de proceso de datos de la propia empresa adjudicataria o de sus contratistas.

…

En la medida de lo posible, se procurará la utilización de componentes en la infraestructura cloud que permitan la migración futura de la solución a la nube SARA de la AGE.

6.1. Confidencialidad en general

El contratista se compromete a garantizar la más estricta confidencialidad y reserva sobre cualquier dato o información a los que pueda tener acceso o pudiera conocer con ocasión de la ejecución del contrato, así como sobre los resultados obtenidos de su tratamiento, y a que únicamente se utilizarán para la consecución del objeto del contrato, no pudiendo comunicarlos, utilizarlos, ni cederlos a terceros bajo ningún concepto, ni siquiera para su conservación. Estas obligaciones se extienden a todas las personas que, bajo la dependencia del contratista o por su cuenta, hayan podido intervenir en cualquiera de las fases de ejecución del contrato.

La obligación de confidencialidad y reserva conlleva la de custodia e impedir el acceso a la información y documentación facilitadas y a las que resulten de su tratamiento de cualquier tercero ajeno al servicio contratado, entendiéndose como tal tanto cualquier persona ajena a la empresa contratista como cualquiera que, aun no siéndolo, no esté autorizada para acceder a tal información.

Asimismo, el contratista se compromete a velar por la integridad de los datos, es decir, a la protección de la información facilitada y a la que resulte de su tratamiento contra la modificación o destrucción no autorizada de los datos.

6.2. Protección de datos personales

Se deberá cumplir lo estipulado en la ley orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, adaptada al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y por el que se deroga la Directiva 95/46/CE(Reglamento General de Protección de Datos), incluyendo lo dispuesto en la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre y en el Real Decreto 3/2010, de 8 de enero.

Conforme a la Disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Medidas de seguridad en el ámbito del sector público, las medidas de seguridad a aplicar en el marco de los tratamientos de datos personales se corresponderán con las de la Administración púbica de origen y se ajustarán al Esquema Nacional de Seguridad.

Se requerirá a INDRA SOLUCIONES TECNOLOGÍAS DE LA INFORMACIÓN, SLU la manifestación expresa del sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos conforme a los artículos 35.1d y 122.2 de la LCSP modificado por artículo 5 del Real Decreto Ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

6.3. Seguridad

INDRA SOLUCIONES TECNOLOGÍAS DE LA INFORMACIÓN, SLU implementará las medidas técnicas y organizativas de seguridad apropiadas y elaborará la documentación pertinente, de acuerdo con el correspondiente análisis de riesgos, según lo establecido en 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.

7 PROPIEDAD INTELECTUAL

Sin perjuicio de lo dispuesto en la legislación vigente en materia de propiedad intelectual, el adjudicatario acepta expresamente que la propiedad de todos los productos que sean elaborados por el adjudicatario, incluidos sus empleados y en su caso cualquier empresa subcontratada, en ejecución del Contrato y, en particular, todos los derechos de propiedad intelectual y/o industrial que deriven de los mismos, corresponde únicamente a la administración contratante, con exclusividad y sin más limitaciones que las que vengan impuestas por el ordenamiento jurídico.

A los efectos previstos en el párrafo anterior, la empresa adjudicataria se compromete a la entrega a la SGAD de toda la documentación técnica, trabajos y materiales generados, en cuyo poder quedarán a la finalización del Contrato sin que el contratista pueda conservarla, ni obtener copia de esta, ni utilizarla o facilitarla a terceros sin la expresa autorización de la SGAD, que la daría, en su caso, previa petición formal del contratista con expresión del fin."

Aportan los siguientes certificados emitidos a favor de INDRA:

- ISO 27018 Certificado de Privacidad en la Nube: Los sistemas de información que soportan los procesos de negocio y activos de información necesarios para la prestación de servicios de outsourcing de TI Administración, Soporte, Explotación e Infraestructura), tanto en entornos físicos como virtualizados cloud), según la declaración de aplicabilidad en vigor a fecha de emisión del certificado.
- ISO 27001 Certificado del Sistema de Gestión de Seguridad de la Información: Los sistemas de información que soportan los procesos de negocio y activos de información necesarios para la prestación de servicios de outsourcing de TI Administración, Soporte, Explotación e Infraestructura), tanto en entornos físicos como virtualizados cloud), según la declaración de aplicabilidad en vigor a fecha de realización de la auditoría.
- STI-0014/2009 Certificado del Sistema de Gestión de Servicio de Tecnologías de la Información: El SGS de los servicios de outsourcing de TI Administración, Soporte, Explotación e Infraestructura), tanto en entornos físicos como virtualizados cloud), según el catálogo de servicios en vigor. Certificado del Sistema de Gestión de Servicio de Tecnologías de la Información.Para la gestión del sistema RADAR COVID, INDRA ha contratado los servicios de Amazón Web Services INC.

Para la gestión del sistema RADAR COVID, INDRA ha contratado los servicios de Amazón Web Services INC.

1.21.- Amazon Web Services INC:

- Amazon Web Services (AWS) es un conjunto de servicios que ofrece Amazon Web Services INC, e incluye entre otros, servicios de servidores virtuales en la nube, almacenamiento escalable en la nube y gestión de bases de datos relacionales.

El sitio web de AWS informa de que Todos los servicios de AWS cumplen con el Reglamento General de Protección de Datos.

No existe un contrato especifico suscrito entre AWS e INDRA, los servicios se contratan on-line, y es condición necesaria aceptar las condiciones contractuales haciendo clic en la opción "*contratar el producto*". Durante el proceso de contratación on-line el contratante debe elegir la zona geográfica en la que residirán sus datos. El contrato incluye, entre otras, las siguientes cláusulas:

"3.1 Seguridad de AWS. Sin limitación a lo dispuesto en la sección 10 a sus obligaciones contenidas en la sección 4.2, implementaremos medidas adecuadas y razonables diseñadas para ayudarle a asegurar su contenido contra cualquier pérdida, acceso o revelación accidental o ilícita.

3.2 Protección de Datos. Usted podrá especificar las regiones AWS en las cuales se conservará su contenido. Usted aceptará la conservación de su contenido en las regiones AWS de su elección y la transferencia de su contenido a las mismas. Nosotros no accederemos o usaremos su contenido, salvo cuando ello sea necesario para mantener o proporcionar los servicios ofrecidos, o para dar cumplimiento a una disposición legal u orden judicial de una autoridad gubernamental. Nosotros no (a)

revelaremos su contenido a ninguna autoridad gubernamental o tercero (b) según lo dispuesto por la sección 3.3, trasladaremos su contenido de las regiones AWS seleccionadas por usted; salvo, en cada caso, cuando sea necesario para cumplir con una disposición legal u orden judicial de autoridad gubernamental. A menos que ello viole la ley o una orden judicial de una autoridad gubernamental, le daremos aviso de cualquier requerimiento legal u orden según se menciona en esta sección 3.2. Únicamente haremos uso de la información de cuenta de conformidad con el aviso de privacidad, y usted consiente dicho uso. El aviso de privacidad no se aplica a su contenido. "

- Ley aplicable:

"13.4 Ley aplicable. Este Contrato, así como cualquier controversia que pueda surgir en virtud de este, se regirá por las Leyes Aplicables, excluyendo cualquier referencia a las reglas sobre conflicto de leyes. La Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías no se aplicará a este Contrato.

13.5 Controversias. Cualquier controversia o reclamación relacionada en cualquier forma con su utilización de los Servicios Ofrecidos, o cualquier producto o servicio vendido o distribuido por AWS, serán resueltos por los Tribunales Competentes, y usted acepta la jurisdicción y competencia exclusiva de los Tribunales Competentes, conforme a las disposiciones adicionales a continuación.

(a) cuando la Parte Contratante AWS correspondiente sea Amazon Web Services, Inc., las partes acuerdan que resultarán partes aplicables las disposiciones de la presente Sección 13.5(a). Las controversias se resolverán a través de arbitraje vinculante, de conformidad con lo dispuesto en la Sección 13.5, en lugar de ser resueltas en un tribunal, salvo que usted podrá presentar reclamaciones en un tribunal de menor cuantía si estas califican para ello. La Ley Federal de Arbitraje y la legislación federal en materia de arbitraje se aplica a este Contrato. No hay jueces o jurados en el arbitraje, y la revisión por parte de un tribunal de un laudo arbitral es limitada. Sin embargo, un árbitro puede conceder de manera individual las mismas indemnizaciones y medidas que un tribunal (incluidas medidas cautelares o declarativas o indemnización por daños y perjuicios), y debe observar los términos de este Contrato como lo haría un tribunal. Para iniciar un procedimiento de arbitraje, usted deberá enviar una carta solicitando el arbitraje y describiendo su reclamación a nuestro agente Corporation Service Company, 300 Deschutes Way SW, Suite 304, Tumwater, WA 98501. El arbitraje será efectuado por la Asociación Americana de Arbitraje (AAA) bajo sus reglas, que están disponibles enwww.adr.org o llamando al 1-800-778-7879. El pago por la presentación, administración y los honorarios del árbitro se regirá por las reglas de la AAA. Nosotros reembolsaremos esos cargos por reclamaciones menores a 10 000 USD, a menos que el árbitro determine que las reclamaciones son frívolas. No reclamaremos gastos de abogados y costas del arbitraje a menos que el árbitro determine que las reclamaciones sean frívolas. Usted podrá elegir que el arbitraje se lleve a cabo por teléfono, mediante comunicaciones por escri-

to, o en una ubicación convenida por las partes. Usted y nosotros acordamos que cualquier procedimiento de resolución de controversias se llevará a cabo individualmente y no mediante una demanda colectiva, consolidada o representativa. Si por cualquier motivo, la reclamación se llevara a juicio ante un tribunal en lugar de resolverse mediante arbitraje, usted y nosotros renunciamos a cualquier derecho a un juicio con jurado. Sin perjuicio de lo anterior, usted y nosotros acordamos que usted o nosotros podremos entablar demanda en un tribunal para que se prohíba la infracción o cualquier uso indebido de derechos de propiedad intelectual.…"

- Manifiestan que los datos del sistema RADAR COVID son almacenados en los servidores de AWS ubicados en la zona geográfica de Irlanda. Aportan el documento "Arquitectura AWS Cloud: Definición de Servicios" elaborado por INDRA en el que se especifica que la zona en la que residen los servidores de AWS para dar servicio a la app RADAR COVID se encuentra en Irlanda.

Aportan copia de un certificado emitido por AWS a petición de INDRA en el que se certifica que:

"El cliente o partner puede elegir las regiones de AWS en las que se almacenará su contenido y el tipo de almacenamiento. Puede replicar y respaldar el contenido en más de una región de AWS. AWS no transferirá ni replicará su contenido fuera de las regiones de AWS elegidas sin su consentimiento salvo exigencia legal o la necesidad de mantener los servicios de AWS. (para más información visite: https://aws.amazon.com/es/compliance/data-privacy-faq/)

Dentro de la UE, el cliente o partner puede elegir las siguientes regiones operativas actualmente: Francfort, Irlanda, Milán, París, Estocolmo."

- Aportan un certificado de fecha 13 de marzo de 2020 emitido por BDO Auditores, S.L.P., en el que se certifica que los sistemas de información reseñados, todos ellos de categoría ALTA, y los servicios que se relacionan en el Anexo al certificado han sido auditados y encontrados conforme con las exigencias del 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, según se indica en el correspondiente Informe de Auditoría del Esquema Nacional de Seguridad de fecha 06 de marzo de 2020. El anexo contiene una relación de 105 servicios auditados entre los que se encuentran servicios de nube, alojamiento, gestión de bases de datos, seguridad, backup, etc.…

Respecto a la información facilitada a los usuarios:

1.22.- Aportan copia de las distintas versiones de la política de privacidad de la app que además está disponible en https://radarcovid.gob.es/.

La primera versión fue publicada el día 7 de agosto de 2020 junto con la versión 1.0 de la app "Radar COVID" (versión piloto), en la cual se informa respecto a los derechos de protección de datos: "*Dado que la aplicación Radar COVID no almacena datos personales, no son de aplicación los derechos de acceso, rectificación, supresión, limitación, oposición y portabilidad, así como a no ser objeto de decisiones basadas únicamente en el tratamiento automati-*

zado de sus datos. *En todo caso, tenemos obligación de indicarte que te asiste en todo momento el derecho para presentar una reclamación ante Agencia Española de Protección de Datos (www.aepd.es).*

La política de privacidad publicada en octubre de 2020 informa de los siguientes aspectos:

.- Qué es la aplicación y cómo funciona.

.- Quiénes son los responsables del tratamiento:

La aplicación tiene como responsables de tratamiento tanto al Ministerio de Sanidad, como a las Comunidades Autónomas. Así mismo, la Secretaría General de Administración Digital ejerce como encargada del tratamiento."

.- Qué datos tratan:

Los datos manejados por la aplicación no permiten la identificación directa del usuario o de su dispositivo, y son solo los necesarios para el único fin de informarte de que has estado expuesto a una situación de riesgo de contagio por la COVID-19, así como para facilitar la posible adopción de medidas preventivas y asistenciales.

En ningún caso se rastrearán los movimientos de los USUARIOS, excluyendo así cualquier forma de geolocalización.

No se almacenará ni tratará la dirección IP de los USUARIOS.

No se almacenarán los códigos de confirmación de positivo junto con otros datos personales de los usuarios.

Como parte del sistema de alerta de contactos de riesgo de la COVID-19, se procesarán los siguientes datos para los usuarios que hayan dado positivo por COVID-19 para los fines especificados a continuación:

- *Las claves de exposición temporal con las que el dispositivo del usuario ha generado los códigos aleatorios enviados (identificadores efímeros Bluetooth), a los dispositivos con los que el usuario ha entrado en contacto, hasta un máximo de 14 días anteriores. Estas claves no guardan relación alguna con la identidad del USUARIO, y se suben al servidor para que puedan ser descargadas por aplicaciones Radar COVID en poder de otros usuarios. Con estas claves, mediante un procesamiento que tiene lugar en el teléfono móvil de forma descentralizada, se puede advertir al USUARIO sobre el riesgo de contagio por haber estado en contacto reciente con una persona que ha sido diagnosticada por COVID-19, sin que la aplicación pueda derivar su identidad o el lugar donde tuvo lugar el contacto.*
- *Un código de confirmación de un solo uso de 12 dígitos facilitado por las autoridades sanitarias al USUARIO en caso de prueba positiva por COVID-19. Este código debe ser introducido a continuación por el usuario en la aplicación para permitir la carga voluntaria al servidor de las claves de exposición temporal.*
- *El consentimiento del usuario, si aplica, para la remisión de*

claves de exposición temporal al nodo europeo de interoperabilidad de aplicaciones de rastreo de contactos. Toda la información se recogerá con fines estrictamente de interés público en el ámbito de la salud pública, y ante la situación de emergencia sanitaria decretada, a fin de proteger y salvaguardar un interés esencial para la vida de las personas, en los términos descritos en esta política de privacidad, y atendiendo a los artículos 6.1.a), 9.2.a), 6.1.c), 6.1.d), 6.1.e), 9.2.c), 9.2.h) y 9.2.i)

- La legislación aplicable:
  - *Reglamento (UE) 2016/679, 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).*
  - *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.*
  - *Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública.*
  - *Ley 33/2011, de 4 de octubre, General de Salud Pública.*
  - *Ley 14/1986, de 25 de abril, General de Sanidad.*
  - *Real Decreto ley 21/2020, de 9 de junio, de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por el COVID-19.*
  - *Acuerdo de 9 de octubre de 2020, entre el Ministerio de Asuntos Económicos y Transformación Digital (Secretaría de Estado de Digitalización e Inteligencia Artificial) y el Ministerio de Sanidad acerca de la aplicación "Radar COVID".*
- Cómo se obtienen y de dónde proceden los datos:

  El código de confirmación de positivo por COVID-19 facilitado por el Servicio Público de Salud. Esto permitirá la subida al servidor de las claves de exposición temporal con las que el dispositivo del usuario ha generado los códigos aleatorios enviados (identificadores efímeros Bluetooth) a los dispositivos con los que el usuario ha entrado en contacto, hasta un máximo de 14 días anteriores. Estas claves únicamente se suben al servidor con el consentimiento explícito e inequívoco del USUARIO, al haber introducido un código de confirmación de positivo por COVID-19.
- Para qué y por qué se utilizan los datos:

  La recogida, almacenamiento, modificación, estructuración y en su caso, eliminación, de los datos generados, constituirán operaciones de tratamiento llevadas a cabo por el Titular, con la finalidad de garantizar el correcto funcionamiento de la App, mantener la relación de prestación del servicio con el Usuario, y para la gestión, administración, información, prestación y mejora del servicio.

La información y datos recogidos a través de la Aplicación serán tratados con fines estrictamente de interés público en el ámbito de la salud pública, ante la actual situación de emergencia sanitaria como consecuencia de la pandemia del COVID-19 y la necesidad de su control y propagación, así como para garantizar intereses vitales tuyos o de terceros, de conformidad con la normativa de protección de datos vigente.

A tal efecto, utilizamos tus datos para prestarte el servicio de "Radar COVID" y para que puedas hacer uso de sus funcionalidades de acuerdo con sus condiciones de uso. De conformidad con el Reglamento General de Protección de Datos (RGPD) así como cualquier legislación nacional que resulte aplicable, la Secretaría General de Administración Digital tratará todos los datos generados durante el uso de la App para las siguientes finalidades:

o Ofrecerte información sobre contactos considerados de riesgo de exposición a la COVID-19.

o Proporcionarte consejos prácticos y recomendaciones de acciones a seguir según se produzcan situaciones de riesgo de cara a la cuarentena o auto-cuarentena.

Se utilizarán los datos siempre y sólo de forma anonimizada para fines estadísticos y epidemiológicos.

Este tratamiento se llevará a cabo a través de la funcionalidad de alerta de contagios que permite identificar situaciones de riesgo por haber estado en contacto estrecho con personas usuarias de la aplicación que se encuentran infectadas por la COVID-19. De esta manera se te informará de las medidas que conviene adoptar después.

- Durante cuánto tiempo se conservan los datos:

Las claves de exposición temporal y los identificadores efímeros de Bluetooth son almacenados en el dispositivo por un periodo de 14 días, después de los cuales son eliminados.

Asimismo, las claves de exposición temporal que hayan sido comunicadas al servidor por los USUARIOS diagnosticados como positivos por COVID-19 también serán eliminadas del servidor al cabo de 14 días.

En todo caso, ni las claves de exposición temporal ni los identificadores efímeros de Bluetooth contienen datos de carácter personal ni permiten identificador los teléfonos móviles de los usuarios.

- Quién tiene acceso a los datos

Los datos gestionados por la aplicación móvil (claves diarias de exposición temporal e identificadores efímeros Bluetooth) se almacenan únicamente en el dispositivo del usuario a los efectos de poder hacer cálculos y avisar al USUARIO sobre su riesgo de exposición a la COVID-19.

Solo en el caso de reportar un diagnóstico positivo por COVID-19, las claves de exposición temporal de los últimos 14 días generadas en el dispositivo, y bajo el consentimiento explícito e inequívoco del USUARIO, son subidas al servidor para su difusión al conjunto de USUARIOS de este sistema.

Estas claves no guardan relación alguna con la identidad de los dispositivos móviles ni con datos personales de los USUARIOS de la Aplicación.

- Cuáles son tus derechos y cómo puedes controlar tus datos:

La normativa vigente te otorga una serie de derechos en relación con los datos e información que tratamos sobre ti. Concretamente, los derechos de acceso, rectificación, supresión, limitación y oposición.

Puedes consultar el alcance y detalle completo de los mismos en la página web de la Agencia Española de Protección de Datos (AEPD) aquí.

Con carácter general, podrás ejercitar todos estos derechos en cualquier momento y de forma gratuita. Puedes dirigirte a los Responsables de Tratamiento por vía electrónica, bien Ministerio de Sanidad o Comunidad Autónoma de residencia. En el caso del Ministerio de Sanidad, puede hacerlo a través de este ***formulario*** [pinchando en el formulario enlaza con la web del Ministerio de Sanidad, Consumo y Bienestar Social (https://sede.mscbs.gob.es/canalesAcceso/oficinas.htm)]*,o presencialmente a través de la red de oficinas de asistencia en materia de registros utilizando este* ***modelo de solicitud*** [enlaza con el formulario de solicitud de ejercicio de derechos Reglamento General de Protección de Datos del MSCBS]

Asimismo, te asiste en todo momento el derecho para presentar una reclamación ante Agencia Española de Protección de Datos

- Cómo protegemos tus datos

Los Responsables, así como la SGAD en condición de encargada del tratamiento, garantizan la seguridad, el secreto y la confidencialidad de tus datos, comunicaciones e información personal y han adoptado las más exigentes y robustas medidas de seguridad y medios técnicos para evitar su pérdida, mal uso o su acceso sin tu autorización. Las medidas de seguridad implantadas se corresponden con las previstas en el anexo II (Medidas de seguridad) del 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.

Finalmente, te informamos que tanto el almacenamiento como el resto de las actividades del tratamiento de datos no personales utilizados estarán siempre ubicados dentro de la Unión Europea.

- Qué debes tener especialmente en cuenta al utilizar "Radar COVID”

Has de tener en cuenta determinados aspectos relativos a la edad mínima de utilización de Aplicación, la calidad de los datos que nos proporcionas, así como la desinstalación de la Aplicación en tu dispositivo móvil.

Edad mínima de utilización: para poder utilizar “Radar COVID” tienes que ser mayor de 18 años o contar con la autorización de tus padres y/o tutores legales. Por tanto, al darte de alta en la Aplicación, garantizas al Titular que eres mayor de dicha edad o, en caso contrario, que cuentas con la mencionada autorización.

Calidad de los datos que nos proporcionas: la información que nos facilites en el uso de los servicios de la Aplicación deberá de ser siempre real, veraz y estar actualizada.

Desinstalación de la Aplicación: en general, puede haber dos situaciones en las que se proceda a la desactivación técnica de la Aplicación en tu dispositivo: 1) que lo realices voluntariamente, y 2) que desde el Titular se proceda a la desactivación técnica de la Aplicación en tu dispositivo (p.ej. en casos en los que detectemos que has incumplido las condiciones de uso de la Aplicación).

- Transferencia de datos a países de la Unión Europea:

Radar COVID participa en la plataforma de integración de aplicaciones de la unión europea, de manera que se compartirán las claves positivas con terceros países de la UE y viceversa.

Cuando el dispositivo del usuario descarga las claves positivas para analizar posibles contactos estrechos, descargará también las claves positivas de terceros países adheridos al proyecto europeo. Esto permitirá identificar posibles contactos estrechos tanto si el usuario ha estado visitando alguno de estos países como si ha estado en contacto estrecho con un visitante procedente de estos países.

Cuando el usuario introduce un código de confirmación de diagnóstico positivo por COVID-19, se solicitará el consentimiento del usuario libre, específico, informado e inequívoco para compartir sus claves infectadas con terceros países a través de la plataforma de interoperabilidad europea facilitando el rastreo digital de posibles contactos estrechos. La comunicación de tus claves infectadas a la red de países europeos adheridos a este proyecto es completamente voluntaria.

No se efectuarán transferencias de datos fuera de la Unión Europea.

- Política de cookies

Utilizamos solamente cookies técnicas que permiten al usuario la navegación y la utilización de las diferentes opciones o servicios que se ofrecen en la Aplicación como, por ejemplo, acceder a partes de acceso restringido o utilizar elementos de seguridad durante la navegación.

Respecto al almacenamiento y seguridad de los datos:

1.23.- En los terminales móviles se almacenan las claves diarias que permiten la generación de los identificadores de proximidad efímeros (Rolling Proximity Identifiers o RPI). A su vez, se almacenan los identificadores efímeros recibidos desde los teléfonos móviles cercanos. Esta información se almacena un máximo de 14 días.

1.24.- El servidor almacena las claves de personas “infectadas” para su posterior descarga por parte de las aplicaciones móviles. Los datos son almacenados en base de datos relacionales y para cada positivo reportado se almacenará, la fecha de inicio de síntomas, y las 14 claves diarias tomadas a partir de la fecha de inicio de síntomas. Toda esta información reside en el dispositivo móvil.

No se almacena ni gestiona ningún dato sobre las pruebas diagnósticas reali-

zadas a ninguna persona. Se recolectan las balizas de los usuarios que hayan sido diagnosticados de Covid-19 pero no hay relación entre estas balizas y datos concretos de ningún usuario.

Los datos se almacenan cifrados en base a los algoritmos de cifrados definidos para bases de datos Aurora (AES-256).

Aportan la estructura de la base de datos y descripción de tablas y campos, de lo que se desprende que la base de datos no incorpora datos identificativos de personas físicas (Teléfono, imei, MAC, IP, etc.…).

1.25.- Respecto a las medidas técnicas y organizativas implementadas que garanticen la seguridad de los datos personales manifiestan:

La aplicación RADAR COVID, así como toda su infraestructura forma parte de los sistemas de información gestionados a través de los servicios de outsourcing de TI de la empresa INDRA, para Administración, Soporte, Explotación e Infraestructura tanto en entornos físicos como virtualizados cloud. Como ya se ha expuesto en el punto “Respecto a las terceras entidades intervinientes” de este informe, aportan certificados de cumplimiento de los estándares ISO 27018, ISO 27001 y STI-0014/2009.

1.26.- Aportan copia del informe de auditoría de seguridad de la app piloto de fecha 15 de julio de 2020 elaborado por Minsait, unidad de negocio de tecnología y consultoría de INDRA, en el que se especifica que no se han realizado pruebas sobre el propio protocolo Bluetooth y las comunicaciones realizadas por el mismo, y que las versiones analizadas, el reporte de positivos se realiza de forma directa, no implicando a Sanidad en este proceso al tratarse de un entorno de pruebas, por lo que los resultados presentados no aplicaran al nuevo sistema si difiere del comprobado en este entorno.

Tras el análisis de los hallazgos obtenidos mediante las distintas pruebas ejecutadas, la seguridad global es considerada como Baja, debido a la existencia de al menos una vulnerabilidad catalogada como Alta.

Atendiendo a las vulnerabilidades de severidad alta, el informe concluye que:

- La aplicación hace uso de contraseñas débiles.

Y entre las vulnerabilidades de severidad media y baja, el informe recoge:

- El canal de comunicación se encuentra cifrado con protocolos y algoritmos de cifrado débiles.

1.27.- Aportan el documento elaborado por el Centro Criptológico Nacional (CCN) que es el resultado obtenido de la auditoria de seguridad de la aplicación móvil Radar COVID y de sus conexiones, con objeto de evaluar su nivel de seguridad y cumplimiento. El análisis ha tenido como objetivo la verificación del nivel de cumplimiento de los requisitos y medidas de seguridad contemplados en la normativa CCN-STIC. La revisión análisis estático de la aplicación Android Radar COVID se ha realizado entre los días 20 y 21 de agosto de 2020. El análisis de las conexiones llevadas a cabo por las aplicaciones se ha realizado posteriormente en el entorno de producción y preproducción. La revisión de las conexiones en el entorno de preproducción se ha llevado a realizado entre los días 28 de septiembre y 2 de octubre de 2020.

A la finalización del análisis, el estado de exposición del sistema es el siguien-

te:

- 14 vulnerabilidades encontradas.
- 4 corregidas.
- 10 quedan pendientes de corregir:
  - 3 son de criticidad MEDIA.
  - El resto BAJA.

Las vulnerabilidades de criticidad MEDIA pendientes de corregir afectan a la falta de medios de protección ante la posibilidad de terceros de hacer ingeniería inversa a la aplicación con la intención de obtener datos sensibles o manipular su funcionamiento, evadir restricciones y/o comprender el funcionamiento interno de la misma.

En esta misma línea, también se han detectado deficiencias en la protección de las comunicaciones de la aplicación con el backend de la misma. Estas deficiencias se han encontrado durante el análisis en preproducción, recomendándose su comprobación en el entorno final, es decir, en el backend en producción.

El resultado de la inspección es considerado APTO: la evaluación de la seguridad dentro de esta área no ha encontrado desviación alguna cuantificable que pudiera impedir la validación con respecto a la configuración de seguridad requerida.

El informe concluye que en la revisión de la aplicación móvil Radar COVID, en los términos de seguridad de las TIC, no se ha encontrado deficiencias con gravedad CRÍTICA para impedir el correcto funcionamiento en el campo de la ciberseguridad, quedando excluidos los análisis y comportamientos funcionales, sin perjuicio de las actuaciones que lleve a cabo el Ministerio de Asuntos Económicos y Transformación Digital.

1.28.- Aportan dos documentos denominados “Informe de Análisis de riesgos. Servicio RADAR COVID 19” elaborado en cumplimiento del Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la administración electrónica, de fecha de septiembre de 2020. El primero utiliza el catálogo de salvaguardas del ENS, implementado por PILAR, el segundo incorpora además el catálogo de salvaguardas del Reglamento General de Protección de Datos (RGPD) implementado por PILAR. Del informe del análisis de riesgos que incorpora ambas salvaguardas se desprende lo siguiente:

- El alcance del Análisis de Riesgos comprende la infraestructura que se encuentra detallada en el documento “App Bluetooth contra Covid-19 v5.pdf” y que es necesaria para prestar el Servicio Radar Covid de la Secretaria de Estado de Digitalización e Inteligencia Artificial (app contact tracing, backend desplegado en nube AWS, y redes de comunicaciones).

- Metodología de Análisis de Riesgos: Identificación de la Fase de desarrollo del Plan de Adecuación al ENS y descripción de las tareas de la Metodología MAGERIT, utilizada para realizar las actividades y tareas del Análisis de Riesgos y la descripción del trabajo realizado:

- Categorización de Activos
- Categorización de Amenazas
- Categorización de Salvaguardas
- Estimación del Estado del Riesgo

• Se ha realizado la valoración de acuerdo con la información disponible sobre el Sistema de Información RADAR COVID19 en relación con las Dimensiones de Seguridad: Autenticidad, Confidencialidad, Integridad, Disponibilidad y Auditabilidad o Trazabilidad.

La valoración del Servicio Radar Covid, debido a la tipología de datos que trata y a lo indicado en la Guía CCN-STIC 803, la valoración en cada una de las dimensiones de seguridad (Autenticidad, confidencialidad, Integridad, Disponibilidad y Trazabilidad) debería ser al menos MEDIO, sin embargo, debido a la situación política y socioeconómica en la que nos encontramos originada por la pandemia Covid 19 y al impacto que supondría una brecha de seguridad de la información que trata, el Servicio Radar Covid ha sido evaluado con una categoría ALTA.

• La relación de amenazas que se ha considerado para el Análisis de Riesgos y que constituye el catálogo de amenazas implementadas de forma estándar en la herramienta PILAR son: Desastres naturales, de origen industrial, errores, fallos no intencionados y ataques intencionados.

• Los activos contemplados son: Servicio Radar Covid, Teléfono Móvil, Redes de Comunicaciones, App Radar Covid, Administradores / Operadores, Desarrolladores, Desarrollo y Mantenimiento de la App, Ciudadanos, Soportes, Equipos AWS, Instalaciones AWS, Repositorio Descargas (APPLE STORE), Servicio Cloud, Repositorio Descargas (ANDROID STORE).

• Se ha identificado el grado de madurez de cada uno de los artículos del RGPD que deben ser tenidos en consideración.

• El valor del Riesgo Potencial obtenido de la herramienta PILAR es de 6,3 sobre 10 (Riesgo muy crítico). Los activos que presentan nivel de riesgo crítico son: Redes de comunicaciones, app RADAR COVID, soporte, instalaciones AWS y equipos AWS.

- El valor del Riesgo Residual (tras aplicar las salvaguardas) obtenido de la herramienta PILAR es de 2,6 sobre 10 (Riesgo medio). una vez que se han tenido en cuenta las salvaguardas implantadas, el nivel de riesgo de los activos se reduce considerablemente, hay 12 activos con riesgo despreciable, 1 con riesgo bajo y 1 con riesgo medio.

- El valor del Riesgo Objetivo (Objetivo a alcanzar tras la implantación de las salvaguardas propuestas) obtenido de la herramienta PILAR es de 1,8 sobre 10 (Riesgo bajo).

Para el Servicio RADAR COVID19 se ha propuesto realizar las acciones necesarias para minimizar el riesgo residual de manera que no haya ningún activo con riesgo de nivel MEDIO. Para ello se han seleccionado aquellos riesgos que se encuentran por encima del valor 2 y, sobre ellos, se han identificado las salvaguardas que se encontraban por debajo del

valor recomendado por PILAR para el Esquema Nacional de Seguridad para subirlas al valor recomendado.

Se recomienda abordar un conjunto de acciones para mejorar las medidas de seguridad existentes actualmente, con el objeto de ajustar el nivel de riesgo del Servicio Radar Covid19 a un nivel BAJO. Estas acciones se han focalizado en las medidas de seguridad que pueden minimizar las amenazas que aportan un nivel de riesgo MEDIO en el presente Análisis de Riesgos. Estas acciones permitirán alcanzar el nivel de Riesgo Objetivo propuesto, ya que aumentarían el grado de madurez de las medidas de seguridad Firma electrónica y Mecanismos de autenticación. Las acciones propuestas en este caso son:

- Utilizar certificados cualificados para la firma digital que se utiliza en el servicio de verificación de los positivos.

- Aunque el acceso a la consola de AWS se realiza mediante *AWS Multi-Factor Authentication (MFA)*, y por tanto cumple con la medida de utilizar un segundo factor de autenticación, se recomienda verificar que los elementos criptográficos hardware utilizan algoritmos y parámetros acreditados por el CCN. Además, se recomienda revisar el mecanismo control de acceso a la Base de Datos PostgreSQL para concluir que cumple con los requisitos de nivel alto.

1.29.- Aportan el documento "*Informe de Evaluación de Impacto relativa a la Protección de Datos del tratamiento RADAR COVID*" de fecha septiembre de 2020, cuyo contenido recoge los siguientes aspectos más relevantes:

• El objetivo del documento es realizar la Evaluación del Impacto relativa a la Protección de los Datos (EIPD) del tratamiento llevado a cabo por la Aplicación "Radar COVID" (en adelante "la Aplicación"), según lo exigido en el Reglamento (UE) 2016/679 del Parlamento Europeo (RGPD) cuando el tratamiento conlleve un alto riesgo para los derechos y libertades de las personas físicas.

• La elaboración del informe sigue las directrices establecidas por la Agencia Española de Protección de Datos (en adelante "AEPD") en la "Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD".

• Respecto a la necesidad de realizar una Evaluación de Impacto relativa a la Protección de Datos en el tratamiento evaluado, el informe indica que concurren factores que contribuyen a generar un nivel de riesgo elevado, debiéndose realizar una EIPD al objeto de determinar un escenario de gestión del riesgo adecuado.

• Respecto a los responsables, corresponsable y encargados del tratamiento el informe recoge lo siguiente:

El responsable de tratamiento es la Dirección General de Salud Pública, dependiente del Ministerio de Sanidad.

El encargado de tratamiento es la Secretaría General de Administración Digital, dependiente del Ministerio de Asuntos Económicos y Transformación Digital, que ha desarrollado la Aplicación.

• Respecto a los Datos personales objeto del tratamiento:

- La aplicación genera datos de proximidad (claves de exposición temporal con las que el dispositivo del usuario ha generado los códigos aleatorios o Identificador de proximidad rodante - RPI). Estos datos se comunicarán a las autoridades sanitarias únicamente cuando se haya confirmado que un usuario en cuestión está infectado de COVID-19 y a condición de que la persona opte por que así se haga, es decir, de manera voluntaria.
- Dato mediante el que el usuario es advertido previamente de un contacto de riesgo. Estos datos permiten estimar cuántos usuarios son advertidos por la aplicación de un riesgo potencial de contagio, sin poder rastrear su identidad, y le permite al Servicio Nacional de Salud preparar las iniciativas y los recursos necesarios para atender a los usuarios que han recibido la notificación.
- El día en que el usuario desarrolló síntomas compatibles con COVID-19.
- Código proporcionado por las autoridades sanitarias para permitir al usuario activar una alerta de advertencia. Este número de 12 cifras será proporcionado por las autoridades sanitarias a los usuarios de la aplicación mediante Quick Response code (QR). Los usuarios podrán, voluntariamente, introducir dicho código en la Aplicación para confirmar el diagnóstico positivo y desencadenar el procedimiento de notificación a sus contactos estrechos. Este código es una confirmación de diagnóstico positivo de un usuario. Existe verificación de dicho código para evitar que cualquier usuario envíe pruebas falsas.
- La dirección IP que utiliza el dispositivo para conectarse a Internet.

  Estos datos no permiten la identificación directa del usuario o de su dispositivo, existiendo estudios sobre la robustez de los protocolos de criptografía y anonimización, aunque existe la posibilidad de que puedan romperse y asociarse los identificadores con números de teléfono y personas, aplicando suficiente tiempo y capacidad de cómputo, si bien esto se considera altamente improbable. Por otra parte, debe tenerse en cuenta que el tratamiento de la información no solo afecta al usuario de la aplicación, sino también la de todos los terceros con los que ha estado en contacto.

• Respecto a la finalidad del tratamiento:

- La finalidad principal de la App es informar a las personas que hayan estado muy cerca de alguien que resulte ser un portador confirmado del virus, a fin de romper las cadenas de transmisión lo antes posible. De esta manera, la Aplicación permite identificar a las personas que han estado en contacto con alguien infectado por la COVID-19 e informarles de las medidas que conviene adoptar después, como someterse a auto cuarentena o a las pruebas correspondientes.
- Para ello la App mantiene los contactos de las personas que utilizan la Aplicación y que pueden haber estado expuestas a la infección de la COVID-19.
- Cuando una persona da positivo en el test de COVID-19 y decida com-

partir libremente este dato, la App alerta a aquellas otras personas que podrían haber sido infectadas y con las que se haya tenido contacto los últimos 14 días. Para ello, esta persona deberá compartir un número de 12 cifras que será proporcionado por las autoridades sanitarias. El móvil realiza una comprobación de si los ID aleatorios coinciden con alguno que haya sido marcado como positivo.

- Se determina el día en que el usuario desarrolló síntomas compatibles con COVID-19 y fecha de contacto con personas infectadas. Los datos también podrán ser procesados fines de investigación científica o fines estadísticos. En tal caso los datos se encontrarán totalmente anonimizados.

• Se hace una descripción de los elementos que intervienen en cada una de las fases del ciclo de vida de los datos del tratamiento (actividad, actores y sistemas).

• Se hace una descripción de las tecnologías intervinientes.

• Respecto a la licitud y normativa:

En virtud de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (artículo 5), el almacenamiento de información en el dispositivo del usuario o la obtención de acceso a la información ya almacenada se permite únicamente si: i) el usuario ha dado su consentimiento, o ii) el almacenamiento o el acceso son estrictamente necesarios para el servicio de la sociedad de la información, en este caso la Aplicación, que el usuario ha solicitado de manera expresa (esto es, mediante la instalación y activación). En el caso de la Aplicación objeto de evaluación, no se cumple el requisito ii), ya que la carga de datos de proximidad para el rastreo de contactos y alerta no es necesaria para el funcionamiento de la Aplicación en sí misma, por tanto, es necesario obtener el consentimiento libre, específico, explícito e informado, mediante una clara acción afirmativa del usuario.

Como base jurídica para un tratamiento lícito de datos personales, el RGPD reconoce explícitamente las dos citadas: misión realizada en interés público (art. 6.1.e) o intereses vitales del interesado u otras personas físicas (art. 6.1.d).

Indican que, para el tratamiento de datos de salud no basta con que exista una base jurídica del art. 6 RGPD, sino que de acuerdo con el art. 9.1 y 9.2 RGPD exista una circunstancia que levante la prohibición de tratamiento de dicha categoría especial de datos (entre ellos, datos de salud). LA AEPD entiende que dichas circunstancias cabe encontrarlas, en este caso, en varios de los epígrafes del art. 9.2 RGPD.

• Respecto al análisis de la necesidad, proporcionalidad del tratamiento:

- Principio de limitación de la finalidad: La finalidad principal de la App es informar a las personas que hayan estado muy cerca de alguien que resulte ser un portador confirmado del virus, a fin de romper las cadenas de transmisión lo antes posible. De esta manera, la Aplicación per-

mite identificar a las personas que han estado en contacto con alguien infectado por la COVID-19 e informarles de las medidas que conviene adoptar después, como someterse a autocuarentena o a las pruebas diagnósticas correspondientes.

- Principio de minimización de datos: indican que se recaban exclusivamente los datos personales que se requieren para las finalidades indicadas.
- Principio de limitación del plazo de conservación: Los plazos se basan en la importancia médica y en lapsos realistas para las medidas administrativas que, si procede, deban tomarse.

  Los datos generados para el rastreo de contactos y alerta: Los datos de proximidad se suprimirán tan pronto como dejen de ser necesarios para alertar a las personas y como máximo tras un período de un mes (período de incubación más el margen).

  Los datos se almacenan en el dispositivo del usuario, y solo aquellos que hayan sido comunicados por los usuarios y que sean necesarios para cumplir la finalidad se cargan en el servidor central de validación de positivos a disposición de las autoridades sanitarias cuando se haya elegido tal opción (es decir, solo se cargarían los datos en el servidor de «contactos estrechos» de una persona que hubiera dado positivo a la infección de COVID-19).

  En todo caso, los datos personales solo deben conservarse durante la crisis de la COVID- 19. Después, como regla general, todos los datos personales deberían borrarse o anonimizarse.

• Medidas para la reducción del riesgo:

- La aplicación no recoge información que no tenga relación con el objeto específico o no sea necesaria — por ejemplo, estado civil, identificadores de las comunicaciones, elementos del directorio del equipo, mensajes, registros de llamadas, datos de localización, identificadores de dispositivos, etc.

- Los datos difundidos por las aplicaciones solo incluyen algunos identificadores únicos y seudónimos, generados por la aplicación y específicos de esta. Esos identificadores se renuevan periódicamente, con una frecuencia compatible con el propósito de contener la propagación del virus y suficiente para limitar el riesgo de identificación y de rastreo físico de personas.

- Aunque el modelo es descentralizado, siempre va a ser necesario un servidor central, de la autoridad sanitaria, donde registrar los códigos de las personas diagnosticadas con COVID-19. Este servidor de rastreo de contactos debe limitarse a recoger el historial de contactos o los identificadores seudónimos de un usuario que haya sido diagnosticado como infectado como resultado de una evaluación adecuada realizada por las autoridades sanitarias y de una acción voluntaria del usuario.

- Se aplicarán técnicas criptográficas avanzadas para garantizar la seguridad de los datos almacenados en los servidores y aplicaciones y los intercambios entre las aplicaciones y el servidor remoto. También se procederá a la autenticación mutua entre la aplicación y el servidor.

- La notificación de los usuarios infectados de SARS-CoV-2 en la aplicación se someterá a una autorización adecuada mediante un código de un solo uso unido a una identidad seudónima de la persona infectada y vinculado con un laboratorio de pruebas de detección o con un profesional de atención sanitaria. Si no se puede obtener confirmación de forma segura, no tendrá lugar ningún tratamiento de datos que presuponga la validez del estado del usuario.

- El responsable del tratamiento, en colaboración con las autoridades, tiene que facilitar información clara y explícita sobre el enlace que permita descargar la aplicación oficial nacional de rastreo de contactos, con el fin de mitigar el riesgo de que se utilicen aplicaciones de terceros.- En virtud de los principios de integridad y confidencialidad, teniendo en cuenta que los datos de salud merecen una protección más elevada, se aplicarán medidas de carácter técnico y organizativo actualizadas adecuadas que garanticen un nivel de seguridad suficiente. Tales medidas consisten en la seudonimización, el cifrado y la celebración de acuerdos de confidencialidad, así como en una distribución estricta de los roles de acceso y el establecimiento de restricciones y registros de acceso. Asimismo, hay que tener en cuenta las disposiciones nacionales que pueden establecer requisitos técnicos concretos u otras garantías, tales como la observancia de las normas de secreto profesional.

• Evaluación de riesgos y salvaguardas

La evaluación de riesgos realizada para el servicio “Radar COVID” se encuentra recogida en el “Análisis de Riesgos Servicio Radar Covid”, generado con la herramienta “PILAR” mediante el que se ha llevado a cabo la evaluación de riesgos y salvaguardas para el tratamiento “Radar COVID” y toda la infraestructura que se ha implementado para este servicio.

• Plan de acción:

Para el Servicio Radar COVID se propone en el Informe de AARR, realizar una serie de acciones necesarias para minimizar el riesgo residual de manera que no haya ningún activo con riesgo de nivel MEDIO. para ello se han seleccionado aquellos riesgos que se encuentran por encima del valor {2} y, sobre ellos, se han identificado las salvaguardas que se encontraban por debajo del valor recomendado por PILAR para el Esquema Nacional de Seguridad para subirlas al valor recomendado.

• Conclusiones recogidas en el informe de EIPD:

Se han propuesto una serie de acciones y recomendaciones en el Informe de AARR cuya implantación supondría que ninguno de los activos alcanzaría un riesgo medio, sino que todos se podrían calificar de riesgo bajo e incluso muchos de ellos de riesgo despreciable.

Respecto a la interoperabilidad:

1.30.- El día 16 de junio de 2020 se adopta por consenso del grupo de trabajo de eHealth Network el documento “*Directrices de eHealth Network para los Estados miembros de la UE y la Comisión Europea sobre especificaciones de interoperabilidad para cadenas de transmisión transfronterizas entre aplicacio-*

nes aprobadas. Elementos detallados de interoperabilidad entre soluciones basadas en claves COVID +", en el que se propone una arquitectura definitiva para implementar del servicio Federation Gateway. El servicio Federation Gateway, acepta claves de diagnóstico de todos los países, las almacena temporalmente y las proporciona para que se descarguen en todos los países. Además, todos los backends pueden ser informados de inmediato si hay nuevos datos disponibles, de modo que los retrasos de transmisión se mantengan mínimos.

El día 16 de julio de 2020 se publicó en el DOUE la Decisión de Ejecución (UE) 2020/1023 de la Comisión de 15 de julio de 2020 que modifica la Decisión de Ejecución (UE) 2019/1765 en lo concerniente al intercambio transfronterizo de datos entre las aplicaciones móviles nacionales de rastreo de contactos y advertencia para combatir la pandemia de COVID-19. Esta Decisión establece disposiciones sobre el papel de los Estados miembros participantes y de la Comisión en relación con el funcionamiento de la pasarela federativa para la interoperabilidad transfronteriza de las aplicaciones móviles nacionales de rastreo de contactos y advertencia.

El día 2 de septiembre de 2020 se adopta por consenso del grupo de trabajo de eHealth Network el documento "*Certificado europeo de interoperabilidad. Gobernanza. Arquitectura de seguridad para el seguimiento y la advertencia de contactos aplicaciones*" que establece que el intercambio seguro y confiable de claves de diagnóstico entre países europeos es realizado por el European Federation Gateway Service (EFGS) que distribuye los datos entre los estados miembros. Este intercambio de claves de diagnóstico está asegurado por criptografía firmas transparentes para todos los países que participan en el sistema. Las firmas digitales se pueden utilizar para lograr la integridad y autenticidad de los datos. Una confianza bien definida del modelo es necesario para vincular la clave pública de una entidad a su identidad con el fin de permitir otros participantes para verificar el origen de los datos o la identidad del interlocutor. En el contexto de la EFGS esto significa que las claves públicas de los Estados miembros europeos también ya que la clave pública de los EFGS debe estar vinculada a sus identidades para establecer la confianza entre los participantes. De esta forma, los Estados miembros pueden verificar la integridad y autenticidad de las claves de diagnóstico firmadas proporcionadas por la EFGS. Este documento establece los servicios de confianza y seguridad que se establecerán en la EFGS.

1.31.- Con fecha 15 de octubre de 2020 la SGAD aporta a la inspección de datos copia de la Declaración y carta de intención sobre la conexión de ESPAÑA con el EFGS remitida por el Secretario General de Administración Digital a la Comisión Europea, así como copia del preceptivo formulario de solicitud de intención de participación en el EFGS y anexos (encuesta y check list).

Manifiestan que la entrada en servicio de la interoperabilidad con Radar COVID se prevé para el 30 de octubre de 2020.

2.- Con fecha 16 de diciembre de 2020 se solicitó información a la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud (SGSDII), respecto a las instrucciones dadas al encargado del tratamiento, y en particular en relación con la protección de datos desde el diseño y por defecto de la app "RADAR COVID" y copia, en su caso, de los informes elaborados por el De-

legado de Protección de Datos, y en particular los relativos a la supervisión de los tratamientos y a la necesidad de elaboración de la evaluación de impacto relativa a la protección de datos, así como las medidas llevadas a cabo por la SGSDII en base a los puntos 3 de la segunda y tercera cláusulas del Acuerdo, teniendo entrada con fecha 28 de enero de 2021 escrito de respuesta en el que informan, entre otros, de lo siguiente:

> El Ministerio de Sanidad ejerce el rol de responsable del tratamiento a través de la Secretaría General de Salud Digital, Innovación e Información del SNS (SGSDII), y la Secretaría General de Administración Digital (en adelante, SGAD), dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial (en adelante, SEDIA), del Ministerio de Asuntos Económicos y Transformación Digital, ejerce el rol de encargado del tratamiento desde la firma del Acuerdo suscrito entre ambos ministerios entre el Ministerio de Asuntos Económicos y Transformación Digital y el Ministerio de Sanidad acerca de la aplicación "RADAR COVID", publicado en el BOE de 15/10/2020.
>
> Informan sobre las solicitudes de informes y estadísticas realizadas por parte de la SGSDII a la SGAD desde agosto de 2020 y el seguimiento realizado.
>
> Respecto a la evaluación de impacto de los tratamientos que realiza la app Radar COVID, informan que el 15 de diciembre de 2020 se hizo una revisión del EIPD para EFGS, sugiriendo la realización de un test de penetración y/o una auditoría de ciberseguridad externa más amplia tras revisión del documento de análisis de riesgos y análisis de impacto remitido por el encargado del tratamiento.

Respecto a la app de GOOGLE:

3.- Se han realizado las siguientes comprobaciones en un dispositivo móvil con sistema operativo Android versión 10.0:

> 3.1.- Se ha comprobado que el sistema operativo ha instalado un nuevo servicio denominado "*Notificaciones de exposición al COVID 19"* versión 17203704005. Tras acceder a este servicio se verifica lo siguiente:
>
> - Informa de las comprobaciones de exposición que se han realizado en los últimos 14 días (día y hora).
> - Dispone de una opción que permite eliminar los identificativos aleatorios.
> - Informa que se comparte con la app la fecha, la duración y la intensidad de la señal asociada a la exposición.
> - Informa de cómo funciona y cómo utilizar el sistema de exposiciones.
> - Informa de que el sistema de exposición no usa, guarda ni comparte la ubicación del dispositivo y que es necesario activar la ubicación del dispositivo porque la tecnología de las notificaciones de exposición utiliza la búsqueda de dispositivos Bluetooth para saber cuáles están cerca ya que en todos los teléfonos con Android 6.0 y versiones superiores, para poder usar esa búsqueda Bluetooth, tienen que estar activados los ajustes de ubicación del dispositivo para todas las aplicaciones, no solo para las que usan el sistema de notificaciones de exposición.
>
> 3.2.- La versión 1.0 de la app "Radar COVID" (versión piloto) fue subida al repositorio Google Play el día 7 de agosto de 2020, posteriormente se han publi-

cado sucesivas actualizaciones (desde la 1.0.1 hasta la 1.0.7) hasta la versión 1.1 (a fecha de las comprobaciones realizadas por la inspección de datos) que se actualizó el 29 de octubre de 2020, en la que se han realizado las siguientes comprobaciones:

- En el repositorio de aplicaciones de GOOGLE consta que la app a la fecha del informe ha sido descargada por más de un millón de usuarios e incluye un enlace a la política de privacidad.

- Informa de los siguientes permisos solicitados por la App:

  - Ejecutar servicio en primer plano
  - Acceder a toda la red
  - Ver conexiones de red
  - Solicitar permiso para ignorar optimizaciones de la batería.
  - Evitar que el teléfono entre en modo suspensión
  - Enlazar con dispositivos bluetooth
  - Ejecutarse al inicio.

Tras instalar la aplicación se accede a la misma, verificando lo siguiente:

- La app no requiere registrarse como usuario, ni solicita datos de carácter personal. El único dato solicitado es el idioma.

- Informa de las funcionalidades de la aplicación, que funciona sin revelar la identidad del usuario ni del dispositivo. No recoge nombre, teléfono ni geolocalización y que en todo momento se pude dejar de utilizar.

- Incluye un enlace a la política de privacidad, debiendo aceptarla para continuar. Incluye un enlace a las condiciones de uso.

- Solicita permiso para activar exposición al COVID mediante la activación del bluetooth y para ignorar la optimización de la batería y mantener la ejecución en segundo plano de la app.

- Una vez finalizada la instalación, se muestra una ventana con información sobre contactos de riesgos tenidos y con dos botones, uno para activar y desactivar la app y otro para comunicar un positivo COVID-19.

- Pulsando el botón para comunicar un positivo, la app solicita la fecha de inicio de los síntomas o la fecha de la toma de la muestra o, si se desconoce dejarla en blanco y un código de 12 dígitos e informa de que la información se tratará siempre anónimamente.

Si se desactiva la antena GPS del terminal (geolocalización) el sistema operativo lanza la siguiente notificación: “notificación de exposición inactiva. Para utilizar esta función activa la ubicación”

Respecto a la App de APPLE

4.- Se han realizado las siguientes comprobaciones en un dispositivo iPhone SE, con versión software iOS 13.6.1.:

- En la actualización previa, iOS 13.5.1 y con motivo de la expansión de la COVID-19, se han incorporado APIs orientadas a intentar detener la propa-

gación que aprovechando las funcionalidades del teléfono a nivel de conectividad bluetooth.

- En el historial de versiones constan las versiones desde la 1.0 hasta la 1.08.

- Se ha procedido a la instalación de la app “RADAR COVID” en el dispositivo, realizándose las siguientes comprobaciones:

  - La app no requiere registrarse como usuario, ni solicita datos de carácter personal.
  - Informa de que la aplicación funciona sin revelar la identidad del usuario, y que en todo momento se pude dejar de utilizar.
  - Incluye un enlace a la política de privacidad, debiendo aceptarla para continuar. Incluye un enlace a las condiciones de uso.
  - Solicita permiso para activar exposición al COVID mediante la activación del bluetooth y para recibir notificaciones.
  - Una vez finalizada la instalación, se muestra una ventana con dos botones, uno para activar y desactivar la app y otro para comunicar un positivo COVID-19.
  - Pulsando el botón para comunicar un positivo, la app solicita la fecha de inicio de los síntomas o la fecha de la toma de la muestra o, si se desconoce dejarla en blanco y un código de 12 dígitos e informa de que la información se tratará siempre anónimamente.
  - En ningún momento se solicita activación del servicio de ubicación.

Respecto al protocolo DP-3T en el que se basa RADAR COVID 19:

5.- DP-3T es una colaboración de investigadores de toda Europa que unieron fuerzas para crear una solución técnica abierta al rastreo de proximidad para la epidemia COVID-19 atendiendo al respeto la privacidad personal. Han diseñado y desarrollamos sistemas de rastreo de proximidad con el objetivo de preservar la privacidad.

DP-3T ha hecho pública documentación técnica de este protocolo en el repositorio https://github.com/DP-3T/documents, la cual además es aportada por el inspeccionado como base de los desarrollos del sistema RADAR COVID 19, y del análisis de ésta, se destacan los siguientes puntos relevantes:

- El documento “*Decentralized Privacy-Preserving. Proximity Tracing .Overview of Data Protection and Security*” pone de manifiesto que en este sistema descentralizado hay cinco actores principales relevantes para la protección de datos: usuarios, autoridades sanitarias, un servidor back-end, proyectos de investigación epidemiológica y proveedores de sistemas operativos de telefonía móvil (en este caso, Apple y Google). Apple y Google solo proporcionan un servicio de notificaciones push, el mismo que para cualquier aplicación y son conscientes de que la aplicación se ha instalado, actuando como procesadores, pero no pueden ver ningún contenido o datos. El mismo documento pone de manifiesto que “*dado que Apple y Google proporcionan el sistema operativo que se ejecuta en dispositivos móviles, uno tiene que confiar en ellos, ya que potencialmente podrían tener conocimiento de información relacionada con el*

sistema de rastreo de proximidad (quién está infectado, quién infectó a quién, gráficos sociales, etc.)".

Además, el documento reseña que "*el sistema está diseñado de tal manera que ninguna entidad más allá del dispositivo de un usuario procesa o almacena datos personales identificables sobre el usuario. En su conjunto, el sistema cumple los objetivos de tratamiento que normalmente requerirían la transmisión de datos personales. Creemos que, en el marco del funcionamiento normal, ninguno de los datos utilizados para lograr el rastreo de proximidad debe caracterizarse como datos personales, ya que ningún actor titular de los datos tiene la capacidad de volver a identificarlos con medios razonablemente susceptibles de ser utilizados.*"

En cuanto a los identificadores, los teléfonos móviles con la aplicación de seguimiento de proximidad instalada emiten identificadores bluetooth efímeros (EfIDs) a través de Bluetooth de baja energía. Estos identificadores efímeros son generados pseudo-aleatoriamente por el teléfono, derivado de la clave secreta SK del propio teléfono.

- El documento "*Best Practices Operational Security for Proximity Tracing*" describe mecanismos de seguridad que se pueden agregar a las aplicaciones de seguimiento de proximidad para garantizar que las propiedades de seguridad y privacidad proporcionadas por los protocolos no se vean socavadas por otros componentes del sistema. De este documento se desprende lo siguiente:

"Hay que distinguir dos tipos de solicitudes al servidor: solicitudes no sensibles y confidenciales. En los sistemas de seguimiento de proximidad descentralizados, todos los usuarios recuperan regularmente nuevas claves de diagnóstico y configuraciones de aplicaciones potencialmente nuevas. Estas solicitudes no son sensibles. Todos los usuarios realizan estas solicitudes y, por lo tanto, los registros de estas no pueden revelar ninguna información confidencial sobre los usuarios, más allá del hecho de que estos usuarios utilizan una aplicación de seguimiento de proximidad. Las solicitudes realizadas por los usuarios relacionadas con la carga de claves de diagnóstico por parte de los usuarios positivos COVID-19 y las solicitudes para confirmar el estado de notificación de los usuarios expuestos son sensibles. Estas solicitudes deben ser tratadas con cuidado. "

El documento resalta como punto vulnerable del sistema las comunicaciones que se establecen entre los dispositivos y los servidores, las cuales incluyen metadatos.

El documento propone que las aplicaciones programen acciones falsas. Este mecanismo de protección funciona mediante (1) la producción de acciones falsas que son indistinguibles de las acciones reales y (2) la distribución de estas acciones falsas a lo largo del tiempo. Como resultado, cualquier acción observada podría, con una probabilidad razonable, ser una acción falsa.

El documento "*Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems",* también en referencia al tráfico de datos sobre pacientes infectados incide en que "C*ualquier sistema de rastreo de proximidad en el que las personas infectadas suban datos directamente desde su teléfono a un servidor central sin medidas, revela a un posible observador de la red que un paciente subió datos al servidor central.*

La mayoría de las propuestas para los sistemas de seguimiento de proximidad suponen que poco después de que un usuario de la aplicación reciba un resultado positivo de la prueba, cargará la información necesaria para desencadenar el seguimiento de contactos desde su dispositivo personal a un servidor central. Esto permite que un espía conectado a la red, por ejemplo, un curioso proveedor de servicios de Internet, proveedor de WiFi, sabría que se trata de un usuario infectado. También permite al servidor central obtener una pseudoidentición para la persona infectada.

Un proxy no ayuda a mitigar este ataque. Los usuarios pueden cargar regularmente paquetes ficticios, por ejemplo, mensajes vacíos del mismo tamaño que un informe real, al servidor. El servidor simplemente ignorará estos paquetes ficticios. Dado que los usuarios utilizan una conexión cifrada con el servidor, los observadores de red no pueden distinguir estos paquetes ficticios de las cargas reales, ocultando así su estado de infección incluso de los observadores de la red."

Esta vulnerabilidad fue corregida en la app Radar COVID y subida al repertorio Github el día 8 de octubre, para las siguientes versiones de la aplicación: Android, versión 1.0.7, Apple, versión 1.0.8

Respecto de las APIs de Apple y Google:

6.- Se ha hecho pública documentación técnica de esta interface en distintas webs de Apple y Google, la cual además ha sido aportada por el inspeccionado como base de los desarrollos del sistema RADAR COVID 19, y del análisis de ésta, se destacan los siguientes puntos relevantes:

- El documento "*Exposure Notification Bluetooth Specification"* provee la especificación técnica detallada para un nuevo protocolo Bluetooth que preserva la privacidad para apoyar la notificación de exposición. Resalta como requisito esencial en el diseño de esta especificación mantener la privacidad de los usuarios por los siguientes medios:

    - La especificación Bluetooth de notificación de exposición no utiliza la ubicación para la detección de proximidad. Utiliza estrictamente balizamiento Bluetooth para detectar la proximidad.

    - El identificador de proximidad de un usuario cambia en promedio cada 15 minutos y necesita que la clave de exposición temporal se correlacione con un contacto. Este comportamiento reduce el riesgo de pérdida de privacidad por la difusión de los identificadores.

    - Los identificadores de proximidad obtenidos de otros dispositivos se procesan exclusivamente en el dispositivo.

    - Los usuarios deciden si contribuyen a la notificación de exposición.

    - Si se diagnostica con COVID-19, los usuarios deben proporcionar su consentimiento para compartir claves de diagnóstico con el servidor. Los usuarios tienen transparencia en su participación en la notificación de exposición.

- El documento “Exposure Notification Cryptography Specification” provee la especificación técnica detallada para el cifrado del nuevo protocolo Bluetooth. Especifica las siguientes consideraciones de privacidad:

  - La programación de claves es fija y definida por los componentes del sistema operativo, lo que impide que las aplicaciones incluyan información estática o predecible que podría utilizarse para el seguimiento.

  - Se requiere una clave de exposición temporal para correlacionar entre los identificadores de proximidad cambiante de un usuario. Esto reduce el riesgo de pérdida de privacidad por la difusión de los identificadores.

  - Sin la publicación de las claves de exposición temporal, es computacionalmente inviable para un atacante encontrar una coincidencia/ correspondencia en un identificador de proximidad. Esto evita una amplia gama de ataques de repetición y suplantación.

  - Al informar de claves de diagnóstico, la correlación de los identificadores de proximidad por otros se limita a períodos de 24 horas debido al uso de claves de exposición temporal que cambian diariamente. El servidor no debe conservar los metadatos de los usuarios que cargan claves de diagnóstico después de incluir esas claves en la lista agregada de claves de diagnóstico por día.

7.- Otras consideraciones relevantes:

Informe de School of Computer Science & Statistics, Trinity College.

7.1.- En julio de 2020 el centro universitario “School of Computer Science & Statistics, Trinity College. Dublín” hizo público un informe en el que se analiza los datos reales transmitidos a los servidores back-end por las aplicaciones de rastreo de contactos implementadas en Alemania, Italia, Suiza, Austria, Dinamarca, España, Polonia, Letonia e Irlanda, así como los datos transmitidos por las APIs de GOOGLE y APPLE, con el fin de evaluar la privacidad de los usuarios.

Concluye el informe del Trinity College que analizados los datos transmitidos a los servidores back-end por las aplicaciones de rastreo de contactos implementadas en dichos países con el fin de evaluar la privacidad de los usuarios constan de dos componentes independientes: una aplicación "cliente" administrada por la autoridad nacional de salud pública y el servicio de notificación de exposición de Google/Apple, que en los dispositivos Android es administrado por Google y forma parte de Google Play Services. Las aplicaciones cliente de la autoridad de salud generalmente se comportan bien desde el punto de vista de la privacidad. Sin embargo, el componente de Google Play Services de estas aplicaciones es preocupante desde un punto de vista de privacidad. Google Play Services se pone en contacto con los servidores de Google aproximadamente cada 20 minutos, lo que permite potencialmente el seguimiento de la ubicación con productos precisos a través de la dirección IP. Además, los servicios de Google Play también comparten el IMEI del teléfono, el número de serie del hardware, el número de serie SIM, el número de teléfono del te-

léfono y la dirección de correo electrónico del usuario con Google, junto con los datos detallados en las aplicaciones que se ejecutan en el teléfono. Esta recopilación de datos se habilita simplemente habilitando los servicios de Google Play, incluso cuando todos los demás servicios y configuraciones de Google están deshabilitados.

Con motivo de este informe la Autoridad de Control Irlandesa ha interpelado a GOOGLE la cuestión del procesamiento de datos personales en el contexto del uso de la API, cuya respuesta ha sido compartida con todas las autoridades a través de IMI (Informal Consultation 141776).

En la respuesta dada, Google alega lo siguiente:

> *"Las métricas y la telemetría que cubre este informe describen una práctica de la industria para los sistemas operativos móviles (no solo en Android) que ayuda a garantizar que los dispositivos permanezcan actualizados, mantenga a las personas y los sistemas a salvo de los ataques y permita un funcionamiento fiable del ecosistema de dispositivos androides. Como se explica más adelante, no hay conexión entre las observaciones generales sobre la telemetría de Android en el informe y el uso de aplicaciones de notificación de exposición. Aunque siempre estamos abiertos a trabajar con la comunidad de investigación en mejoras generales para Android, estamos decepcionados con la forma en que los investigadores han intentado confundir la telemetría general de Android con las API de notificaciones de exposición.*
>
> *El Servicio de Configuración de Dispositivos Android envía periódicamente datos desde dispositivos Android a Google. Estos datos ayudan a Google a garantizar que el dispositivo esté actualizado y funcione lo mejor posible". Con el fin de garantizar el funcionamiento continuo de los dispositivos Android, este sistema procesa identificadores de dispositivos y cuentas, atributos de dispositivo, versiones de software y software de seguridad, conectividad de red y datos de rendimiento. Los propósitos de este procesamiento incluyen ayudar a garantizar que el dispositivo reciba actualizaciones de software y parches de seguridad, hacer que las aplicaciones y servicios funcionen de forma coherente en una amplia variedad de dispositivos Android con diferentes especificaciones y software, proteger el dispositivo y el sistema Android contra el fraude, el abuso y otros comportamientos dañinos, mantener métricas agregadas sobre dispositivos Android.*
>
> *No hay conexión entre las observaciones generales sobre la telemetría de Android y el Servicio de Configuración de Android en el informe de investigación y el uso de aplicaciones de notificación de exposición, excepto el uso de un dispositivo Android para cualquier propósito significa necesariamente cierta información es necesaria para operar el dispositivo. De acuerdo con nuestros compromisos de privacidad para las API de notificación de exposición, Apple y Google no reciben información sobre el usuario final, los datos de ubicación o información sobre cualquier otro dispositivo que el usuario haya estado cerca.*
>
> *Aparte del servicio de configuración de dispositivos Android, los datos de diagnóstico muy limitados y anónimos se recopilan de las API de notificaciones de exposición y esto se ha hecho transparente. Por ejemplo,*

Google ha publicado las especificaciones en el sitio para desarrolladores de Android. Por su parte, Google hace esto con el fin de verificar que la funcionalidad básica (es decir, el mecanismo de notificaciones de exposición) está funcionando y para proporcionar una señal de alerta temprana para investigar modelos de dispositivos específicos en caso de cualquier problema.

Por diseño, no se registra ninguna información de identificación del usuario del sistema de notificaciones de exposición ni en su funcionamiento ni en los datos de diagnóstico limitados recopilados de él. Mensajes de registro no identificados, recibidos en lotes agregados, que solo indican información sobre el funcionamiento del sistema, como si la funcionalidad BLE funciona. Este sistema de registro también interrumpe explícitamente cualquier vínculo entre los mensajes de registro del mismo dispositivo. Además, los identificadores como las direcciones IP necesarias para entregar el mensaje de registro no se registran en el disco de esta canalización de registro.

Hasta ahora, la información de diagnóstico ha ayudado a identificar los primeros problemas en las implementaciones de notificaciones de exposición en todo el mundo. Por ejemplo, ayudó a identificar modelos de dispositivos que no admitieran la versión inicial de las notificaciones de exposición y a desarrollar trabajos para garantizar una amplia disponibilidad. Sin esta información, no habríamos podido tener una respuesta rápida y contundente a esta urgente pandemia mundial."

7.2.- El día 9 de septiembre de 2020 la Secretaría de Estado de Digitalización e Inteligencia Artificial publicó el código fuente de la App en el repositorio Github.com, en el que se pudo observar que en las líneas 198-199 aparece un comentario recomendando el uso de la librería de desarrollo Firebase para Google Analytics. En respuesta al requerimiento de la Inspección de Datos a este respecto, el representante de la Secretaría General de Administración Digital aporte un informe en el que se pone de manifiesto lo siguiente:

"*Las librerías de software Firebase de Google fueron utilizadas en la fase piloto como consecuencia del reporte de incidencias ANR (aplicación no responde) en los dispositivos móviles, sobre incidentes no reportados o errores que no son visibles para el usuario, pero que pueden afectar al correcto funcionamiento de la aplicación.*

…

Esta funcionalidad sólo se ha utilizado en la fase piloto no estando en uso en las versiones en producción actualmente como puede verse en el análisis del código fuente publicado en el repositorio github."

7.3.- Con fecha 30 de septiembre de 2020 tuvo entrada en la AEPD un correo electrónico suscrito por 11 docentes de distintas universidades comunicando una vulnerabilidad de la app RADAR COVID (…). El correo incluye un informe técnico y una valoración jurídica.

Según dicho informe, sólo los usuarios positivos de COVID suben las claves TEK claves con el resultado de un test al servidor de radar-covid-backenddp3t-server. Por lo tanto, cada vez que se observa una subida de la clave desde un teléfono a este servidor, se puede inferir que el propietario del teléfono es CO-

VID-positivo. La encriptación entre la aplicación y el servidor no ayuda a encubrir esa información: incluso si el endpoint y el contenido de la subida no son observables, la longitud de los mensajes revelará una subida de la clave TEK al servidor. La comunicación puede ser observada por diversas entidades. Por ejemplo, el proveedor de telecomunicaciones (si la conexión se hace a través de GSM); el proveedor de servicios de Internet si la conexión se hace a través de Internet; o cualquier persona con acceso a la misma red (WiFi o Ethernet) que el usuario. En el caso de la app Radar COVID, en la que las subidas se hacen utilizando el endpoint de Cloudfront que se utiliza para la descarga de las claves TEKs, Amazon también tiene la capacidad de observar las direcciones IP de los usuarios de Radar COVID y asociarlas al hecho de que esos usuarios comunican un test de COVID positivo. Pero, además del hecho de comunicar la dirección IP, habida cuenta de que, como se muestra en el informe técnico, sólo los usuarios positivos de COVID suben las claves al servidor de radar-covid-backend-dp3t-server, esa IP queda asociada a los datos de claves TEK subidos, que corresponden siempre a la comunicación de un test positivo de COVID. De este modo, el funcionamiento de la app permite vincular de modo inequívoco una IP con el hecho de que su titular está subiendo un test positivo de COVID.

Con fecha 2 de octubre de 2020 la inspección de datos solicita información al respecto a la SEDIA y con fecha 7 y 27 de octubre de 2020 tienen entrada sendos escritos de respuesta en el que se pone de manifiesto lo siguiente:

> Esta vulnerabilidad ya era conocida por el equipo de desarrollo de Radar COVID, ya que figuraba al menos en un documento técnico publicado en abril de 2020 por el equipo DP-3T: Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems.
>
> No obstante, el equipo de desarrollo no consideró necesario resolver este problema en las primeras versiones de Radar COVID dado que, para explotar esta vulnerabilidad, se debe presuponer un remoto escenario donde el operador de telecomunicaciones está interesado en obtener esta información clínica de sus clientes estudiando el tráfico de datos generado por las apps Radar COVID.
>
> Número de identificadores que se han visto afectados por la vulnerabilidad:
>
> La aplicación Radar COVID se puso en servicio a nivel nacional el 19 de agosto de 2020.
>
> La vulnerabilidad fue corregida en la subida correspondiente al 8 de octubre, para las siguientes versiones de la aplicación: Android, versión 1.0.7, Apple, versión 1.0.8.
>
> A fecha de 8 de octubre, se habían declarado un total de 3.059 códigos a nivel nacional.
>
> Acciones realizadas para su resolución:
>
> El código del sistema Radar COVID se publicó en abierto el pasado 9 de septiembre de 2020, para conocimiento general, lo que ha permitido que numerosos expertos en desarrollo, privacidad, protección de datos y ciberseguridad pudieran tener acceso al mismo.

A raíz de esta publicación y su posterior análisis, una serie de expertos en privacidad se pusieron en contacto con el equipo de soporte de Radar COVID a mediados de septiembre para informar sobre la vulnerabilidad anteriormente descrita. Esta vulnerabilidad ha sido documentada por el equipo DP-3T como NR-2 (traffic analysis reveals data about infected patients) en su informe “Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems”.

La solución al problema, ya documentada en el documento mencionado, consiste en que todas las aplicaciones Radar COVID generen tráfico aleatorio con el mismo patrón de interacción con el servidor (tamaño de paquetes, flujo de envío/repuesta, y tiempos de procesamiento) que las declaraciones de positivo. De esta manera, se hace indistinguible el tráfico real del simulado.

A raíz de tener conocimiento de esta vulnerabilidad, el equipo de Radar COVID implementó un algoritmo mediante el cual todas las aplicaciones realizan periódicamente envío de tramas de datos ficticios (tramas fake). Estas tramas son indistinguibles de las tramas reales, tanto en volumen de información transmitida: se hace padding con claves fake hasta completar tramas con 30 claves en total; como en tiempo de procesamiento en el servidor: dado que el tiempo de procesado de las tramas fake en servidor sería inferior porque se descartan sin almacenar en BBDD, se incluye una espera artificial hasta completar 2 segundos de procesamiento en servidor, que se corresponde con el tiempo medio de procesamiento de positivos reales.

El tráfico ficticio se implementa usando una función al efecto en los dispositivos móviles, tanto Android como iOS. De la misma manera, se implementa en el backend una funcionalidad complementaria, identificando esas tramas falsas que se han generado y descartando su contenido.

La aleatoriedad de estas comunicaciones se ha implementado inicialmente siguiendo una distribución uniforme, remitiendo tramas con un intervalo promedio en torno a las 3 horas.

Con posterioridad, el equipo DP-3T ha sugerido que el tráfico falso esté sujeto a una función exponencial, con un promedio de una remisión cada cinco días, lo que introduce latencias de tiempo aleatorio entre las diferentes tramas generadas, que hacen que el tráfico sea virtualmente imposible de distinguir con los envíos reales.

Se ha mantenido un intercambio de correos y una videoconferencia entre el equipo Radar COVID y el equipo DP-3T a lo largo del mes de octubre, y finalmente se aceptó la propuesta de cambiar la distribución uniforme a una distribución exponencial. Este cambio se va a incorporar en una nueva versión del sistema que se liberará previsiblemente el viernes 30 de octubre de 2020, junto con otras funcionalidades.

<u>Respecto a la utilización por terceros de los datos expuestos:</u>

Manifiestan que al equipo de Radar COVID no le consta de ninguna utilización por terceros de los datos expuestos.

Se ha verificado por la inspección de datos que la versión 1.0.7 de la app Radar COVID subida a Google play el 8 de octubre de 2020 informa, entre las novedades, la inclusión de envío de comunicaciones de positivos fake. Se ha verificado que la versión 1.1.0 ha sido subida al repositorio de Google el día 29 de octubre de 2020.

También se ha verificado que la publicación de los componentes del software ha sido actualizada en distintas ocasiones en https://github.com/radarcovid en varias fechas desde el 8 y el 4 de noviembre de 2020."

OCTAVO: Con fecha 21 de mayo de 2021 la directora de la AEPD acordó iniciar procedimiento sancionador a la SEDIA, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), por presunta infracción de los siguientes artículos del RGPD: 5.1.a); 5.2; 12; 13; 25; 28.1, 28.3 y 28.10; y 35, tipificadas en los artículos 83.4.a) y 83.5.a) y b) del RGPD.

NOVENO: Con fecha 7 de junio de 2021 la SEDIA presenta un escrito a través del cual solicita la ampliación del plazo para aducir alegaciones y aportar documentos u otros elementos de juicio, y además, la remisión del expediente sancionador.

DÉCIMO: Con fecha 8 de junio de 2021 el órgano instructor acuerda la ampliación de plazo instada hasta un máximo de cinco días y con fecha 11 de junio de 2021 la remisión de la copia del expediente, de acuerdo con lo dispuesto en los artículos 32.1 y 53.1 a) de la LPACAP.

El acuerdo de ampliación se notifica en fecha 8 de junio de 2021, a través de Carpeta Ciudadana.

La remisión de la copia del expediente se produce en fecha 14 de junio de 2021, vía mensajero, según certificado de entrega que consta en el expediente.

UNDÉCIMO: Con fecha 15 de junio de 2021 se presenta, en tiempo y forma, escrito en el que aduce alegaciones y manifiesta lo que a su derecho conviene:

En síntesis manifiesta que:

ALEGACIONES DE CARÁCTER GENERAL:

El proyecto de construcción de la solución nacional de rastreo de contactos, Radar COVID, ha sido muy exigente por los muy estrechos plazos de tiempo manejados (lo que impuso realizar contrataciones por trámite de emergencia), por las dificultades tecnológicas inherentes, y por la complejidad de interoperar con los 19 sistemas sanitarios de las Comunidades y Ciudades Autónomas, como con otros países de nuestro entorno, a través del nodo de interoperabilidad de la Comisión Europea.

A pesar de estas dificultades, fue desarrollada con gran rapidez, con solvencia técnica y epidemiológica, y con las máximas garantías de protección de datos, utilizando el protocolo más garante con la privacidad (DP3-T), que recoge consideraciones estrictas de privacidad por diseño, este protocolo es el utilizado por una mayoría de países en la implementación de este tipo de aplicaciones.

Dada la premura de plazos, se implantó un sistema de trabajo de reuniones semanales con todos los agentes implicados

- El Ministerio de Sanidad (en lo sucesivo, MSND) y la Comunidad Canaria, participando en todas las reuniones del piloto e implicándose en todas las decisiones estratégicas que se tomaron para su desarrollo, ejecución y evaluación.

- El MSND, presente en todas estas reuniones, liderando la ejecución de los trabajos, como no podía ser de otra forma al ser el responsable del Sistema Nacional de Salud y dando las indicaciones precisas en todo el proceso de evolución de la aplicación desde el piloto, pasando por la fase de pruebas hasta la consolidación de la app.

- La SGAD, ejecutando los desarrollos tecnológicos e impulsando el uso de la aplicación para conseguir una mayor efectividad de esta, siempre contando con la cobertura necesaria para hacerlo, y con un mandato específico en cada caso del MSND como autoridad sanitaria del país:

  o Carta de la Directora de Salud Pública para el piloto.

  o Acuerdo del Consejo Interterritorial del Sistema Nacional de Salud para el uso en pruebas de Radar COVID.

  o Acuerdo de 13 de octubre para el uso definitivo de la aplicación y firma de los correspondientes convenios.

Correspondiéndole a la SGAD en todos los casos, el rol de Encargado de tratamiento, que es el que ha ejercido en todo el desarrollo y evolución de la aplicación.

También que se ha incorporado al equipo de Radar COVID técnicos expertos en accesibilidad provenientes de la Fundación ONCE y CERMI para dotar aún de más transparencia todos los procesos llevados a cabo para la mejora de la accesibilidad de la aplicación y como validadores externos de la misma.

Se han tomado medidas de transparencia, poco habituales, en la Administración Pública española como la publicación del Análisis de Riesgos, y la Evaluación de Impacto, así como del código fuente de la aplicación para general escrutinio de profesionales y expertos en privacidad, seguridad y protección de datos.

El documento de Evaluación de Impacto, además, ha sido analizado por el grupo eHealth de la Unión Europea, dando fe de la privacidad de la aplicación y de la no recogida de ningún dato personal o que permita identificar al usuario.

Además, se han atendido las peticiones y dudas que los analistas o técnicos, han planteado sobre el código fuente publicado en Github.

Se han respondido multitud de preguntas parlamentarias, preguntas del Defensor del Pueblo, consultas por derecho de acceso en virtud a la Ley de Transparencia, miles de preguntas de usuarios de la aplicación, etc.

Desafortunadamente el inicio de actuaciones previas de investigación por parte de la AEPD el 21 de mayo de 2020 no ha permitido el intercambio de información.

La SGAD ha actuado en todo momento respetando las indicaciones dadas por el MSND, actuando siempre en línea y con los requisitos establecidos en las iniciativas europeas en esa materia, e intentando, en el ejercicio de sus competencias, y de acuerdo con el rol asignado, dar respuesta a las exigencias que en ese momento demandaba la ciudadanía actuando, dentro de la urgencia que han requerido los trabajos durante la situación de emergencia, con respeto pleno a todas las exigencias legales requeridas.

ALEGACIONES ESPECÍFICAS:

RESPECTO A LAS PETICIONES DE INFORMACIÓN DE LA AEPD

El inicio de actuaciones de investigación por parte de la AEPD, coincidió en el tiempo con el anuncio del proyecto piloto de rastreo de contactos en la Gomera, en un momento en el que aún no estaba ni constituido el equipo de trabajo del proyecto Radar COVID, y por tanto tampoco estaba iniciado el proyecto, en sentido estricto.

Por ello, los primeros requerimientos de información que solicitaba la AEPD hacían referencia a documentos que no estaban disponibles simplemente porque no existían todavía, ya que no eran necesarios al tratarse de datos ficticios.

El contrato de emergencia celebrado entre la SGAD e INDRA tiene su inicio a 15 de junio de 2020.

A la vista de las alegaciones de la SGAD en respuesta a los requerimientos de la AEPD, con fecha 26 de febrero de 2021, la SGID emitió un informe de actuaciones previas de investigación.

En este informe se investiga a: SEDIA, y a la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud del MSND.

No se investiga a las autoridades sanitarias de las Comunidades Autónomas, aun cuando el Acuerdo del 19 de agosto de 2020 del Consejo Interterritorial de Salud sobre el uso de la aplicación Radar Covid, en fase de pruebas, por parte de las Comunidades y Ciudades Autónomas, señala su competencia como responsable del tratamiento de datos en su respectivo territorio.

Igualmente del texto de los Convenios firmados entre la SGAD y las Consejerías de Salud de diferentes Comunidades Autónomas se desprende que estas últimas tienen una corresponsabilidad en el tratamiento de datos, en particular los relativos al rastreo de contactos automatizado, como es la gestión de los códigos de confirmación de positivo.

RESPECTO A LOS TRATAMIENTO DE DATOS PERSONALES

La aplicación Radar COVID efectúa cierto tratamiento de datos, tales como: identificadores efímeros (datos seudonimizados) o código de 12 dígitos de declaración de posi-

tivo.

Es una aplicación que sigue el protocolo DP3-T, de protección de la privacidad por diseño, utilizando el sistema de notificación de exposiciones que Apple y Google anunciaron el 10 de abril de 2020, y empleado en 19 países de la Unión Europea para construir sus aplicaciones de rastreo de contactos.

Por ello, se alegó inicialmente que no había tratamiento de datos personales.

También es preciso recordar que la aplicación no realiza un registro de usuarios, ni obtiene información del dispositivo móvil, ni geolocaliza, ni recoge la dirección IP del dispositivo móvil. Solo precisa de comunicaciones bluetooth para intercambiar códigos aleatorios (identificadores bluetooth efímeros) que no revelan la identidad del usuario de la aplicación y que son siempre entre dos terminales móviles y con el previo consentimiento del usuario.

En todo caso, la SGAD remitió, en su momento, las condiciones de uso y política de privacidad de la aplicación a la AEPD, solicitando que se revisaran y se aportaran observaciones. Dado que la Agencia ya estaba actuando en el procedimiento de actuaciones previas, no hubo posibilidad de tal informe, situación que ha continuado en el tiempo hasta ahora.

Adicionalmente, en el periodo, del 29 de junio al 29 de julio, la aplicación estuvo operativa para un piloto de simulación de pandemia en la isla de la Gomera. Los datos relativos a declaración de casos positivos por COVID-19 eran completamente simulados, como lo demuestran las condiciones de uso y política de privacidad de aquel momento.

En un momento posterior, se actualiza la política de privacidad para recoger los tratamientos de datos en relación con:

1. Claves de exposición temporal.

2. Códigos de 12 dígitos para declaración de positivos.

3. Consentimiento del usuario para remisión de claves.

Hay otros datos, como las direcciones IP, que aunque se pueden llegar a obtener, no se procesan. Esto se indica expresamente en la política de privacidad.

Finalmente se indica que la aplicación no realiza un registro de usuarios, ni obtiene información del dispositivo móvil.

No obstante todo lo anterior, no se descarta que en el futuro se puedan realizar, por los Organismos competentes, análisis de datos agregados sobre volumen de descargas de la aplicación, volumen de usuarios contagiados, u otros indicadores anónimos y agregados, para proyectos de investigación científica, cumpliendo siempre la normativa de protección de datos.

Señalar, por último, en este apartado, que respecto al tratamiento de datos de la app,

no se ha recibido ningún aviso, por su hipotético mal uso, de los Delegados de Protección de Datos de los Ministerios de Sanidad, y de Asuntos Económicos y Transformación Digital.

RESPECTO AL ROL DE LA SGAD EN EL TRATAMIENTO DE DATOS

Por razones de claridad, conviene distinguir dos etapas:

1º. La etapa en la que se hace el proyecto piloto la SEDIA fue autorizada a fecha 9 de junio de 2020 por la DGSP del MSND a conducir un proyecto piloto en la isla de la Gomera, lo que permitió la realización del correspondiente expediente de contratación.

La contratación recogía el diseño, construcción de la aplicación, la consecución de un piloto, y la evaluación de este, así como adaptaciones de la aplicación en función de los resultados del piloto. El contrato se realizó con una duración de cinco meses, hasta el 14 de noviembre de 2020

En su autorización la DGSP establece el 9 de junio de 2020 que: *el responsable del tratamiento de los datos de este piloto será la autoridad sanitaria de la Comunidad en que se va a llevar a cabo.*

Quedando la SEDIA como encargada del tratamiento de los datos y resultados.

La DGSP participó en las reuniones semanales del piloto, para la conformación de los fines y medios del proyecto. En particular, D, X.X.X., Director del Centro de Coordinación y Alertas Sanitarias, así como personal de su unidad, formaron parte del seguimiento semanal. Así mismo formaron parte del comité de seguimiento autoridades sanitarias del Gobierno de Canarias, y responsables del área de Modernización Digital.

En todo caso, los datos que se manejaron en el piloto realizado entre los meses de junio y julio de 2020 solo manejaban datos simulados de infección, no poniéndose en compromiso ningún dato personal, ni mucho menos relacionado con la salud de los participantes en el piloto. El equipo del proyecto, junto con expertos independientes han publicado un artículo de los trabajos realizados en San Sebastián de la Gomera en la revista Nature Communications, dando idea de la utilidad de esta herramienta a efetos de cortar cadenas de transmisión del virus: “A population-based controlled experiment assessing the epidemiological impact of digital contact tracing”, ver https://www.nature.com/articles/s41467-020-20817-6

2º.- La etapa en la que se pone en marcha la aplicación en fase de pruebas y posteriormente la aplicación definitiva.

El Acuerdo adoptado el 19 de agosto de 2020 en el Consejo Interterritorial del Sistema Nacional de Salud, señalaba que:

> *“durante la vigencia de este Acuerdo, el responsable del tratamiento será el MSND y, en su respectivo territorio, cada una de las Comunidades y Ciudades Autónomas que se vayan incorporando durante la fase de pruebas al uso de la aplicación, ostentando plenamente sus competencias en materia sanitaria. El encargado del tratamiento será, en ambos casos, la Secretaría de Estado de*

Digitalización e Inteligencia Artificial."

Este Acuerdo permite que las CC.AA. puedan asumir temporalmente, hasta la firma de los citados convenios, la gestión de los códigos de diagnóstico positivo que se asignen a aquellos ciudadanos con una prueba PCR positiva.

Posteriormente se publicó en BOE la "Resolución de 13 de octubre de 2020, de la Subsecretaría, por la que se publica el Acuerdo entre el Ministerio de Asuntos Económicos y Transformación Digital y el Ministerio de Sanidad", acerca de la aplicación Radar COVID."

En este Acuerdo se faculta a la SGAD para la subscripción de Convenios con Comunidades y Ciudades Autónomas, especificando que: "*en los mencionados Convenios de colaboración, el Ministerio de Sanidad y la Consejería competente en materia de sanidad de la Comunidad o Ciudad Autónoma de que se trate figurarán como responsables del tratamiento de datos de carácter personal y la SGAD como encargado del tratamiento."*

En los diferentes Convenios, que cuentan con todas las autorizaciones legamente exigibles, celebrados entre el MSND y las Comunidades Autónomas se ha señalado reiteradamente que:

> "*la Consejería de Salud es Responsable del Tratamiento de datos de la aplicación Radar COVID. En dicha condición le corresponden, entre otras, las siguientes actividades de tratamiento:*
>
> *a) Solicitar a la SGAD, según se requieran, los códigos de confirmación de positivo por prueba.*
>
> *b) Facilitar los códigos de confirmación anteriores a los usuarios con un diagnóstico positivo".*
>
> *Correspondiendo a la SGAD entre otras funciones la de……."h) Cumplir con los cometidos como encargada del tratamiento indicados por el Ministerio de Sanidad como responsable del mismo".*

Por tanto queda plenamente acreditado que en todo momento la SGAD actuó y actúa única y exclusivamente como encargada del tratamiento, mientras el MSND y Comunidades Autónomas eran y son las responsables de dicho tratamiento.

Hay que remarcar que en ningún momento el MSND ha incumplido sus obligaciones en el proyecto Radar COVID, y ha facilitado directrices, como por ejemplo las recogidas en el documento técnico: "Procedimiento de implementación de la App Radar COVID como complemento a los sistemas manuales de identificación de contactos", coordinado por el Centro de Coordinación de Alertas y Emergencias Sanitarias, Dirección General de Salud Pública, Calidad e Innovación y aprobado por la Ponencia de Alertas y Planes de Preparación y Respuesta.

Además, tal como se ha visto en las alegaciones de carácter general, en todo momento tanto en el desarrollo del piloto, como en el uso de Radar COVID en pruebas, como

en el Acuerdo de 13 de octubre estaban definidos los roles de responsable de tratamiento y de encargado de tratamiento, por lo que no pueden existir dudas de la legitimación que cada uno tenía en el desarrollo de la aplicación.

Asimismo, resulta llamativa la referencia al MSND de la página 84 del Acuerdo de inicio de Procedimiento sancionador: “Si el Ministerio de Sanidad hubiese querido encomendar a la SEDIA el desarrollo de la App Radar COVID, hubiera mostrado su voluntad inequívocamente. Y lo hubiera realizado de igual forma que el resto de las encomiendas. Sin embargo, este hecho no se produjo.”

Esa afirmación no toma en consideración que la encomienda, artículo 11 de la Ley 40/15 no puede afectar a la competencia ni a su ejercicio, dado que el Ministerio y la SEDIA pueden relacionarse mediante cualquier otro instrumento o medio permitido por la normativa vigente en aras del interés público, artículo 9 de la citada ley que permite delegar su ejercicio.

RESPECTO AL ROL DE INDRA

1.- Señala la AEPD que “no se justifica por qué INDRA ofrece garantías suficientes como encargado del tratamiento”:

En ningún momento, el pliego de condiciones para el diseño, desarrollo, piloto y evaluación de un sistema que permita el rastreo de contactos en relación con la pandemia ocasionada por la Covid-19 indica que INDRA sea la encargada del tratamiento, tal rol siempre lo ha jugado la SGAD.

Hay que recordar que en la Memoria justificativa del expediente de contratación se aportaba una justificación de la conveniencia de la contratación a INDRA por su experiencia en proyectos tecnológicos.

En concreto, se cita:

> “*Para llevar a cabo de forma inmediata el desarrollo de este Sistema se precisará de un equipo multidisciplinar, que recoja perfiles con conocimiento funcional sobre rastreo de contactos, arquitectos de soluciones móviles, especialistas en experiencia de usuario, técnicos de pruebas y ciberseguridad. Se ha considerado que la empresa INDRA SOLUCIONES TECNOLOGÍAS DE LA INFORMACIÓN, S.L.U., que destaca por su amplia experiencia en todo tipo de proyectos tecnológicos, así como en el diseño de soluciones móviles en relación con la crisis sanitaria de la COVID-19 (COVID MONITOR, App C19-Pass), está preparada técnica y organizativamente para realizar este proyecto y dispone de la capacidad de reunir un equipo con los perfiles exigidos de forma inmediata con el fin de poder efectuar las tareas y acciones para alcanzar los objetivos del proyecto de desarrollo*.”

INDRA es una empresa multinacional, de amplísima experiencia en proyectos con el Sector Público, y reúne garantías suficientes para satisfacer el objeto del contrato. De hecho, INDRA se somete periódicamente a auditorías independientes para la certificación de sus sistemas de gestión y producción de acuerdo con los principales estándares internacionales, entre los que se encuentran los recogidos en el Anexo I.

2.- Por otra parte, la AEPD señala en su informe que *"si (La SEDIA) hubiera actuado en la condición de encargado del tratamiento […] debería haber requerido al responsable del tratamiento la autorización previa que exige el RGPD por escrito, antes de recurrir a otro encargado (INDRA) para desarrollar el servicio encomendado".*

Por una parte, la SEDIA siempre ha actuado en calidad de encargado del tratamiento.

La contratación a favor de INDRA recoge en el clausulado deberes en materia de protección de datos personales:

> *"Se deberá cumplir lo estipulado en la ley orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, adaptada al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y por el que se deroga la Directiva 95/46/CE(Reglamento General de Protección de Datos), incluyendo lo dispuesto en la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre y en el Real Decreto 3/2010, de 8 de enero. Conforme a la Disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Medidas de seguridad en el ámbito del sector público, las medidas de seguridad a aplicar en el marco de los tratamientos de datos personales se corresponderán con las de la Administración púbica de origen y se ajustarán al Esquema Nacional de Seguridad.*
>
> *Se requerirá a INDRA SOLUCIONES TECNOLOGÍAS DE LA INFORMACIÓN, S.L.U. la manifestación expresa del sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos conforme a los artículos 35.1d y 122.2 de la LCSP modificado por artículo 5 del Real Decreto Ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones."*

Y en todo caso, la SGAD informó al MSND sobre la contratación de los desarrollos y la operación del sistema a la empresa INDRA, y el MSND por tanto era conocedor desde el primer momento de esta contratación y no puso ninguna objeción.

RESPECTO A LA EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS.

En primer lugar, cabe mencionar que si bien la EIPD publicada en septiembre 2020 fue la versión 1.1, ya existía una versión 1.0 del EIPD con anterioridad al 19 de agosto de 2020. La EIPD facilitada a la AEPD fue la versión 1.1 pues es la que se publicó, coincidiendo con el despliegue en septiembre 2020 de una versión de la aplicación, con soporte de lenguas cooficiales.

Durante el periodo que va del 19 de agosto hasta la publicación en septiembre 2020, se debatió internamente sobre la conveniencia o no de la publicación de dicho documento.

El ruego encarecido del Comité Europeo de Protección de Datos (en lo sucesivo, CEPD) no constituye por sí mismo una obligación de publicación de esta información,

aunque sí constituye una fuerte recomendación. De hecho, la Administración General del Estado (en lo sucesivo, AGE), que es la persona jurídica única, que ostenta la condición de responsable y de encargado del tratamiento a través de órganos distintos, no viene publicando, ni la EIPD, ni los Análisis de Riesgos sobre las que se basan.

La SGAD recabó criterio al delegado de protección de datos del METD. Su criterio fue que, con carácter general, no debían publicarse estos documentos.

En todo caso, finalmente se siguió la recomendación del CEPD, y se procedió a publicar la EIPD y el Análisis de Riesgos previo en septiembre de 2020.

RESPECTO A LAS CONDICIONES DE USO Y POLÍTICA DE PRIVACIDAD

1.- Indica la AEPD en su informe que:

> *"En la primera versión de la App prevista para el Programa Piloto en la isla de la Gomera (julio 2020) se recogía en dos documentos distintos la información relativa a la privacidad.[..] Sin embargo, ninguno de ellos definía quién era el responsable o encargado del tratamiento"*

Hay que recordar que la primera versión de la App (piloto) sirvió a efectos de comprobar
aspectos como la usabilidad, percepción de privacidad, y eficacia de la solución en un entorno simulado. En ningún caso se manejaban datos de salud de los participantes en el piloto.

Y la política de privacidad incluía el siguiente aviso:

> *"El USUARIO de esta aplicación queda avisado de que al descargar la aplicación en su dispositivo móvil y utilizarla, se está limitando a participar voluntariamente en una EXPERIENCIA PILOTO CON DATOS FICTICIOS de alerta de contagios de la COVID-19 en LA ISLA DE LA GOMERA.*
>
> *Se informa asimismo de que esta aplicación dejará de funcionar una vez que termine la experiencia piloto.*
>
> *Por tanto, en el uso de la aplicación, todas las notificaciones de exposiciones a posible contagio de la enfermedad que el usuario pueda recibir corresponden a supuestos simulados y, por el mismo motivo, al tratarse de una experiencia piloto con datos ficticios, las sugerencias de adopción de medidas preventivas y asistenciales que tras esa notificación le facilite la aplicación no tienen otro valor que comprobar que la aplicación es capaz de facilitar sugerencias de ese tipo a un usuario que recibiera una notificación de exposición a posible contagio"*

2.- En la pág. 110 del acuerdo se indica que: "*Por otra parte se han producido diversas revisiones en las 'Condiciones de uso' y 'política de privacidad' existentes".*

El equipo de Radar COVID, ha ido revisando y actualizando los documentos con el ánimo de mejorar su contenido y facilitar su lectura y comprensión. Adicionalmente, se

han incorporado cuestiones adicionales como la interoperabilidad europea.

Con cada actualización del aplicativo, si existía cambio en las condiciones de uso y política de privacidad, se solicitaba de nuevo consentimiento expreso por parte de los usuarios.

3.- En la pág. 111 se menciona que *"No queda claro quién es el responsable del tratamiento ni tampoco los datos del DPD, que ni siquiera se mencionan en la política de privacidad*".

La política de privacidad actual (https://radarcovid.gob.es/politica-de-privacidad) establece como responsables del tratamiento al MSND y Comunidades Autónomas, y como encargado del tratamiento a la Secretaría General de Administración Digital.

4.- Respecto al incremento de 700 palabras en la política de privacidad, la SGAD ha ido revisando los documentos con el ánimo de mejorar su contenido y facilitar su lectura y comprensión. Se corresponde con explicaciones más extensas de los apartados de privacidad, así como la ampliación a nuevos usos de la aplicación, como la interoperabilidad con las aplicaciones de rastreo de contactos de la Unión Europea.

Las nuevas funcionalidades (como la conexión de Radar COVID al nodo europeo de interoperabilidad) ha conllevado la actualización de las condiciones de uso y política de privacidad, a fin de aportar transparencia e información a las personas usuarias de la aplicación.

5.- Respecto a la información indicada en los términos que establecen los artículos 12 y 13 del RGPD:

Las condiciones de uso y política de privacidad han estado siempre accesibles para los interesados, tanto desde la aplicación móvil, como desde la web http://radarcovid.-gob.es.

Por ende, es necesario el consentimiento expreso a estos dos documentos para poder utilizar la aplicación. En el tiempo que la aplicación está operativa, la SEDIA no ha recibido ninguna queja del Delegado de Protección de Datos del MSND en relación a la aplicación Radar COVID.

6.- Sobre la información relativa al responsable, destinatarios o los derechos de los artículos 15 a 22:

Solo recordar que en la política de privacidad se dan enlaces tanto a un formulario de la AEPD para el ejercicio de derechos, como a un enlace del MSND, para contactar con el Delegado de Protección de Datos.

RESPECTO A LA VULNERABILIDAD DETECTADA (RECLAMACIONES 2 y 3)

La vulnerabilidad reportada por un conjunto de expertos en privacidad fue recibida a mediados de septiembre de 2020. La vulnerabilidad fue analizada y se programó una corrección coincidiendo con una próxima liberación de la aplicación. Fue corregida el 8 de octubre de 2020, y compartido el código que corregía el problema con el equipo

técnico de la Escuela Politécnica Federal de Lausana (EPFL), que es quien había impulsado el protocolo DP3-T, garante de la privacidad.

Asimismo, no se ha detectado ni se tiene constancia de que esta teórica vulnerabilidad haya sido explotada o aprovechada en ningún caso real, seguramente por la dificultad y poco beneficio que se obtendría de su implantación.

No existe ningún sistema 100% seguro, y se optó por continuar, ya que la alternativa era paralizar el uso y desarrollo de la app con el consiguiente riesgo en pleno estado de alarma por emergencia sanitaria.

RESPECTO A LAS FUENTES DOCUMENTALES USADAS POR LA AEPD

Las notas de prensa tienen un valor meramente informativo de una actuación pública y no atributivo de ninguna competencia, reservada esta facultad atributiva a las normas y actos mencionados en las alegaciones previas de este documento.

Por tanto, consideramos que no se les puede dar el valor de lo descrito en el ACUERDO DE USO DE LA APLICACIÓN “RADAR COVID”, EN FASE DE PRUEBAS, POR PARTE DE LAS COMUNIDADES Y CIUDADES AUTÓNOMAS del Consejo Interterritorial del Sistema Nacional de Salud (19 de agosto 2020), la Resolución de 13 de octubre de 2020, de la Subsecretaría, por la que se publica el Acuerdo entre el Ministerio de Asuntos Económicos y Transformación Digital y el MSND, acerca de la aplicación "Radar COVID (BOE de 15 de octubre) o los diferentes Convenios firmados entre la SGAD y las CCAA´s y publicados en el BOE.

En todos ellos se recoge el rol de la SEDIA: El encargado del tratamiento será, la Secretaría de Estado de Digitalización e Inteligencia Artificial.

CONCLUSIÓN

La SGAD estima que no ha habido infracción de los preceptos mencionados en el apartado PRIMERO del ACUERDO DE INICIO DE PROCEDIMIENTO SANCIONADOR, y por tanto no procede el inicio de este procedimiento.

Por otra parte, si de la resolución se derivan medidas que hubiere que adoptar para el mejor cumplimiento de la normativa de protección de datos, existe una férrea voluntad por parte de la SGAD para proceder en ese sentido, siguiendo, en todo caso, las directrices y pautas de la AEPD.

Estas alegaciones ya fueron contestadas en la propuesta de resolución y se reiteran, en parte, en los Fundamentos de Derecho (en lo sucesivo, FD) de esta Resolución.

DUODÉCIMO: Con fecha 22 de septiembre de 2021 la instructora del procedimiento acordó practicar las siguientes pruebas:

1. Se dan por reproducidas a efectos probatorios las reclamaciones interpuestas por una ***C.C.C.***, ***A.A.A.***, ***B.B.B.*** y RIGHTS INTERNATIONAL SPAIN, y la documentación que a ellas acompaña.
2. Los documentos obtenidos y generados por los Servicios de Inspección ante la SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL (SE-

DIA) y la DIRECCIÓN GENERAL DE SALUD PÚBLICA (DGSP), y el Informe de actuaciones previas de la Subdirección General de Inspección de Datos que forman parte del expediente E/03936/2020.

3. Asimismo, se dan por reproducidas a efectos probatorios, las alegaciones al acuerdo de iniciación PS/00222/2021 presentadas por la SEDIA, en fecha 15 de junio de 2021, a través del Reg. Aux. de la Secretaría de Estado de Función Pública.

4. Se REQUIERE a la SEDIA para que aporte la información y/o documentación siguiente:

   4.1. Respecto a la APLICACIÓN PILOTO Radar COVID puesta en marcha entre el 29 de junio y el 29 de julio de 2020 en la isla de la Gomera y desde el 18 de agosto de 2020 a nivel nacional:

   a) Número total de usuarios de la aplicación que participaron en la fase piloto y número total de códigos pseudo-aleatorios o identificadores de proximidad que se subieron al servidor durante esta fase.

   b) Información sobre los datos recabados a través de la aplicación piloto (incluyendo datos de conexión entre el terminal del usuario y el servidor y los metadatos).

   c) Información sobre el tratamiento de datos personales, entendido como el conjunto de operaciones realizadas sobre esos datos.

   d) Información sobre la siguiente cuestión: ¿En qué consistió materialmente ese tratamiento de datos?

      En concreto, el ciclo de vida de los datos tratados, el proceso de estos desde su recogida hasta su supresión o bloqueo.

   e) Copia del registro de las actividades de tratamiento de datos personales efectuadas en el proyecto piloto. Dicho registro, al que se refiere el artículo 30 del Reglamento (UE) 2016/679, de 27 de abril de 2016, deberá aportarse en su versión inicial, junto con cualquier adición, modificación o exclusión en el contenido de este.

   f) Copia de la evaluación de impacto relativa a la protección de datos respecto al proyecto piloto y documentación relativa a esta. Especificación del sujeto que la elabora y del momento en que se realiza (fecha de inicio y finalización).

   g) Si se elaboró la Evaluación de impacto, documentación acreditativa de la participación del delegado de protección de datos en esta.

   h) Copia de la evaluación de impacto, versión 1.0, a la que hace referencia en las alegaciones (página 20).

   i) Documentación acreditativa de la participación del delegado de protección de datos en la evaluación de impacto versión 1.0.

   j) Análisis de riesgos de protección de datos sobre el proyecto piloto y documentación relativa a este. Especificación del sujeto que lo elabora y del momento en que se realiza (fecha de inicio y finalización).

   k) Copia del contenido de las actas de las reuniones celebradas entre la SEDIA y la Dirección General de Salud Pública, Calidad e Innovación, u otro

órgano superior o directivo del Ministerio de Sanidad, que incluyan la información relativa a las decisiones acordadas en materia de protección de datos aplicables al proyecto piloto, con identificación de la condición de los distintos intervinientes (responsables o encargados).

l) Copia del contenido de las actas de las reuniones celebradas entre la SEDIA, el Ministerio de Sanidad (u órgano superior o directivo de este) y la Comunidad Autónoma de Canarias, sobre el proyecto de la aplicación de Radar COVID, que incluyan la información relativa a las decisiones acordadas en materia de protección de datos aplicables al proyecto piloto.

m) Documentación acreditativa del contrato u otro acto jurídico suscrito entre la Dirección General de Salud Pública, Calidad e Innovación u otro órgano superior o directivo del Ministerio de Sanidad y la SEDIA, para la realización del proyecto piloto, conforme a lo dispuesto en el artículo 28.3 del Reglamento (UE) 2016/679, de 27 de abril de 2016.

n) Documentación acreditativa de las instrucciones documentadas de la Dirección General de Salud Pública, Calidad e Innovación u otro órgano superior o directivo del Ministerio de Sanidad, dirigidas a la SEDIA, conforme a lo dispuesto en el artículo 28.3.a) del Reglamento (UE) 2016/679, de 27 de abril de 2016.

o) Documentación acreditativa de la autorización previa, por escrito, específica o general, a favor de la SEDIA o de la Secretaría General de la Administración Digital (SGAD) por parte de la Dirección General de Salud Pública, Calidad e Innovación u otro órgano superior o directivo del Ministerio de Sanidad, en relación con el contrato suscrito con INDRA, conforme a lo dispuesto en el artículo 28.2 del Reglamento (UE) 2016/679, de 27 de abril de 2016.

p) Copia de los pliegos de cláusulas administrativas y de prescripciones técnicas, en caso de existir, y copia del contrato de encargado o subencargado del tratamiento suscrito entre la SEDIA o la SGAD e INDRA, en relación con el proyecto piloto.

q) Documentación acreditativa sobre la participación del Ministerio de Sanidad (a través del órgano superior o directivo correspondiente) en el desarrollo y lanzamiento del proyecto piloto.

La información y documentación anterior prevista en el apartado 4.1 -insistimos- se requiere en relación con la prueba piloto, desde el inicio de las actuaciones relativas a la misma, incluyendo la fase previa a su puesta en marcha y desarrollo posterior, hasta su finalización.

4.2. Respecto a la APLICACIÓN Radar COVID puesta en marcha en las diferentes comunidades y ciudades autónomas tras la adhesión a través de los oportunos convenios bilaterales suscritos entre el Ministerio de Sanidad y las Consejerías correspondientes:

a) Datos personales precisados por la aplicación Radar COVID para funcionar correctamente y cumplir con sus finalidades.

b) Información sobre el tratamiento de esos datos personales, entendido como el conjunto de operaciones realizadas sobre esos datos.

c) Información sobre la siguiente cuestión: ¿En qué ha consistido materialmente ese tratamiento de datos?

En concreto, el ciclo de vida de los datos tratados, el proceso de estos desde su recogida hasta su supresión o bloqueo.

d) Documentación acreditativa de si se ha solicitado al delegado de protección de datos del METD asesoramiento sobre la naturaleza jurídica de los datos tratados y la respuesta, que, en su caso, éste haya formulado.

e) Copia del registro de las actividades de tratamiento de datos personales efectuadas en la aplicación Radar COVID. Dicho registro, al que se refiere el artículo 30 del Reglamento (UE) 2016/679, de 27 de abril de 2016, deberá aportarse en su versión inicial, junto con cualquier adición, modificación o exclusión en el contenido de este.

f) Evaluación o evaluaciones de impacto relativas a la protección de datos respecto a la aplicación Radar COVID.

La información y documentación prevista en el apartado 4.2 se requiere en relación con la puesta en servicio de la aplicación Radar COVID a partir del 10 de octubre de 2020, tras la publicación en el BOE de la Resolución de 13 de octubre de 2020, de la Subsecretaría, por la que se publica el Acuerdo entre el METDy el Ministerio de Sanidad, acerca de la aplicación "Radar COVID".

La notificación del acuerdo se practicó en fecha 22 de septiembre de 2021, por medio del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada, según certificado que figura en el expediente.

DÉCIMO TERCERO: Con fecha 25 de octubre de 2021 la SEDIA presenta un escrito a través del cual solicita una ampliación del plazo de práctica de prueba a diez días hábiles más.

El acuerdo que concede un periodo extraordinario de prueba, por un plazo de 10 días, se notifica en fecha 28 de octubre de 2021 a través Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada.

DÉCIMO CUARTO: La SEDIA, con fecha 22 de noviembre de 2021, en respuesta al requerimiento de pruebas notificado aportó a las actuaciones los siguientes documentos:

- Contestación y remisión de documentación en el período de prueba del procedimiento sancionador de la AEPD en relación a la aplicación Radar COVID.
- Doc. 1. Informe de Conclusiones Radar Covid de 28 de enero de 2021
- Doc. 2. Informe EIPD_ COVID Radar v.1.0.pdf
- Doc. 3. AARR_AppCOVID_v1.0.pdf
- Doc. 4. ACTA DE LA REUNIÓN GRUPO DE TRABAJO INTERTERRITORIAL Videoconferencia 17 de junio de 2020
- Doc. 5. PRESENTACION COVID RADAR FUNCIONAMIENTO GENERAL JUNIO 2020
- Doc. 5 bis. PRESENTACION PILOTO A CCAA´S JUNIO 2020

- Doc. 6. PRESENTACION COVID RADAR SEGUIMIENTO 17-07-2020
- Doc. 7. ACTA DE REUNION 21 JULIO2020
- Doc. 8. PRESENTACION COVID RADAR SEGUIMIENTO 24-07-2020
- Doc. 9. ACTA DE REUNION 27 JULIO 2020
- Doc. 10. ACTA DE REUNION 5 AGOSTO **
- Doc. 11. PRESENTACION RADAR COVID SEGUIMIENTO 31 JULIO 2020
- Doc. 12. PRESENTACION 21 AGOSTO 2020
- Doc. 13. ACTA 26 DE AGOSTO 2020
- Doc. 14. Mandato de la Dirección General de Salud Pública del Ministerio de Sanidad, dando su visto bueno para el desarrollo del piloto de aplicación móvil para la trazabilidad de contactos de la COVID-19
- Doc. 14 bis. ACUERDO ENTRE EL METD(SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL) Y EL MINISTERIO DE SANIDAD ACERCA DE LA APLICACIÓN “RADAR COVID
- Doc. 15. Pliego para el diseño, desarrollo, piloto y evaluación de un sistema que permita el rastreo de contactos en relación a la pandemia ocasionada por la covid-19.
- Doc. 16. Nota de prensa 23 JUNIO
- Doc. 17. Nota de prensa 3 AGOSTO
- Doc. 18. Nota de prensa 9 SEPTIEMBRE

DÉCIMO QUINTO: Con fecha 26 de enero de 2022 la instructora del procedimiento formula propuesta de resolución, en la que propone que, por la directora de la AEPD, se sancione con un APERCIBIMIENTO a la SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL, por infracción de los siguientes artículos:

> - Artículos 5.1.a) y 5.2 del RGPD, tipificada en el artículo 83.5.a) del RGPD y en el artículo 72.1. a) de la LOPDGDD, a los solos efectos de determinar los plazos de prescripción.
>
> - Artículos 12 y 13 del RGPD, tipificada en el artículo 83.5.b) del RGPD y en el artículo 72.1.h) de la LOPDGDD, a los solos efectos de determinar los plazos de prescripción.
>
> - Artículo 25 del RGPD, tipificada en el artículo 83.4.a) del RGPD y en el artículo 73 de la LOPDGDD en el apartado d), a los solos efectos de determinar los plazos de prescripción.
>
> - Artículo 28.3 del RGPD, tipificada en el artículo 83.4.a) del RGPD y en el artículo 73 de la LOPDGDD en el apartado k), a los solos efectos de determinar los plazos de prescripción.
>
> - Artículo 28.10 del RGPD, tipificada en el artículo 83.4.a) del RGPD y en el artículo 73 de la LOPDGDD en el apartado m), a los solos efectos de determi-

nar los plazos de prescripción.

- Artículo 35 del RGPD, tipificada en el artículo 83.4.a) del RGPD y en el artículo 73 de la LOPDGDD en el apartado t), a los solos efectos de determinar los plazos de prescripción.

Con fecha 27 de enero de 2022, a través del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada, se notifica la propuesta de resolución.

DÉCIMO SEXTO: Con fecha 7 de febrero de 2022 la SEDIA solicita una ampliación del plazo para formular alegaciones a la propuesta de resolución.

DÉCIMO SÉPTIMO: Con fecha 7 de febrero de 2022 el órgano instructor acuerda denegar motivadamente la solicitud de ampliación de plazo instada.

DÉCIMO OCTAVO: Con fecha 10 de febrero de 2022 el director de la SGAD, por indicación de la SEDIA, presenta las alegaciones a la propuesta de resolución y adjunta un oficio de solicitud de práctica de la prueba.

En las alegaciones, en síntesis, aduce que:

I. ANTECEDENTES

Cuando la directora de la AEPD instó el inicio de actuaciones previas de investigación (21 de mayo de 2020) ni estaba constituido el equipo de trabajo del proyecto RADAR COVID ni estaba iniciado el proyecto en sentido estricto, por lo que en aquel momento (mayo de 2020) no existían “hechos” que se pudieran examinar.

Los requerimientos fueron respondidos en tiempo y forma, aportando abundantes explicaciones, informaciones y documentación, lo que demuestra la permanente voluntad de colaboración de la SEDIA en el contexto del procedimiento abierto.

Estas actuaciones de oficio se realizan tres meses y medio antes de que existiera la primera reclamación, la denominada “la parte reclamante uno”.

II. ALEGACIONES.

Da por reproducidas las efectuadas a lo largo de la tramitación del expediente, así como la documentación remitida durante el periodo de prueba y actuaciones previas.

A)Respecto de las ALEGACIONES DE CARÁCTER GENERAL:

Aduce que RADAR COVID es una App que fue creada como una herramienta adicional para ayudar a hacer frente a la situación, grave y excepcional, de emergencia sanitaria en España provocada por el coronavirus.

En el **Real Decreto 463/2020, de 14 de marzo,** se dictaron medidas imprescindibles para hacer frente a la situación, que resultaban proporcionadas a su extrema gravedad y no suponían la suspensión de ningún derecho.

En este contexto, la SEDIA, como encargada de tratamiento, actuó conforme a las indicaciones dadas en todo momento por el MSND, como autoridad delegada del Gobierno en materia de Sanidad y en materia de salud pública y como responsable del tratamiento de la aplicación RADAR COVID.

Es cierto que estas indicaciones no se plasmaron en un contrato tal como se prevé en el artículo 28.1 a) del RGPD y ello es así porque el estado de alarma dificultó la formalización de los instrumentos habituales previstos en la legislación para estos supuestos en circunstancias normales. Sí está acreditada, sin embargo, en la documentación aportada en el periodo de prueba, la celebración de una serie de reuniones a las que asistieron representantes del MSND, de la SEDIA y de la empresa adjudicataria del contrato de emergencia para el desarrollo del piloto y de la aplicación RADAR COVID, reuniones en las que se tomaban las decisiones necesarias para avanzar en el desarrollo del piloto y de la aplicación.

La protección de la salud en un contexto de pandemia determinó la necesidad de actuar rápidamente de forma coordinada con la colaboración de todos los agentes implicados y la relación entre responsable y encargado de tratamiento se produjo de una manera más ágil, tal como exigían las circunstancias, pero no por ello menos eficiente ni menos respetuosa con el derecho a la protección de datos de carácter personal ni el respeto al principio de seguridad jurídica

Además de las reuniones periódicas, el METD a través de la SGAD dependiente de la SEDIA, como encargado del tratamiento, mantuvo contactos muy frecuentes con el MSND, para recibir sus indicaciones y estar ambos departamentos alineados en la consecución del objetivo común.

Así, el MSND, a través de la Directora General de Salud Pública, Calidad e Innovación, otorgó su visto bueno para el desarrollo de RADAR COVID, y la SEDIA puso todo su empeño en su puesta en marcha en el menor tiempo posible, sin menoscabo de derecho alguno. La SEDIA actuó siempre movida por razones de interés público y siguiendo las indicaciones del Gobierno y su autoridad delegada (el Ministro de Sanidad) para ayudar a atajar la emergencia.

España, al igual que otros países de nuestro entorno, a través de SEDIA y de la SGAD, desarrolló bajo la tutela del MSND y en cooperación con otros miembros de la Unión Europea y la red de eHealth, la herramienta digital RADAR COVID, aprovechando los resultados de la experiencia piloto desarrollada en la Isla de la Gomera.

B) Respecto de las ALEGACIONES ESPECÍFICAS:

B.1 Respecto al tratamiento de datos de carácter personal.

El derecho a la protección de datos, como cualquier otro derecho, no es absoluto. No basta con atenerse a la aplicación literal de una norma, sin apelar, ni tener en cuenta su espíritu y finalidad tal como prescribe el artículo 3 del Código Civil.

La exigencia y aplicación de la normativa de protección de datos, en unas circunstancias tan especiales y atípicas, y sin perjuicio del respeto al principio de seguridad jurídica, debe ser equilibrada y ponderada. En ningún momento los organismos responsa-

bles de la protección de datos pueden actuar como si el estado de alarma no hubiese existido o no afectase a la materia de su competencia y al ejercicio de sus facultades.

En la fase de prueba, la SEDIA señala, que los datos recopilados y generados por la aplicación no permiten, por defecto, la identificación directa del usuario o de su dispositivo. Sin embargo, aunque, ateniéndonos al considerando 30 del RGPD, los usuarios podrían llegar a ser identificables mediante la asociación de algún identificador en línea facilitado por el dispositivo u otro tipo de herramientas o protocolos, en el proyecto piloto los datos **no eran reales** (eran de prueba) y los códigos de contagiados para su introducción en la App **eran falsos**. Cuando la App se abrió en La Gomera al público, las personas no podían introducir datos reales de estar infectados.

El tratamiento de estos datos por RADAR COVID ha sido lícito, cabe recordar a este respecto con el Informe AEPD 17/2020, de 12 de marzo, que el RGPD prevé que la base jurídica que otorga licitud a este tipo de tratamiento (más allá de los casos en donde preste consentimiento el interesado), la encontramos en los artículos 6.1.d) (cuando sea necesario para proteger intereses vitales del interesado u otras personas físicas) y 6.1.e) (**cuando sea necesario para el cumplimiento de una misión realizada en interés público).**

B.2 Respecto al rol de la SGAD en el tratamiento de datos

1º. La etapa en la que se hace el proyecto piloto.

El 9 de junio de 2020 la SEDIA recibió el visto bueno de la Dirección General de Salud Pública del MSND para conducir un proyecto piloto en la isla de la Gomera, lo que posibilitó la realización del correspondiente expediente de contratación. En su autorización estableció que: *Por otro lado, entendemos que **el responsable del tratamiento de los datos de este piloto será la autoridad sanitaria de la Comunidad** en que se va a llevar a cabo.* Quedando la SEDIA como encargada del tratamiento de los datos y resultados.

El MSND, a través de la DGSP participó en las reuniones semanales del piloto para la conformación de los fines y medios del proyecto. En particular, D, **X.X.X**., Director del Centro de Coordinación y Alertas Sanitarias, así como personal de su unidad, formaron parte del seguimiento semanal. Asimismo, formaron parte del comité de seguimiento autoridades sanitarias del Gobierno de Canarias.

En todo caso, los datos que se manejaron en el piloto realizado entre los meses de junio y julio de 2020 eran datos simulados de infección (datos no reales), no poniéndose en compromiso ningún dato personal, ni mucho menos relacionado con la salud de los participantes. El equipo del proyecto, junto con expertos independientes, ha publicado un artículo de los trabajos realizados en San Sebastián de la Gomera en la revista *Nature Communications*, dando idea de la utilidad de esta herramienta a efectos de cortar cadenas de transmisión del virus.

2º.- La etapa en la que se pone en marcha la aplicación en fase de pruebas y posteriormente la aplicación definitiva.

El Acuerdo del Consejo Interterritorial del Sistema Nacional de Salud, de 19 de agosto

de 2020, permitió que las CCAA pudieran asumir temporalmente, hasta la firma de los citados convenios, la gestión de los códigos de diagnóstico positivo que se asignasen a aquellos ciudadanos con una prueba diagnóstica positiva de infección activa (PCR u otras técnicas).

Por otra parte, el 25 de agosto de 2020, tras la celebración del Consejo de Ministros, el Presidente del Gobierno presentó la hoja de ruta para hacer frente al ascenso de la "segunda curva epidemiológica", en el contexto de la pandemia del SARS-C0V2 en nuestro país. Entre otras medidas, citó el refuerzo de los medios digitales de rastreo, solicitando a los ciudadanos el uso de RADAR COVID.

Posteriormente se publicó el Acuerdo, de 9 de octubre de 2020, que facultó a la SGAD para la suscripción de Convenios con Comunidades y Ciudades Autónomas, especificando que: "*en los mencionados Convenios de colaboración, **el Ministerio de Sanidad y la Consejería competente en materia de sanidad de la Comunidad o Ciudad Autónoma de que se trate figurarán como responsables del tratamiento de datos de carácter personal y la SGAD como encargado del tratamiento***."

En los diferentes Convenios, que cuentan con todas las autorizaciones legamente exigibles, celebrados entre la SGAD y las CCAA se ha señalado reiteradamente que: "*la Consejería de Salud es Responsable del Tratamiento de datos de la aplicación RADAR COVID. En dicha condición le corresponden, entre otras, las siguientes actividades de tratamiento:*

> *a) Solicitar a la SGAD, según se requieran, los códigos de confirmación de positivo por prueba.*
> *b) Facilitar los códigos de confirmación anteriores a los usuarios con un diagnóstico positivo" .*

Correspondiendo a la SGAD entre otras funciones la de (…): "*h) Cumplir con los cometidos **como encargada del tratamiento indicados por el Ministerio de Sanidad como responsable del mismo".***

Queda plenamente acreditado que en todo momento y de acuerdo con los instrumentos jurídicamente vinculantes, que la SGAD actuó y actúa única y exclusivamente como encargada del tratamiento, mientras que el MSND y las CCAA eran y son las responsables de dicho tratamiento.

En este sentido, el MSND ha facilitado directrices a la SEDIA-SGAD, como por ejemplo las recogidas en el documento técnico denominado "*Procedimiento de implementación de la App RADAR COVID como complemento a los sistemas manuales de identificación de contactos*", coordinado por el Centro de Coordinación de Alertas y Emergencias Sanitarias, Dirección General de Salud Pública, Calidad e Innovación y aprobado por la Ponencia de Alertas y Planes de Preparación y Respuesta.

En tal sentido, RADAR COVID ha sido elaborada siguiendo los criterios epidemiológicos de la "Estrategia de detección precoz, vigilancia y control del COVID-19" publicada por el Ministerio de Sanidad.

En todo momento, tanto en el desarrollo del piloto en la Isla de la Gomera, como en el

uso de RADAR COVID en pruebas por las CCAA, y en su uso superada dicha fase de pruebas, estaban definidos los roles de responsable de tratamiento y de encargado de tratamiento. Los documentos que dan prueba de ello son:

a) La carta de 9 de junio de 2020 de Directora General de Salud Pública, Calidad e Innovación dando el visto buen a la realización de la App.

b) El Acuerdo del Consejo Interterritorial de 19 de agosto de 2020.

c) y el Acuerdo publicado en el BOE el 15 de octubre de 2020.

Respecto a la afirmación recogida en la propuesta en la página 159: "*La AEPD no entra ni a examinar ni a calificar cuál debe ser el instrumento jurídico a través del cual se encomienda formalmente a la SEDIA el encargo del tratamiento referido al proyecto piloto RADAR COVID* (…)" , la SEDIA se remite de nuevo a los documentos señalados anteriormente.

La AEPD hace un prolijo razonamiento para señalar, que a su juicio, la SEDIA ha jugado, con claridad, el rol de responsable del tratamiento, pero en los documentos que se han citado, la SEDIA siempre figura con encargada del tratamiento y sus actuaciones han ido siempre dirigidas a cumplir esta función.

También alude al valor de las Notas de Prensa del METD, que la AEPD otorga en la página 140: "*las notas de prensa elevan la transparencia y rendición de cuentas a su máxima expresión y se incluyen como parte de los hechos probados por esta razón*."

La SEDIA no puede más que discrepar de esta afirmación. Las Notas de Prensa son simples anuncios que realizó el METD para informar a la ciudadanía y los medios de comunicación, de actividades que estaban proyectadas o en curso de realización. Tienen un valor de difusión y publicidad, en ningún caso pueden ser consideradas, con un valor tan singular como para afirmar que "*elevan la transparencia a su máxima expresión*", ya que hay otros instrumentos más eficaces para cumplir esta función, previstos por la normativa y descritos en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

Tampoco es posible inferir de estas que, desde un principio, la SEDIA actuó como responsable del tratamiento, ya que, el hecho de informar a la ciudadanía sobre determinados asuntos que recaen dentro del ámbito de la competencia del departamento, no implica necesariamente que el que informa sea el que determine todos los contenidos sobre los que se informa.

Las Notas de Prensa no pueden servir para adjudicar roles de Responsable del tratamiento ni de Encargado del tratamiento, ya que son meros documentos informativos y no atributivos de competencias, por ello, es imposible sacar este tipo de conclusiones.

Tampoco es posible adjudicar a la SEDIA el rol de responsable de tratamiento solo porque en un documento sobre las FAQ RADAR COVID se señalen las finalidades del tratamiento, ni porque se identifique a la SGAD como titular de la aplicación en las Condiciones de Uso de la aplicación.

La SEDIA, a través de la SGAD ha desarrollado estas y otras aplicaciones, y ha desarrollado una labor de difusión que probablemente el MSND no estaba en condiciones de hacer porque la situación de pandemia exigía una mayor dedicación a otros asuntos más relevantes en el ámbito de sus competencias.

De cara a la ciudadanía, y tal y como se ha señalado, fue el Gobierno el que impulsó la creación de esta aplicación e instó a la población al uso de RADAR COVID, ya que era una aplicación que podía contribuir a mitigar la pandemia en un momento de auge de los contagios y, además, era una solución que se estaba poniendo en funcionamiento en la práctica totalidad de países de nuestro entorno europeo, por lo que no cabe afirmar que fuera la SEDIA la que, por los anuncios de prensa, tuviera una apariencia para la ciudadanía como responsable del tratamiento cuando su papel era simplemente contribuir, en colaboración con todo el Gobierno a aportar soluciones en el ámbito de sus competencias de impulso de la digitalización de las administraciones públicas (y todo ello sin tener en cuenta que la propia existencia de categorías jurídicas como las de responsable y encargado del tratamiento de protección de datos son difícilmente aprehensibles para el común de los destinatarios de una nota informativa ministerial, ni siquiera para operadores jurídicos no especializados, y pretender que la población general pueda extraer las conclusiones y la subsiguiente atribución de roles que plantea la propuesta de resolución de la lectura de una nota de prensa y traer anudados unos incumplimientos de la normativa vigente excede, a nuestro juicio, lo razonable).

Y como ya se ha señalado, el hecho de colaborar, impulsar y tener un papel relevante en intentar convencer a la población del uso de RADAR COVID, para prevenir los contagios y reducir los ingresos hospitalarios y con ello las muertes, ofreciendo una explicación de las características de la aplicación en los medios de comunicación, no puede llevar a la conclusión de que se esté desarrollando otro papel diferente al asignado en los documentos reiteradamente señalados. Sólo puede entenderse esta participación desde el punto de vista de una actuación coordinada del Gobierno en el que todos los departamentos contribuían, en un Estado de alarma declarado a limitar las consecuencias de la pandemia.

Conviene recordar, en este punto, que no fue hasta el 6 de agosto de 2020, cuando se publicó la modificación de la estructura del MSND con la creación de la SGSDII, con la consiguiente atribución de nuevas competencias en materia de digitalización de la salud y de elaboración de Apps en materia sanitaria a este departamento

Señala además la AEPD que dicho rol lo desempeñó la SEDIA sin tener cobertura legal para llevar a cabo este rol y sin delegación o encomienda que permita el ejercicio de la competencia, cuestión que no puede ser admitida al no pretender nunca la SEDIA ejercer otro rol distinto al de encargado de tratamiento que era el que tenía adjudicado.

B.3 Respecto al rol de INDRA

La SEDIA, en su condición de encargado de tratamiento, contó desde el primer momento, con la autorización del MSND, como responsable del tratamiento, para la contratación de INDRA, que, contaba con las garantías suficientes para garantizar la aplicación del RGPD.

B.4 Respecto a las Evaluaciones de Impacto

Señala la AEPD en la página 184 que: "*el CEPD considera que ha de llevarse a cabo una evaluación de impacto relativa a la protección de datos (EIPD)* ***antes de empezar a utilizar una aplicación*** *de este tipo por cuanto se considera que el tratamiento puede entrañar un alto riesgo […]. El CEPD* ***recomienda encarecidamente la publicación de las EIPD*****."**

En primer lugar, cabe mencionar que si bien la EIPD publicada en septiembre 2020 fue la versión 1.1, ya existía una versión 1.0 del EIPD con anterioridad al 19 de agosto de 2020. La EIPD facilitada a la AEPD fue la versión 1.1 pues es la que se publicó, coincidiendo con el despliegue en septiembre 2020 de una versión de la aplicación, con soporte de lenguas cooficiales.

Durante el periodo del 19 de agosto hasta la publicación en septiembre 2020, se debatió internamente sobre la conveniencia o no de su publicación.

De hecho, de acuerdo con el artículo 3.4 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP), la AGE, que actúa para el cumplimiento de sus fines con personalidad jurídica única, ostenta la condición de responsable y de encargado del tratamiento a través de órganos distintos y no viene publicando ni la EIPD, ni los Análisis de Riesgos sobre las que se basan, de los sistemas que desarrolla.

De cara a dar cumplimiento a la recomendación del CEPD, la SGAD recabó criterio al Delegado de Protección de Datos del METD. Su criterio fue que, con carácter general, no debían publicarse estos documentos.

En todo caso, finalmente se siguió la recomendación del CEPD, y se procedió a publicar la EIPD y el Análisis de Riesgos previo en septiembre de 2020 (https://github.com/radarcovid/radar-coviddocumentation).

Por otra parte es criterio de la AEPD, y así lo recoge en la página 189 de su propuesta de resolución, que:

"*Por último, indicaremos que la realización posterior de la EIPD no "subsana" la falta de realización de esta en el momento oportuno y con la participación de todos los actores necesarios, especialmente porque la falta de evaluación de los riesgos y de adopción de las medidas técnicas y organizativas oportunas, ya ha producido un daño intangible en los derechos y libertades de los ciudadanos, más reprochable si se trata de Administraciones Públicas".*

Conviene recordar en este punto que la aplicación piloto de RADAR COVID utilizaba datos simulados por lo que si bien, la EIPD se hizo en un momento posterior a la puesta en funcionamiento del piloto, sí se hizo con anterioridad al momento en que la aplicación iba a manejar datos de salud de los usuarios.

B.5 Respecto a las condiciones de uso y política de privacidad

Indica la AEPD en su propuesta de resolución (pág. 174) que: "*De los hechos proba-*

dos, resulta acreditado que la primera versión de la App prevista para el programa piloto (julio 2020), recogía en dos documentos distintos la información relativa a la privacidad:

> * Condiciones de uso: *https://radarcovid.covid19.gob.es/terms-of-service/use-conditions.html*
>
> ** Política de privacidad: https://radarcovid.covid19.gob.es/terms-of-service/privacypolicy.html. Sin embargo, ninguno de ellos definía quién era el responsable o encargado del tratamiento."*

Hay que recordar que la primera versión de la App (piloto) sirvió a efectos de comprobar aspectos como la usabilidad, percepción de privacidad, y eficacia de la solución en un entorno simulado. En ningún caso se manejaban datos de salud de los participantes en el piloto.

Y la Política de Privacidad de la app incluía el siguiente aviso:

> "*El USUARIO de esta aplicación queda avisado de que al descargar la aplicación en su dispositivo móvil y utilizarla, se está limitando a participar voluntariamente en una EXPERIENCIA PILOTO CON DATOS FICTICIOS de alerta de contagios de la COVID-19 en LA ISLA DE LA GOMERA.*
>
> *Se informa asimismo de que esta aplicación dejará de funcionar una vez que termine la experiencia piloto.*
>
> *Por tanto, en el uso de la aplicación, todas las notificaciones de exposiciones a posible contagio de la enfermedad que el usuario pueda recibir corresponden a supuestos simulados y, por el mismo motivo, al tratarse de una experiencia piloto con datos ficticios, las sugerencias de adopción de medidas preventivas y asistenciales que tras esa notificación le facilite la aplicación no tienen otro valor que comprobar que la aplicación es capaz de facilitar sugerencias de ese tipo a un usuario que recibiera una notificación de exposición a posible contagio".*

El equipo de RADAR COVID, ha ido revisando y actualizando los documentos con el ánimo de mejorar su contenido y facilitar su lectura y comprensión, haciendo uso de su facultad de responsabilidad proactiva en la mejora constante de la app y su documentación asociada.

Adicionalmente, se han incorporado cuestiones adicionales como la interoperabilidad europea, a través del nodo europeo de interoperabilidad para las aplicaciones nacionales de rastreo de contactos (European Forwarding Gateway Service -EFGS). Hay que indicar que para la conexión de RADAR COVID al nodo europeo de interoperabilidad se remitió información del sistema, condiciones de uso y política de privacidad de la aplicación, y fue aprobado por el Grupo Conjunto de Responsables de Tratamiento (eHealth Network Joint Controller Group), donde el MSND del Gobierno de España figuraba como uno de los miembros.

Con cada actualización del aplicativo (siguiendo el principio de responsabilidad proacti-

va), si existía cambio en las condiciones de uso y política de privacidad, se solicitaba de nuevo consentimiento expreso por parte de los usuarios.

En la página 175 de la propuesta, la AEPD señala: "*No queda claro quién es el responsable del tratamiento ni tampoco los datos del Delegado de Protección de Datos, que ni siquiera se mencionan en la política de privacidad".*

Cabe recordar por parte de SEDIA que la política de privacidad actual (https://radarcovid.gob.es/politica-de-privacidad) **establece como responsables del tratamiento al Ministerio de Sanidad y Comunidades Autónomas, y como encargado del tratamiento a la Secretaría General de Administración Digital**.

En la página 178 de la propuesta de resolución sancionadora, la Agencia afirma: "E*n suma, la política de privacidad se ha visto modificada en numerosos aspectos hasta tal punto que supone un incremento de 700 palabras a la versión inicial" .*

El incremento corresponde con explicaciones más extensas de los apartados de privacidad, así como la ampliación a nuevos usos de la aplicación, como la interoperabilidad con las aplicaciones de rastreo de contactos de la Unión Europea.

Por otra parte, cualquier cambio de la aplicación incluyendo nuevas funcionalidades (como la conexión de RADAR COVID al nodo europeo de interoperabilidad) ha conllevado la actualización de las condiciones de uso y política de privacidad, a fin de aportar transparencia e información a las personas usuarias de la aplicación.

En la página 179 la Agencia afirma: "*En suma, la SEDIA, actuando como responsable del tratamiento, no tomó las medidas oportunas para facilitar al interesado toda la información en los términos que establecen los artículos 12 y 13 del RGPD. Esta información, debió proporcionarse de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, y, además, en su caso, visualizable.*

Ello es especialmente pertinente en situaciones como la que acontece, en la que la proliferación de agentes y la complejidad tecnológica de la App hacen que sea difícil para la ciudadanía saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como sucede en el caso analizado."

La SEDIA desea recordar a este propósito que las condiciones de uso y política de privacidad han estado siempre accesibles para los interesados, tanto desde la aplicación móvil, como desde la web http://radarcovid.gob.es.

Por ende, es necesario el consentimiento expreso del usuario para poder utilizar la aplicación, además de ser su uso totalmente voluntario.

En el tiempo que la aplicación lleva operativa, **la SEDIA no ha recibido ninguna queja, ni formal ni informal, del Delegado de Protección de Datos del MSND en relación a la aplicación RADAR COVID.**

En la pág. 181 de la propuesta se concluye: "Incidir en que inicialmente no se incluyó información respecto al responsable, destinatarios o los derechos de los artículos 15 a 22. Tampoco en la versión final se ha incluido la información relativa al Delegado de

Protección de Datos……..".

Desde la SEDIA, solo recordar que en el apartado "¿Cómo se protege mi privacidad?", la app recoge lo siguiente:

> "Aquí tienes una lista de algunas de las medidas con las que RADAR COVID protege tus datos:
>
> - La aplicación no recopila ningún dato que permita rastrear tu identidad. Por ejemplo, no te preguntará y no podrá conocer tu nombre, apellidos, dirección, número de teléfono o dirección de correo electrónico.
>
> - La aplicación no recopila ningún dato de geolocalización, incluidos los del GPS. Además, tampoco realiza ningún seguimiento de tus desplazamientos.
>
> - El código de Bluetooth Low Energy (de baja energía) que se transmite a través de la aplicación se genera aleatoriamente y no contiene ninguna información sobre tu smartphone ni sobre ti.
>
> - Además, este código cambia varias veces cada hora para proteger aún más tu privacidad.
>
> - Los datos que se guardan en tu teléfono móvil están cifrados.
>
> - Las conexiones entre la aplicación y el servidor están cifradas.
>
> - Todos los datos, tanto los que se guardan en el dispositivo (códigos intercambiados con otros teléfonos móviles) son eliminados al cabo de 14 días.
>
> - Asimismo, los datos recogidos en el servidor, procedentes de los teléfonos móviles donde se ha reportado un diagnóstico positivo por COVID-19, son eliminados al cabo de 14 días.
>
> - Ningún dato almacenado en los teléfonos móviles o en el servidor permite la identificación ni del propio dispositivo móvil ni del usuario del mismo"

B.6 Respecto a las vulnerabilidades detectadas

Como ya se indicó en anteriores ocasiones por parte de la SGAD, la vulnerabilidad reportada por un conjunto de expertos en privacidad fue conocida a mediados de septiembre de 2020. Fue analizada y se programó una corrección coincidiendo con una próxima liberación de la aplicación. Fue corregida el 8 de octubre de 2020, y compartido el código que corregía el problema con el equipo técnico de la Escuela Politécnica Federal de Lausana (EPFL), que es quien había impulsado el protocolo DP3-T, garante de la privacidad.

La corrección fue atendida en plazos razonables de tiempo de acuerdo a su impacto. Como se argumentó a la AEPD, se juzgó muy remoto el escenario en el que podía explotarse la vulnerabilidad, con un tercero con capacidad suficiente de espiar las redes de comunicaciones, y de cruzar la información remitida por RADAR COVID con otras

informaciones a su alcance, que permitieran establecer una relación entre la identidad del usuario y su condición médica de positivo por COVID-19, era muy remoto.

Ese juicio se mostró acertado, pues no se ha detectado ni se tiene constancia de que esta teórica vulnerabilidad haya sido explotada o aprovechada en ningún caso real, seguramente por la dificultad y poco beneficio que se obtendría de su implantación.

Es conocido por todos que no existe ningún sistema informático 100% seguro, y por ello se optó, una vez ponderadas estas circunstancias por continuar el desarrollo (aplicando el principio “in dubio pro actione”). Dado que la alternativa era paralizar el uso y desarrollo de la app con el consiguiente riesgo y menoscabo para la salud colectiva, al privar a la sociedad de una herramienta con un gran potencial de ayuda en pleno estado de alarma por emergencia sanitaria.

III. CONCLUSIÓN DEL ESCRITO DE ALEGACIONES

La SEDIA es consciente que puede haber discrepancias en los criterios sobre las actuaciones en las que se ha concretado el trabajo de puesta en marcha, en un tiempo razonable, de una aplicación necesaria en el contexto de pandemia en el que se desarrolló, con un estado de emergencia declarado. Pero siempre ha actuado con una responsabilidad proactiva para corregir los posibles errores u omisiones de la App, asumiendo el principio de privacidad desde el diseño, actuando en defensa del interés público y de la ciudadanía, y colaborando con la AEPD en todo lo solicitado.

De hecho, la SEDIA solicitó informe a la AEPD en el momento en que estaba prevista la extensión de la aplicación a las CCAA en agosto de 2020, momento en el que habría sido muy valiosa la aportación de la AEPD, pero el inicio de las actuaciones previas, determinó a juicio de la AEPD la imposibilidad de contar con este informe.

Como ya señalamos anteriormente y ahora repetimos, la situación de emergencia y la declaración el estado de alarma alteró el orden jurídico ordinario y el modo de actuar habitual de la Administración.

La situación excepcional determinó una modulación en los procedimientos de la administración y exigió actuar con celeridad para así poder llegar a tiempo y que la aplicación cumpliera con sus fines en un momento en que todos los gobiernos de nuestro entorno europeo e internacional, la estaban demandando. Y hubo que desarrollar una aplicación piloto con datos simulados, hubo que hacer la contratación de emergencia en que se suprimieron trámites esenciales, en favor de la agilidad, y hubo que extender rápido la aplicación a las CCAA a través de los instrumentos jurídicos más inmediatos y acordes con la situación que permitieran cohonestar la cobertura jurídica y la agilización de trámites burocráticos.

Se hicieron las evaluaciones pertinentes, los análisis que permitió la premura con que hubo de desarrollarse la aplicación y se actuó siempre con la finalidad última de ejercer una responsabilidad proactiva para permitir un adecuado respeto a la protección de datos de carácter personal.

En definitiva, conforme a las argumentaciones y razonamientos anteriores, la SEDIA considera que no ha lugar a sanción de apercibimiento, porque no ha existido un in-

cumplimiento flagrante, consciente y deliberado de la normativa de protección de datos y de todos los artículos que se citan en la propuesta de resolución del expediente sancionador.

IV. CONSIDERACIONES COMPLEMENTARIAS

Mediante escrito independiente, la SEDIA ha solicitado, en virtud de lo establecido en el artículo 89.2 de la LPACAP, la práctica de la prueba consistente en la puesta a disposición de la SGAD de la siguiente documentación que se considera fundamental para el ejercicio de la defensa en el procedimiento sancionador abierto en relación a la aplicación RADAR COVID:

> a) Propuesta de resolución del Instructor/a en relación con el procedimiento abierto contra el MSND por la aplicación RADAR COVID, a fin de apreciar el criterio de la AEPD en relación con la actividad desarrollada por dicho departamento que aunque goza de la misma personalidad jurídica que la SEDIA, es tratada por la AEPD como un ente distinto.
>
> b) Informes íntegros del Gabinete Jurídico de la AEPD citados que se citan en el Fundamento de Derecho Noveno (17/2020 y 32/2020) de la Propuesta de Resolución, para poder apreciarlo en su conjunto y aceptarlo o rebatirlo según sea su criterio.

(La cursiva, negrita, y el subrayado es de la SEDIA).

Estas alegaciones serán objeto de respuesta en los FD de la presente Resolución.

De las actuaciones practicadas en el presente procedimiento y de la documentación obrante en el expediente, han quedado acreditados los siguientes:

HECHOS PROBADOS

PRIMERO: El Real Decreto 403/2020, de 25 de febrero, desarrolla la estructura orgánica básica del Ministerio de Asuntos Económicos y Transformación Digital. Se publicó el 27 de febrero de 2020 en el BOE, entrando en vigor el mismo día de su publicación.

Dispone en su artículo 1 que el METD se encarga de

> *"la política de telecomunicaciones y para la transformación digital, en particular impulsando la digitalización de las Administraciones Públicas".*

Dentro de este marco, la SEDIA tiene, conforme al artículo 8, atribuidas las funciones de

> *"el impulso de la digitalización del sector público y la coordinación y cooperación interministerial y con otras Administraciones Públicas respecto a dichas materias, sin perjuicio de las competencias atribuidas a otros departamentos ministeriales".*

La SGAD, conforme al artículo 9, es:

> "*el órgano directivo al que corresponde, bajo la autoridad de la persona titular de la Secretaría de Estado de Digitalización e Inteligencia Artificial, la dirección,*

coordinación y ejecución de las competencias atribuidas al Departamento en materia de transformación digital de la administración, incluyendo el desarrollo técnico y aplicación de las Leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y 40/2015, de 1 de octubre, y su normativa reglamentaria, en lo que concierne a la actuación y funcionamiento del sector público por medios electrónicos."

SEGUNDO: El Real Decreto 454/2020, de 10 de marzo, por el que se desarrolla la estructura orgánica básica del Ministerio de Sanidad, y se modifica el Real Decreto 139/2020, de 28 de enero, por el que se establece la estructura orgánica básica de los departamentos ministeriales fue publicado en el BOE de 12 de marzo de 2020. Entró en vigor el mismo día de su publicación en el BOE hasta el 6 de agosto de 2020, fecha en la que entró en vigor el Real Decreto 735/2020 de 4 de agosto.

En su artículo 1 dispone:

Corresponde al Ministerio de Sanidad, la propuesta y ejecución de la política del Gobierno en materia de salud, de planificación y asistencia sanitaria, así como el ejercicio de las competencias de la Administración General del Estado para asegurar a los ciudadanos el derecho a la protección de la salud.

En su artículo 3 dispone:

1. La Dirección General de Salud Pública, Calidad e Innovación es el órgano que asume las funciones relativas a la sanidad exterior; la promoción de la salud y la prevención de las enfermedades y lesiones; la coordinación de la vigilancia en salud pública; (…).

2. Le corresponde la elaboración de los sistemas de información, la gestión de la información y la identificación de la población protegida y el acceso a la información clínica y terapéutica, el impulso de planes de salud y programas de calidad en el Sistema Nacional de Salud, incluido el Plan Nacional sobre el SIDA, así como el análisis y evaluación del funcionamiento del sistema sanitario español y su comparación con otros sistemas sanitarios. (…)".

TERCERO: El Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19, en el artículo 4.2.d) designa al Ministro de Sanidad como autoridad competente delegada en su área de responsabilidad.

CUARTO: Con fecha 28 de marzo de 2020 se publica en el BOE la Orden SND/297/2020, de 27 de marzo, por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19.

El resuelvo primero dice:

Primero. Desarrollo de soluciones tecnológicas y aplicaciones móviles para la recopilación de datos con el fin de mejorar la eficiencia operativa de los servicios sanitarios, así como la mejor atención y accesibilidad por parte de los ciudadanos.

1. Encomendar a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo urgente y operación de una aplicación informática para el apoyo en la

gestión de la crisis sanitaria ocasionada por el COVID-19. Dicha aplicación permitirá, al menos, realizar al usuario la autoevaluación en base a los síntomas médicos que comunique, acerca de la probabilidad de que esté infectado por el COVID-19, ofrecer información al usuario sobre el COVID-19 y proporcionar al usuario consejos prácticos y recomendaciones de acciones a seguir según la evaluación.

La aplicación permitirá la geolocalización del usuario a los solos efectos de verificar que se encuentra en la comunidad autónoma en que declara estar. La aplicación puede incluir dentro de sus contenidos enlaces con portales gestionados por terceros con el objeto de facilitar el acceso a información y servicios disponibles a través de Internet.

La aplicación no constituirá, en ningún caso, un servicio de diagnóstico médico, de atención de urgencias o de prescripción de tratamientos farmacológicos. La utilización de la aplicación no sustituirá en ningún caso la consulta con un profesional médico debidamente cualificado.

El responsable del tratamiento será el Ministerio de Sanidad y el encargado del tratamiento y titular de la aplicación será la Secretaría General de Administración Digital. El Ministerio de Sanidad, como responsable del tratamiento, autoriza a la Secretaría General de Administración Digital a recurrir a otros encargados en la ejecución de lo previsto en este apartado.

2. Encomendar a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de un asistente conversacional/chatbot para ser utilizado vía whatsapp y otras aplicaciones de mensajería instantánea. Proporcionará información oficial ante las preguntas de la ciudadanía. El diseño estará basado en información oficial del Ministerio de Sanidad.

El responsable del tratamiento será el Ministerio de Sanidad y el encargado del tratamiento y titular del chatbot será la Secretaría de Estado de Digitalización e Inteligencia Artificial a través de la Subdirección General de Inteligencia Artificial y Tecnologías Habilitadoras Digitales.

3. Encomendar a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de una web informativa con los recursos tecnológicos disponibles.

Se constata que la aplicación Radar COVID no está incluida dentro de las soluciones tecnológicas y aplicaciones móviles para la recopilación de datos con el fin de mejorar la eficiencia operativa de los servicios sanitarios dada su finalidad, que es distinta: la trazabilidad de los contactos.

Su finalidad se extrae, entre otros, de:

-La “Información general” facilitada por el Gobierno de España cuando indica: ¿Qué es Radar COVID?:

https://radarcovid.gob.es/faq-informacion-general

Radar COVID es una aplicación móvil desarrollada para ayudar a controlar la propagación de la COVID-19 a través de la identificación de los posibles contactos estrechos de casos confirmados a través de la tecnología Bluetooth.

Del “EXPONEN” Séptimo de la Resolución de 13 de octubre de 2020, de la Subsecre-

taría, por la que se publica el Acuerdo entre el Ministerio de Asuntos Económicos y Transformación Digital y el Ministerio de Sanidad, acerca de la aplicación "Radar COVID, que dice:

> *Séptimo.*
>
> *Que «Radar COVID» es una aplicación para dispositivos móviles que promueve la salud pública mediante un sistema de alerta de contagios por la COVID-19. La aplicación, mediante el empleo de identificadores aleatorios efímeros que no guardan relación con la identidad del teléfono móvil empleado o el usuario, detecta la intensidad de señales Bluetooth intercambiadas entre dispositivos que tienen esta aplicación descargada y activa, El dispositivo de cada usuario descarga periódicamente las claves Bluetooth de todos los usuarios de la aplicación que hayan informado a través de la misma que se les ha diagnosticado COVID-19 (previa acreditación de las autoridades sanitarias competentes), procediendo a determinar si el usuario ha establecido contacto de riesgo con alguno de ellos, verificado por las señales Bluetooth intercambiadas. Si es el caso, la aplicación le notifica este hecho, a fin de que pueda para tomar medidas, y contribuir de este modo a evitar que el virus se propague.*

QUINTO*:* En el mes de abril de 2021 se celebra una reunión que tiene por objeto abordar el "Diseño, desarrollo, piloto y evaluación de un sistema que permita la trazabilidad de contactos en relación a la pandemia ocasionada por el Covid-19".

Intervienen las siguientes personas:

Persona	*SEDIA / CCAA / Mº Sanidad / Minsait*
D.D.D.	*SEDIA*
E.E.E.	*SEDIA*
F.F.F.	*SEDIA*
G.G.G.	*SEDIA*
H.H.H.	*Mº Sanidad*
I.I.I.	*Mº Sanidad*
J.J.J.	*SEDIA*
L.L.L.	*Gobierno de Canarias*
M.M.M.	*Minsait*
N.N.N.	*Minsait*
Ñ.Ñ.Ñ.	*Minsait*
O.O.O.	*Minsait*
P.P.P.	*Minsait*
Q.Q.Q.	*Minsait*

Los asuntos tratados son:

> *Se presenta el documento anexo 20200721_Seguimiento SEDIA v5 dónde se recoge el resumen ejecutivo de las conclusiones del análisis de resultados del piloto.*

El acuerdo adoptado es:

> *Se acuerda tener listo para el próximo martes día 28/07/2020 el listado de acciones a llevar cabo sobre la app de cara a una puesta en producción inminente, ya sea en una CCAA, ciudad o a nivel nacional. Se acuerda también preparar un documento descriptivo con un resumen del funcionamiento de la*

app para que las diferentes CCAA puedan analizar su funcionamiento.

SEXTO: Con fecha 6 de mayo de 2020 el METD publica la siguiente nota de prensa:

"*España trabaja a nivel nacional y europeo para la interoperabilidad de las aplicaciones de prevención de contagios frente al COVID-19*.

La vicepresidenta tercera del Gobierno y ministra de Asuntos Económicos y Transformación Digital, Nadia Calviño, junto a los secretarios de Estado de Digitalización e Inteligencia Artificial, Carmen Artigas., y de Telecomunicaciones e Infraestructuras Digitales, Roberto Sánchez, participaron en este encuentro para buscar una posición europea común que permita aprovechar las posibilidades que ofrece la tecnología para contribuir a la gestión de la pandemia y a la posterior recuperación a nivel europeo.

Entre dichas soluciones digitales se puso el foco en las aplicaciones de prevención de contagios. En ese sentido, España destacó la importancia de encontrar un enfoque coordinado a nivel europeo para estas aplicaciones que garantice la interoperabilidad y permita realizar una salida conjunta de la emergencia sanitaria. Además, se señaló la necesidad de aprovechar el potencial que ofrece la economía digital para contribuir a la gestión de la pandemia, siendo necesario encontrar un equilibrio entre los beneficios derivados de estas innovaciones y la privacidad, la seguridad y las cuestiones éticas. (…)

La secretaria de Estado de Digitalización e Inteligencia Artificial, Carmen Artigas, compartió con las autonomías la posición de España a nivel europeo, así como los avances que prepara la Comisión Europea sobre estas herramientas digitales. El objetivo es aunar esfuerzos y compartir puntos de vista sobre las posibilidades existentes en torno al desarrollo de estas aplicaciones y su interoperabilidad, buscando respuestas coordinadas en base a las necesidades de los diferentes territorios".

SÉPTIMO: Con fecha 9 de junio de 2020 la Directora General de Salud Pública, Calidad e Innovación del MSND envió una carta al Secretario General de Administración Digital (SGAD) con el siguiente tenor:

"En relación a la prueba piloto de la aplicación móvil para la trazabilidad de contactos del COVID-19 que está previsto llevar a cabo en la Comunidad Autónoma Canarias, le comunico el visto bueno de este Ministerio para su desarrollo.

Para la realización de la misma, a nuestro juicio, debería remitirse a la Agencia Española de Protección de Datos toda la información que corresponda para garantizar el cumplimiento de la normativa vigente en esta materia.

Por otro lado, entendemos que el responsable del tratamiento de los datos de este piloto será la autoridad sanitaria de la comunidad en que se va a llevar a cabo.

Agradeciendo el trabajo que está realizando la Secretaría de Estado de Digitalización e Inteligencia Artificial en la respuesta frente al COVID-19, reciba un cordial

saludo."

OCTAVO: Con fecha 11 de junio de 2020 entra en vigor el, ya derogado, Real Decreto-ley 21/2020, de 9 de junio, de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por el COVID-19.

Los artículos 5, 26 y 27, disponían:

Artículo 5. Planes y estrategias de actuación para afrontar emergencias sanitarias. Con arreglo a lo previsto por el artículo 65 de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, se procederá a la adopción de planes y estrategias de actuación para afrontar emergencias sanitarias, mediante actuaciones coordinadas en salud pública, atendiendo a los distintos niveles de riesgo de exposición y de transmisión comunitaria de la enfermedad COVID-19 para el desarrollo de las distintas actividades contempladas en este real decreto-ley.

Artículo 26. Provisión de información esencial para la trazabilidad de contactos. Los establecimientos, medios de transporte o cualquier otro lugar, centro o entidad pública o privada en los que las autoridades sanitarias identifiquen la necesidad de realizar trazabilidad de contactos, tendrán la obligación de facilitar a las autoridades sanitarias la información de la que dispongan o que les sea solicitada relativa a la identificación y datos de contacto de las personas potencialmente afectadas.

Artículo 27. Protección de datos de carácter personal.

"1. El tratamiento de la información de carácter personal que se realice como consecuencia del desarrollo y aplicación del presente real decreto-ley 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. En particular, las obligaciones de información a los interesados relativas a los datos obtenidos por los sujetos incluidos en el ámbito de aplicación del presente real decreto-ley se ajustarán a lo dispuesto en el artículo 14 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, teniendo en cuenta las excepciones y obligaciones previstas en su apartado 5.

2. El tratamiento tendrá 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 establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Los datos recabados serán utilizados exclusivamente con esta finalidad.

3. Los responsables del tratamiento serán las comunidades autónomas, las ciudades de Ceuta y Melilla y el Ministerio de Sanidad, 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. El intercambio de datos con otros países se regirá por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, teniendo en cuenta la Decisión n.º 1082/2013/UE del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, sobre las amenazas transfronterizas graves para la salud y el Reglamento Sanitario Internacional (2005) revisado, adoptado por la 58.ª Asamblea Mundial de la Salud celebrada en Ginebra el 23 de mayo de 2005."

Se constata que este real decreto ley no habilita para el desarrollo la aplicación Radar COVID.

NOVENO: Con fecha 15 de junio de 2020 se acordó por el Secretario General de la Administración Digital la contratación de los servicios para la trazabilidad de contactos con relación a la pandemia ocasionada por la COVID 19 a Indra Tecnologías de la Información S.L.

Según consta en el "Pliego de condiciones para el diseño, desarrollo, piloto y evaluación de un sistema que permita el rastreo de contactos en relación con la pandemia ocasionada por la COVID-19" de fecha 10 y 12 de junio de 2020, apartado 1 bajo el epígrafe "Antecedentes":

La Orden SND/297/2020, de 27 de marzo, del Ministro de Sanidad encargó a la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA), del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19.

En particular, dicha Orden establece en su resolución primera, el Desarrollo de soluciones tecnológicas y aplicaciones móviles para la recopilación de datos con el fin de mejorar la eficiencia operativa de los servicios sanitarios, así como la mejor atención y accesibilidad por parte de los ciudadanos.

Adicionalmente, la Dirección General de Salud Pública, Calidad e Innovación, de la Secretaría General de Sanidad (Ministerio de Sanidad) ha dado el Visto Bueno a una prueba piloto de rastreo de contactos en relación a la COVID-19, encargando a la SEDIA el desarrollo de una aplicación móvil para tal fin.

Según consta en el objeto del contrato el proyecto de implantación tendría tres fases: fase pre-piloto, fase piloto y fase post-piloto.

El "Pliego de condiciones para el diseño, desarrollo, piloto y evaluación de un sistema que permita el rastreo de contactos en relación con la pandemia ocasionada por la covid-19", aceptado por INDRA, recoge en el objeto del contrato las necesidades a cubrir y entre otras, las siguientes cláusulas:

"5.4. Infraestructura en la nube (cloud).

Se precisará que los desarrollos del Backend se realicen en una infraestructura en la nube en modo de autogestión, para facilitar la agilidad en el desarrollo de

la solución.

No obstante, lo anterior, tanto el almacenamiento como cualquier actividad de tratamiento de datos se ubicarán en el territorio de la Unión Europea, ya sean éstos provistos y gestionados por la empresa adjudicataria o por sus contratistas y colaboradores, y se alojarán en servidores y/o centros de proceso de datos de la propia empresa adjudicataria o de sus contratistas.

…

En la medida de lo posible, se procurará la utilización de componentes en la infraestructura cloud que permitan la migración futura de la solución a la nube SARA de la AGE.

6.1. Confidencialidad en general

El contratista se compromete a garantizar la más estricta confidencialidad y reserva sobre cualquier dato o información a los que pueda tener acceso o pudiera conocer con ocasión de la ejecución del contrato, así como sobre los resultados obtenidos de su tratamiento, y a que únicamente se utilizarán para la consecución del objeto del contrato, no pudiendo comunicarlos, utilizarlos, ni cederlos a terceros bajo ningún concepto, ni siquiera para su conservación. Estas obligaciones se extienden a todas las personas que, bajo la dependencia del contratista o por su cuenta, hayan podido intervenir en cualquiera de las fases de ejecución del contrato.

La obligación de confidencialidad y reserva conlleva la de custodia e impedir el acceso a la información y documentación facilitadas y a las que resulten de su tratamiento de cualquier tercero ajeno al servicio contratado, entendiéndose como tal tanto cualquier persona ajena a la empresa contratista como cualquiera que, aun no siéndolo, no esté autorizada para acceder a tal información.

Asimismo, el contratista se compromete a velar por la integridad de los datos, es decir, a la protección de la información facilitada y a la que resulte de su tratamiento contra la modificación o destrucción no autorizada de los datos.

6.2. Protección de datos personales

Se deberá cumplir lo estipulado en la ley orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, adaptada al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y por el que se deroga la Directiva 95/46/CE(Reglamento General de Protección de Datos), incluyendo lo dispuesto en la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre y en el Real Decreto 3/2010, de 8 de enero.

Conforme a la Disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Medidas de seguridad en el ámbito del sector público, las medidas de seguridad a aplicar en el marco de los tratamientos de datos personales se corresponderán con las de la Administración púbica de origen y se ajustarán al Esquema Nacional de Seguridad.

Se requerirá a INDRA SOLUCIONES TECNOLOGÍAS DE LA INFORMACIÓN, SLU la manifestación expresa del sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos conforme a los artículos 35.1d y 122.2 de la LCSP modificado por artículo 5 del Real Decreto Ley

14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

6.3. Seguridad

INDRA SOLUCIONES TECNOLOGÍAS DE LA INFORMACIÓN, SLU implementará las medidas técnicas y organizativas de seguridad apropiadas y elaborará la documentación pertinente, de acuerdo con el correspondiente análisis de riesgos, según lo establecido en 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.

7 PROPIEDAD INTELECTUAL

Sin perjuicio de lo dispuesto en la legislación vigente en materia de propiedad intelectual, el adjudicatario acepta expresamente que la propiedad de todos los productos que sean elaborados por el adjudicatario, incluidos sus empleados y en su caso cualquier empresa subcontratada, en ejecución del Contrato y, en particular, todos los derechos de propiedad intelectual y/o industrial que deriven de los mismos, corresponde únicamente a la administración contratante, con exclusividad y sin más limitaciones que las que vengan impuestas por el ordenamiento jurídico.

A los efectos previstos en el párrafo anterior, la empresa adjudicataria se compromete a la entrega a la SGAD de toda la documentación técnica, trabajos y materiales generados, en cuyo poder quedarán a la finalización del Contrato sin que el contratista pueda conservarla, ni obtener copia de esta, ni utilizarla o facilitarla a terceros sin la expresa autorización de la SGAD, que la daría, en su caso, previa petición formal del contratista con expresión del fin."

También recoge en el ANEXO I las características del sistema aplicación móvil y el elemento backend en infraestructura pública:

ANEXO I. CARACTERÍSTICAS DEL SISTEMA APLICACIÓN MÓVIL

1. Inicio y bienvenida aplicación: aviso legal, onboarding informativo, activación de seguimiento Bluetooth. Uso de SDK Google/Apple anónimo y redirección a repositorio genérico (Backend).

a. Permite al usuario la transmisión y recepción de identificadores aleatorios a través del Bluetooth

b. Verificación del código de autorización por parte de la autoridad sanitaria ante positivo por COVID-19. De cara al piloto, como es previsible que no se disponga del servicio de la autoridad sanitaria se simulará la validación del positivo que desencadene el proceso de tracing y se pueda pilotar.

c. Envía al servidor su baliza generadora de claves efímeras en caso de positivo.

d. Pantallas estáticas informativas.

e. Interacción con el SDK google/apple, de acuerdo a la funcionalidad proporcionada:

i. Gestionar las claves aleatorias diarias:

1. Generar diariamente las claves de exposición temporales y rotar los identificadores efímeros basados en ellos.

2. Proveer las claves al Backend para usuarios diagnosticados, incluyendo los valores temporales.

3. Acepta las claves de la App para la detección de exposición, incluyendo las fechas y los niveles de riesgo de transmisión.

4. Almacena claves en el dispositivo.

ii. Gestionar el envío y escaneo Bluetooth:

1. Gestión del envío de claves.

2. Escanea claves emitidas por otros dispositivos.

3. Almacenar las claves observadas en un almacenamiento en el dispositivo.

4. Identificar cuando otro usuario en contacto ha sido un caso confirmado.

5. Calcular y proveer el riesgo de exposición a la aplicación.

6. Presentar las siguientes peticiones de permiso al usuario:

a. Antes de empezar a escanear y enviar las claves.

b. Antes de proveer al servidor las claves al servidor central tras haber sido contagiado.

2. Comunicación de casos positivos:

a. Introducción QR/código COVID-19 (manual, escáner o importación) personal y de uso único.

b. Aviso confirmación QR validado positivo: pantalla informativa.

c. Cuestionario opcional (en caso de positivo): recoge datos anónimos básicos para su tratamiento Backend App (código postal, sintomatología y su fecha, patologías previas,…).

3. Notificación de riesgo: aviso de contacto con positivo confirmado y pantalla de recomendaciones.

4. Salida de la aplicación: posibilidad de salida de la aplicación en cualquier momento, eliminando cualquier rastro de claves efímeras utilizadas.

ELEMENTO BACKEND EN INFRAESTRUCTURA PÚBLICA

1. Gestión de datos en Backend

a. Servir información necesaria para funcionamiento de la App (si se estima necesario. Alternativamente la App puede ser autocontenida).

b. Validación con el sistema de autorización sanitaria ante diagnósticos positivos (si este sistema no estuviera disponible se realizaría una Si-

mulación de esta validación). La aplicación debe comunicarse con un servidor externo (sanitario) que provea el código de autorización que confirme el positivo y pueda autorizar a subir las balizas al servicio en función del siguiente ciclo propuesto:

i. Sistema médico solicita token/QR autenticación al Backend para confirmar positivo COVID-19.

ii. Paciente recibe token/QR autenticación para confirmar el positivo COVID-19.

iii. Paciente envía el token/QR autorizado al Backend para subir su histórico de contactos.

Como es previsible que no se disponga del servicio de la autoridad sanitaria en el alcance inicial se simulará la validación del positivo que desencadene el proceso de tracing para que se pueda probar su funcionamiento.

c. Base de datos con servicio de información centralizada que permita el rastreo de contactos y la gestión de balizas.

i. Recolectar las balizas de los usuarios que hayan sido diagnosticados de COVID-19.

ii. Distribuir las balizas de los casos confirmados hacia los dispositivos.

iii. Integración servicio de autorización de positivos.

iv. Integración con sistemas Terceros. Estudio de la interoperabilidad con Backends de otros Estados para asegurar funcionalidad transfronteriza.

2. Seguridad

a. Implantación de controles para prevenir ataques específicos a nivel de aplicación.

b. Securización comunicaciones con otros dispositivos y con sistemas sanitarios.

c. Anonimización de señales entre dispositivos.

3. Simulación: capacidad de emular respuesta COVID-19 positivo, a efectos de testing (testear comportamiento de tracing).

DÉCIMO: La SEDIA ha acreditado los siguientes certificados emitidos a favor de INDRA:

- ISO 27018 Certificado de Privacidad en la Nube: Los sistemas de información que soportan los procesos de negocio y activos de información necesarios para la prestación de servicios de outsourcing de TI Administración, Soporte, Explotación e Infraestructura), tanto en entornos físicos como virtualizados cloud), según la declaración de aplicabilidad en vigor a fecha de emisión del certificado.
- ISO 27001 Certificado del Sistema de Gestión de Seguridad de la Información: Los sistemas de información que soportan los procesos de negocio y activos de información necesarios para la prestación de servi-

cios de outsourcing de TI Administración, Soporte, Explotación e Infraestructura), tanto en entornos físicos como virtualizados cloud), según la declaración de aplicabilidad en vigor a fecha de realización de la auditoría.

- STI-0014/2009 Certificado del Sistema de Gestión de Servicio de Tecnologías de la Información: El SGS de los servicios de outsourcing de TI Administración, Soporte, Explotación e Infraestructura), tanto en entornos físicos como virtualizados cloud), según el catálogo de servicios en vigor. Certificado del Sistema de Gestión de Servicio de Tecnologías de la Información.Para la gestión del sistema RADAR COVID, INDRA ha contratado los servicios de Amazón Web Services INC.

UNDÉCIMO: Con fecha 17 de junio de 2020 se celebra una reunión del grupo de trabajo interterritorial al que asisten representantes de las Comunidades Autónomas de Andalucía, Aragón, Asturias, Castilla y León, Extremadura, Galicia, Islas Baleares, Islas Canarias, La Rioja, Madrid, Murcia, Navarra y Valencia y de la ciudad autónoma de Melilla, así como por parte de la Secretaría de Estado de Digitalización e Inteligencia Artificial asisten ***G.G.G.***, Subdirector General de Impulso de la Digitalización de la Administración, ***F.F.F.***, asesor técnico para el desarrollo de la aplicación, el equipo técnico a cargo de desarrollo de la aplicación y ***R.R.R.***, asesora Gabinete.

Se expone que:

> *"…tres principales objetivos de la aplicación: preservar la salud pública, ir un paso por delante de la COVID-19 y minimizar su impacto económico facilitando el movimiento de las personas. Para ello, hay tres momentos clave a tener en cuenta: la activación del Bluetooth (que permite preservar la anonimidad de los usuarios), el reporte de diagnósticos positivos y la notificación a usuarios en riesgo de contagios.*
>
> *(…)*
>
> *También se destaca la importancia de la privacidad para la aplicación, garantizando en todo momento la anonimicidad de las personas, permitiendo que la app pueda desactivarse en cualquier momento, almacenando los datos de forma descentralizada solo durante 14 días o generando los avisos en la propia app.*
>
> *Por último, se explica cómo se comporta técnicamente la aplicación: los teléfonos intercambian identificadores Bluetooth aleatorios y, con el consentimiento del usuario, el teléfono carga el histórico de los últimos 14 días de claves en el servidor. Cada teléfono descarga periódicamente las claves Bluetooth de todas las personas diagnosticadas que lo han reportado y que han podido estar en contacto. Con ello, se envían las notificaciones de alerta de contagios."*

DUODÉCIMO: Consta un documento denominado "Diseño Piloto Covid-19 App. Presentación CCAA 17 junio 2020, elaborado por la SEDIA.

En este se definen los parámetros clave del Piloto:

a) Duración

- *15 días de APP activa*

- *Fecha de inicio tentativa: Semana del 29 de Junio.*

b) *Ubicación:*

- *San Sebastián de La Gomera (7.921 habitantes, INE datos provisionales 1/01/2020), municipio ubicado en la Isla de La Gomera.*

c) *Participantes:*

- *Residentes en el municipio captados por distintos canales de acceso al piloto.*
- *Turistas residentes en Tenerife que simulen movimiento por el municipio durante el piloto.*

d) *Alcance de Piloto: Volumen de participantes*

- *Se potenciará la mayor participación posible combinando distintos canales de acceso a la misma, estimándose un volumen entre 2.000 y 3.000 usuarios de la APP .*
- *Se establecerá aproximadamente un 10% de casos con Positivo en COVID simulado inicial, para favorecer la detección de casos de riesgo y así comprobar funcionamiento de APP.*

e) *Valoración cumplimiento objetivos*

- *Análisis datos cuantitativos*
- *Análisis cualitativo: encuestas anónimas y tests de usuarios en remoto (15 usuarios).*

También recoge los “Canales de acceso al Piloto” por los participantes:

Se proponen 4 canales de acceso a la APP para participación controlada en el piloto, a confirmar con el gobierno de Canarias y gobierno local de La Gomera

1. Comunicación directa individual a Empleados públicos

Personas que residen en San Sebastián de la Gomera y trabajan como empleados públicos en distintos ámbitos y personas que residen en Tenerife y puedan desplazarse como “turistas simulados” al municipio durante el piloto

2. Agentes Instaladores

Equipo de agentes que promoverán y ayudarán en la descarga de la APP en espacios públicos y oficinas de atención al ciudadano del municipio, potenciando la captación de personas jóvenes y mayores de 65 años

3. Teléfono de información específico

Posibilidad de habilitar un teléfono para facilitar el acceso a aquellos ciudadanos del municipio que estén interesados en participar, así como para posible comprobación simulada de contagios

4. Buzoneo postal

Valorar la posibilidad de cartas directas o folletos depositados en buzón físico a todos los residentes en el municipio que explique el piloto e invite a participar

DÉCIMO TERCERO: Consta, con fecha 23 de junio de 2020, una nota de prensa publicada por el METD, con el siguiente tenor:

"El Gobierno aprueba el desarrollo del piloto para una aplicación móvil de notificación de contactos de riesgo por COVID-19. (…)

El objetivo es que el Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, y en coordinación con el Servicio Canario de la Salud, ponga en marcha la próxima semana una prueba piloto de esta herramienta tecnológica en la isla canaria de La Gomera.

El piloto tiene como objetivo evaluar aspectos técnicos y de experiencia de uso del ciudadano, con el fin de optimizar el diseño de la aplicación y su grado de confianza. También servirá para calibrar el algoritmo de la app con el fin de garantizar la veracidad de las notificaciones. (…)

Una vez concluida y evaluada la prueba piloto en un escenario real, se podrán tomar las decisiones oportunas para la conexión con el sistema de salud de las diferentes comunidades autónomas.

Esta herramienta tecnológica se suma a las medidas ya puestas en marcha por las autoridades sanitarias para seguir los contactos de los contagios de COVID-19 y que, junto a las medidas de prevención adoptadas, están contribuyendo al control de la pandemia. El contrato aprobado en Consejo Ministros por el procedimiento de emergencia se ha suscrito con la empresa Indra Soluciones Tecnológicas de la Información S.L.U. por un importe de 330.537,52 euros, IVA incluido. (…)

Privacidad

El desarrollo utiliza un modelo descentralizado, basado en el protocolo Decentralized Privacy-Preserving Proximity Tracing (DP-3T), el más respetuoso con la privacidad del usuario. Esto implica que sólo se envían al servidor los identificadores cifrados que cada móvil emite, no los que recibe de otros terminales cercanos. Cada cierto tiempo los móviles descargan los nuevos identificadores de contagios confirmados para comparar con sus registros. Es decir, que el cotejo de datos y análisis de riesgo se lleva a cabo siempre en el móvil del usuario y no en un servidor, lo que garantiza la privacidad.

Esta aplicación cumple, por tanto, con todas las garantías fijadas por la normativa europea para salvaguardar la intimidad de la ciudadanía. Además, garantiza la

proporcionalidad y minimiza el uso de datos personales. El uso de la aplicación será voluntario y enmarcado en los límites de la emergencia sanitaria, en estricto cumplimiento de las recomendaciones de la Comisión Europea al respecto."

DÉCIMO CUARTO: Consta, con fecha 23 de junio de 2020, en la Referencia del Consejo de Ministros, el siguiente Acuerdo:

"ACUERDO por el que se toma razón de la declaración de emergencia para la contratación de los servicios de diseño, desarrollo, piloto y evaluación de un sistema que permita el rastreo de contactos en relación a la pandemia ocasionada por la COVID-19, con una duración de 5 meses, por un importe de 330.537,52 euros, IVA incluido."

"APROBADO EL DESARROLLO DEL PILOTO PARA UNA APLICACIÓN MÓVIL DE NOTIFICACIÓN DE CONTACTOS DE RIESGO POR COVID-19.

El Consejo de Ministros ha dado luz verde al contrato para diseñar, desarrollar y evaluar una prueba piloto para una aplicación móvil que permita notificar a los contactos de un usuario el posible riesgo de contagio por COVID-19. El objetivo es que el Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, y en coordinación con el Servicio Canario de la Salud, ponga en marcha la próxima semana una prueba piloto de esta herramienta tecnológica en la isla canaria de La Gomera. El piloto tiene como objetivo evaluar aspectos técnicos y de experiencia de uso del ciudadano, con el fin de optimizar el diseño de la aplicación y su grado de confianza. También servirá para calibrar el algoritmo de la app con el fin de garantizar la veracidad de las notificaciones. Una vez concluida y evaluada la prueba piloto en un escenario real, se podrán tomar las decisiones oportunas para la conexión con el sistema de salud de las diferentes comunidades autónomas. Esta herramienta tecnológica se suma a las medidas ya puestas en marcha por las autoridades sanitarias para seguir los contactos de los contagios de COVID-19 y que, junto a las medidas de prevención adoptadas, están contribuyendo al control de la pandemia. El contrato aprobado en Consejo Ministros por el procedimiento de emergencia se ha suscrito con la empresa Indra Soluciones Tecnológicas de la Información S.L.U. por un importe de 330.537,52 euros, IVA incluido."

DÉCIMO QUINTO: Con fecha 29 de junio de 2020 se lanza por el Gobierno de España el proyecto piloto que se extiende hasta el 31 de julio de 2020 en la isla de La Gomera.

En el documento de seguimiento de fecha 24.07.2020, constan las siguientes fases y fechas sobre la planificación del piloto Radar COVID:

Consta publicado un Informe de conclusiones (https://radar-resources.s3-eu-west-1.amazonaws.com/28-01-2020-InformeRadarCOVID.pdf) elaborado por la SEDIA, fechado el 28 de enero de 2021, que indica:

La app permite

• Verificar el código de autorización por parte de la autoridad sanitaria ante positivo por COVID-19

• Permite al usuario la transmisión y recepción de identificadores aleatorios a través del Bluetooth

• Envía al servidor su baliza generadora de claves efímeras en caso de positivo

• Pide al servidor las claves anónimas de usuarios contagiados de manera periódica

• Mostrar notificaciones al usuario con instrucciones de qué hacer en caso de que haya estado en contacto a otro usuario positivo COVID-19

Su desarrollo está soportado sobre la alianza Google & Apple para la implementación de un API común encargado de gestionar y proporcionar a los dispositivos claves aleatorias anónimas y su intercambio vía bluetooth a través de las siguientes funciones:

Gestionar las claves aleatorias diarias

• Generar diariamente las claves de exposición temporales y rotar los ids efímeros basados en ellos

• Provee las claves a la aplicación para usuario diagnosticados, incluyendo los valores temporales

• Acepta las claves de la app para la detección de exposición, incluyendo las fechas y los niveles de riesgo de transmisión

• Almacena claves en el dispositivo

Gestiona el envío y escaneo Bluetooth

• Gestión el envío de claves

• Escanea claves emitidas por otros dispositivos

• Almacena las claves observadas en un almacenamiento en el dispositivo

• Identifica cuando otro usuario en contacto ha sido un caso confirmado

• Cálculo y provee el riesgo de exposición a la aplicación

• Presenta las siguientes peticiones de permiso al usuario:

• Antes de empezar a escanear y enviar las claves

• Antes de proveer al servidor las claves al servidor central tras haber sido contagiado G

Objetivos y metodología del piloto

Duración:

- *15 días de APP activa (fases de monitorización y ampliación de monitorización)*
- *Fecha de inicio: Semana del 29 de junio (fase de comunicación y divulgación)*
- *Fecha de fin: semana del 20 de julio (fase de análisis de conclusiones)*

Ubicación:

San Sebastián de La Gomera (aproximadamente 10.000 habitantes incluyendo residentes, turistas y personas que se desplazan diariamente por motivos de trabajo), municipio ubicado en la Isla de La Gomera.

Participantes

- *Residentes en el municipio captados por distintos canales de acceso al piloto.*
- *Visitantes residentes en Tenerife que se desplazaron al municipio durante el piloto, captados por distintos canales de acceso al piloto.*

Alcance de Piloto: Volumen de participantes

- *Se potenciará la mayor participación posible combinando distintos canales de acceso a la misma, estimándose un volumen entre 2.000 y 3.000 usuarios de la APP*
- *Se establecerá aproximadamente un 10% de casos con Positivo en COVID simulado, para favorecer la detección de casos de riesgo y así comprobar funcionamiento de APP*

Valoración cumplimiento objetivos

- *Análisis datos cuantitativos*
- *Análisis cualitativo: encuestas anónimas y tests de usuarios en remoto (15 usuarios)*

Objetivo del piloto

(…) Así, el objetivo del piloto fue monitorizar el funcionamiento de la APP de forma controlada para:

1. Optimizar el diseño de APP (…)

2. Comportamientos y preferencias en materia de prevención de los ciudada-

nos (…)

3. Contrastar hipótesis de partida (…)

4. Obtener insights para el despliegue (…)

Alcance

Como se ha mencionado anteriormente, el piloto se ha planteado desde una perspectiva simulada y controlada, de forma que permite obtener conclusiones de valor respecto a su funcionamiento, uso y comportamiento por parte de la ciudadanía, pero limita la obtención de datos en relación a algunos aspectos:

Descarga abierta vs descarga controlada

Si bien en un primer momento se planteó la posibilidad de controlar el acceso a la descarga de la aplicación exclusivamente al público objetivo del piloto, residentes, trabajadores o visitantes de San Sebastián de la Gomera, se decidió finalmente dejarla abierta debido a 3 factores clave:

• Complejidad de implementación.

• Impacto negativo en la usabilidad por parte de los ciudadanos al tener que introducir códigos de acceso para la descarga.

• Incorporar un factor ajeno al propio funcionamiento de la aplicación en el supuesto despliegue nacional.

Privacidad vs información cualificada.

En el piloto se ha seguido la misma premisa que rige la propia aplicación, la garantía de protección de datos personales y el anonimato en el uso de Radar COVID.

En esa línea, se ha recopilado información agregada de los usuarios de la aplicación, tanto de las personas que se la descargaban, como de las personas que asumían el papel de Casos positivos o recibían notificaciones de alerta de riesgo de contagio.

Esta información agregada impide obtener información comportamental o por perfiles más cualificados de ciudadanos, así como un análisis sociológico de propagación del virus.

Simulación vs Realidad

La estrategia del piloto se basó en una simulación de casos positivos por parte de voluntarios que introdujeron el código que les fue asignado, creando por tanto un brote de propagación ficticio y forzado que no permite analizar de (sic) propagación real de la enfermedad que sería monitorizada por la aplicación.

Metodología.

Enfoque del piloto.

• Conseguir el mayor número de usuarios posible, habilitando distintos canales de acceso a la participación por parte de los ciudadanos objetivo del piloto.

• Incorporar participantes de distintos perfiles poblacionales para detectar facilitadores y barreras de uso diferentes.

• Priorizar la comprobación de la funcionalidad y experiencia de uso de la APP simulando un volumen de casos de positivos elevado (10% de la estimación de población usuaria de la APP durante el piloto) que favoreciera la generación de los KPIs clave de evaluación del piloto, pero manteniendo una tasa de incidencia acumulada prevista razonable desde el punto de vista epidemiológico (2,2%).

• Mantener el control de los casos positivos e introducción de códigos en la APP, limitando el acceso solo a muestras controladas.

• Obtener feedback directo de usuarios del piloto que permita optimizar el diseño.

Monitorización y agilidad en toma de decisiones

Con el objetivo de disponer de información continua sobre evolución de los distintos indicadores de éxito del piloto y reorientar su enfoque si era necesario para alcanzar el objetivo final, se crearon distintas herramientas de reporte y control, que permitirían incorporar los datos recogidos de forma anónima y voluntaria:

• Plantilla diaria de registro de participantes captados por promotores, recogiendo información agregada de sexo y edad del conjunto de personas captadas en cada jornada de promoción.

• Plantilla diaria de entrega de códigos positivos por promotores, recogiendo también información agregada de sexo y edad de las personas a las que se asignaba el papel de voluntario positivo.

• Plantilla diaria de registro de llamadas en CAU, según motivo de llamada

• Plantilla diaria de registro de contenido de llamadas por riesgo de alerta, para la que se creó un argumentario de llamada.

• Cuadro de mando global de indicadores clave de participantes, códigos, notificaciones y demás información que se especifica en el apartado de conclusiones.

El seguimiento continuo de la información permitió tomar decisiones ágiles como el desplazamiento de los promotores a nuevas zonas ante posible saturación de las zonas iniciales o la incorporación de nueva oleada de contagios en naviera.

Resultados del piloto Metodología de evaluación de la eficacia de Radar COVID

Las cuestiones relevantes para evaluar la eficacia de Radar COVID son:

Comportamiento del usuario y actitud hacia la aplicación, evaluando si éste ha favorecido el propósito de Radar COVID en función de:

Adopción ¿Está Radar COVID logrando suficiente masa crítica para ser eficaz? ¿Se adoptan las nuevas versiones de la app?

Compromiso y participación ¿Está motivado el usuario y cumple las instrucciones que facilitan la contención de la pandemia? ¿Es rápido en el cumplimiento de las instrucciones? ¿Cómo de positiva es la foto al contrastarla con iniciativas comparables en Europa?

Retención

Una vez instalada, ¿el usuario continúa con la aplicación activa y en uso o, por el contrario, pierde el interés y la desactiva? Desempeño de la aplicación en la detección del riesgo de contagio entre ciudadanos:

Simulación del brote ¿Cuántos contactos estrechos es capaz de detectar Radar COVID por cada caso positivo confirmado a través de la aplicación?

Resultados que permiten evaluar la eficacia de Radar COVID

Adopción

¿Se ha alcanzado un nivel de adopción que permita obtener conclusiones de funcionamiento y eficacia de Radar COVID?

El nivel de adopción conseguido durante el piloto ha permitido comprobar el funcionamiento de la aplicación y testar su eficacia ante casos positivos de COVID-19, si bien su resultado no es extrapolable al despliegue nacional al haber tenido un nivel promoción en el municipio muy elevado y dirigido.

A la finalización del piloto se habían conseguido más de 58.000 descargas totales, el 90% en Android, y solo en el periodo de activación directa en San Sebastián de la Gomera, entre los días 6 y 20 de julio, la cifra ronda las 11.000 descargas.

Por las limitaciones indicadas en el apartado anterior, no es factible diferenciar cuántas de estas descargas pertenecen a SS de La Gomera para confirmar la previsión objetivo de las 3.500 descargas aproximadamente en el municipio que representaría el 35% de adopción, si bien se pueden realizar algunas estimaciones que sí confirmarían haber alcanzado el umbral deseado, siendo conservadores en la previsión:

• Descargas "asistidas": 924. Descargas que han sido realizadas de forma fehaciente por los agentes promotores ubicados tanto en el municipio de SS de

La Gomera como en los barcos colaboradores en el piloto.

• Empleados públicos: Se impulsó la participación de 758 empleados públicos de los 3 ámbitos institucionales (Ayuntamiento de SS de La Gomera, Cabildo de La Gomera y Servicios de Salud) y se les invitó a que promovieran también la descarga en su entorno más cercano.

• Si asumimos que la tasa de participación es similar a la tasa obtenida de introducción de códigos positivos (61%) y que cada empleado público lo compartió con una media de 3 personas de su entorno más próximo, obtenemos una participación promovida por este colectivo de unos 1.850 usuarios de la aplicación.

• Participación espontánea: Si consideramos que las campañas de difusión y promoción de la iniciativa realizadas a través de ruedas de prensa, notas informativas, actividad en redes sociales e información disponible en los aviones de la compañía BINTER, despertaran el interés de la población del municipio e impactara en una descarga voluntaria de al menos un 2% de la población, se habrían conseguido 200 descargas adicionales.

• Descargas web del Gobierno de Canarias: se han registrado 241 clics al enlace de descarga directa en la web; estimamos que todos los clics han materializado la descarga 66 Con estas estimaciones, se puede concluir que la cifra alcanzada de descarga se sitúa en 3.215 y por tanto ha permitido evaluar la eficacia y funcionamiento de Radar COVID, ya que la cifra final real estimamos que pueda situarse entre este umbral mínimo de 3.215 y las 11.675 descargas que se han producido durante la duración del piloto. Cabe destacar que la tasa de adopción es especialmente alta, considerando adicionalmente que, de los 10.000 habitantes de San Sebastián de La Gomera, aproximadamente un 10% de la población tiene una edad inferior a 10 años (edad límite inferior considerada para tener smartphone y un 11% son personas mayores de 75 años donde podría haber menor tasa de penetración de estos dispositivos, siguiendo la distribución de población publicada por el INE correspondiente a 1 de Enero de 2020 para el conjunto de la isla de La Gomera. Extrapolando al conjunto de la población nacional en el momento de despliegue global, será difícil conseguir esta tasa de adopción, si bien de cara al piloto ha permitido realizar los análisis necesarios del funcionamiento de la app.

DÉCIMO SEXTO: Consta un documento denominado “COVID Radar. Secretaría General de Administración Digital. Funcionamiento general. Madrid, Junio 2020” donde la SEDIA informa lo siguiente:

Estrategia de la app Covid-19

Objetivos de la app

• Preservar la salud pública sin renunciar a la privacidad de los ciudadanos

• Ir un paso por delante del Covid-19: alertar a personas en riesgo es contener el virus de forma proactiva

• Minimizar el impacto económico del Covid-19, al controlar la pandemia sin medidas drásticas y facilitando el movimiento de personas

Los momentos clave

• Activación del Bluetooth

• Reporte de diagnósticos positivos

• Notificación a usuarios en riesgo de contagio

Foco en privacidad

La app cuenta con un proceso de gestión de datos con la privacidad por diseño, velando en todo momento por la anonimidad de los usuarios, según la normativa vigente y estándares europeos.

Las medidas de privacidad contempladas en la primera versión de la solución son las siguientes:

• No se requiere login, ni se solicita al usuario ningún dato personal sea identificativo o no

• El usuario puede desactivar la app cuando quiera

• Para registrar las interacciones entre dispositivos de forma anonimizada, se generan identificadores aleatorios cambiantes que preservan la identidad de los dispositivos

• El acceso a los datos de dichas interacciones se realiza únicamente cuando se diagnostica un nuevo positivo COVID-19 o cuando el Servicio Médico lo considera necesario

• Los datos se almacenan de forma descentralizada durante un plazo de 14 días, tras el cual son suprimidos

• Las notificaciones a usuarios expuestos al Covid-19 se generan en la propia app, sin requerir identificar el dispositivo o el número de teléfono del usuario

También contiene la "Descripción funcional de la app" y el "Funcionamiento de las alertas de contagio Bluetooth".

DÉCIMO SÉPTIMO: Consta un documento denominado "Radar COVID. Seguimiento: 17.07.2020", elaborado por la SEDIA junto al Servicio Canario de Salud, el Gobierno de Canarias, el Gobierno del Cabildo de La Gomera y el Ayuntamiento de San Sebastián de La Gomera donde se informa lo siguiente:

¿Qué observamos diariamente?

Comportamiento del ciudadano

Descargas Acumuladas Radar COVID: 54.591

- *Hay más de **54.000 descargas a nivel nacional**, el 94% en Android*
- *De las casi 10.000 descargas desde el inicio del piloto, nuestros **promotores** han confirmado **924 descargas**, más **59 en web***
- *Se ha impulsado la descarga entre **758 voluntarios** o empleados públicos*

Y respecto al Plan de Acción Fase 3- Semana 20 a 27 julio Análisis de datos y obtención de conclusiones, dice:

DÉCIMO OCTAVO: Con fecha 21 de julio de 2020 se celebra una reunión que tiene por objeto el "Diseño, desarrollo, piloto y evaluación de un sistema que permita la trazabilidad de contactos en relación a la pandemia ocasionada por el Covid-19".

Asisten:

Persona	SEDIA / CCAA / Mº Sanidad / Minsait
D.D.D.	SEDIA
E.E.E.	SEDIA
F.F.F.	SEDIA
G.G.G.	SEDIA
S.S.S.	Gobierno de Canarias
T.T.T.	SEDIA
H.H.H.	Mº Sanidad
I.I.I.	Mº Sanidad
L.L.L.	Gobierno de Canarias
M.M.M.	Minsait
N.N.N.	Minsait
Ñ.Ñ.Ñ.	Minsait
O.O.O.	Minsait
Q.Q.Q.	Minsait

Asuntos tratados:

Se presenta el documento anexo 20200717_Seguimiento SEDIA v13.PPTX dónde se recogen los avances en el piloto Radar COVID.

Acuerdos adoptados:

Se acuerda presentar en el próximo comité de seguimiento un informe completo con el análisis de las conclusiones que se ha extraído de la ejecución ya fi-

nalizada del piloto en la isla de La Gomera.

DÉCIMO NOVENO: Consta un documento denominado “Radar COVID. Seguimiento: 24.07.2020” elaborado por la SEDIA junto al Servicio Canario de Salud, el Gobierno de Canarias, el Gobierno del Cabildo de La Gomera y el Ayuntamiento de San Sebastián de La Gomera, donde se informa lo siguiente:

Escalada e integración con Servicios Sanitarios

Tras recopilar propuestas de las Comunidades Autónomas, nos decantamos por un esquema de generación de códigos centralizado y gestión descentralizada

Análisis de datos

Se han analizado los resultados del piloto en base a:

Grado de adopción y retención

Participación y simulación de oleadas

Detección de contactos estrechos

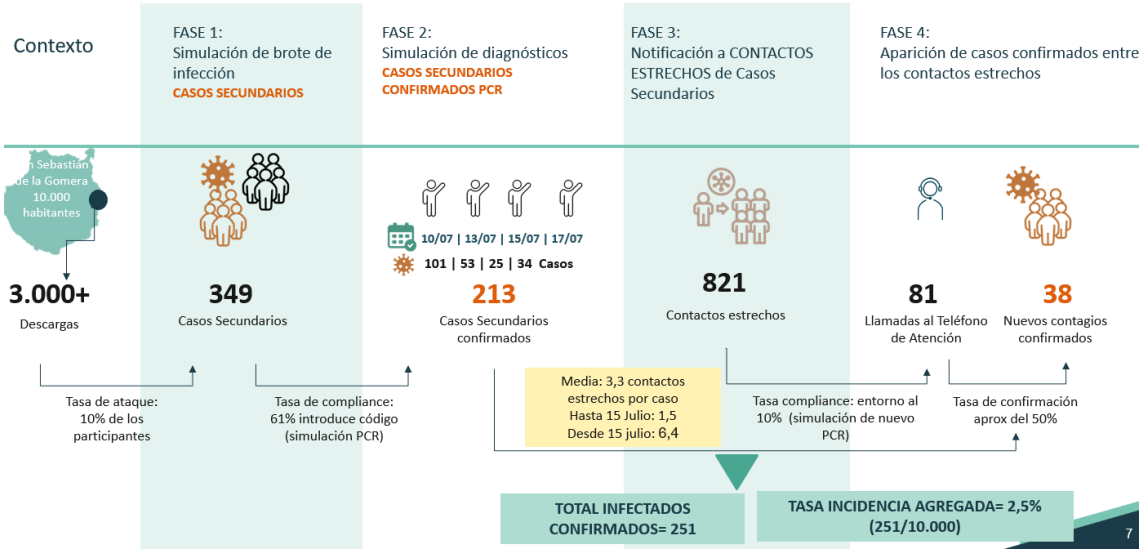
Feedback de usuarios

Resultados del piloto. ¿Qué conclusiones extraemos sobre el éxito del piloto?

Los usuarios continúan utilizando Radar COVID una vez instalada, como muestra el registro de apps activas: 12.700 Aplicaciones activas de media, con una variación de +/-5% entre sus máximos y mínimos (13.417 y 12.116)

Radar COVID es efectivo detectando contactos estrechos desde su recalibrado el día 15 de julio, al poder detectar contactos de personas cercanas al usuario y desconocidos*

Respecto a la “Simulación de brote Aplicación Radar COVID: datos finales” se informa:



¿Qué recomendaciones o enseñanzas de utilidad extraemos de cara a un escalado nacional?

Análisis:

- *Instrumentación para recopilación de datos anónimos para analizar el desempeño de Radar COVID con mayor precisión que la que la anonimidad total actual facilita.*
- *Calibrado: seguimiento estadísticas agregadas y de llamadas al call center para calibrado de pesos del Bluetooth de forma que se evite generar sobrealerta sin renunciar a un volumen útil de notificaciones de contacto estrecho generadas.*

VIGÉSIMO: Con fecha 27 de julio de 2020 se celebra una reunión que tiene por objeto el "Diseño, desarrollo, piloto y evaluación de un sistema que permita la trazabilidad de contactos en relación a la pandemia ocasionada por el Covid-19".

Constan como asistentes:

Persona	SEDIA / CCAA / Mº Sanidad / Minsait
D.D.D.	SEDIA
E.E.E.	SEDIA
F.F.F.	SEDIA
G.G.G.	SEDIA
H.H.H.	Mº Sanidad
I.I.I.	Mº Sanidad
J.J.J.	SEDIA
L.L.L.	Gobierno de Canarias
M.M.M.	Minsait

Persona	SEDIA / CCAA / Mº Sanidad / Minsait
N.N.N.	Minsait
Ñ.Ñ.Ñ.	Minsait
O.O.O.	Minsait
P.P.P.	Minsait
Q.Q.Q.	Minsait

Asuntos tratados:

Se presenta el documento anexo 20200721_Seguimiento SEDIA v5 dónde se recoge el resumen ejecutivo de las conclusiones del análisis de resultados del piloto.

Acuerdos adoptados:

Se acuerda tener listo para el próximo martes día 28/07/2020 el listado de acciones a llevar cabo sobre la app de cara a una puesta en producción inminente, ya sea en una CCAA, ciudad o a nivel nacional. Se acuerda también preparar un documento descriptivo con un resumen del funcionamiento de la app para que las diferentes CCAA puedan analizar su funcionamiento.

VIGÉSIMO PRIMERO: Consta un documento denominado "Radar COVID. Seguimiento de proyecto 31.07.2020", donde la SEDIA define las actividades de lanzamiento recomendadas para el roll out:

SEDIA / MINSAIT
Personalización datos de contacto de CCAA –información usuario y atención positivos
Eliminar encuesta usuario
Eliminar referencias piloto la Gomera
Certificado publicación app
Subir "5" días de TEKs (verificar con MS)
Cambiar nomenclatura de estados actuales
Multiidioma: Inglés
Traducción de textos de la aplicación a inglés
Dosier remitido AEPD
Generar y enviar listado cifrado de códigos positivos a gestionar por la CCAA
Revisión política de privacidad y términos de uso para eliminar referencias a piloto.
Confirmar apertura con Google /Apple
Documento app desde punto de vista Sanidad

COMUNIDADES AUTÓNOMAS
Difusión de aplicación en CCAA para favorecer la adopción: Rueda de prensa, RRSS, promotores locales, medios de comunicación, webs oficiales…
Habilitar teléfono de atención y correo electrónico para consultas relacionadas con aplicación
Facilitar teléfono y dirección de correo electrónico a utilizar para la personalización de CCAA
Definir flujo de reporte y gestión de notificaciones de riesgo de alerta de contagio
Diseñar y gestionar circuito interno de códigos positivos (distribución, control y registro)
Revisar KPIs a implantar revisar
Definir interlocutor técnico por cada CCAA
En caso de apoyo de agentes promotores, formación sobre aplicación y resolución de dudas
Diseñar y coordinar comunicaciones directas con stakeholders clave de la CCAA
Definir sistema de reporte y control de actividad derivada de APP.
Establecer un mecanismo de obtención de feedback sobre funcionamiento e impacto de la APP en usuarios y sistema de salud
Automatización de KPIs

MINISTERIO DE SANIDAD
Validación Informe de Análisis de Conclusiones
Validación guía de app para Mº Sanidad
Grupo de trabajo **Mº Sanidad** + CCAA + SEDIA (procedimientos, gestión códigos, protocolos actuación, …)
Limitar a 5 días previos a la introducción de código el listado de claves positivas enviadas al servidor central
Enviar al servidor el listado de claves positivas desde 2 días anteriores al comienzo de síntomas
¿Incorporar grupo REDETS?

Actividades recomendadas

VIGÉSIMO SEGUNDO: Con fecha 3 de agosto de 2020 el METD publica esta nota de prensa:

"La aplicación móvil de alerta de contagios Radar COVID supera su fase de pruebas cumpliendo todos los objetivos marcados. (…)

Es lo que ha explicado la secretaria de Estado de Digitalización e Inteligencia Arti-

ficial, Carmen Artigas, en una rueda de prensa en la que ha compartido los resultados obtenidos durante el piloto. Junto a ella han intervenido también A.A.C., directora general de Salud Pública e Innovación del Ministerio de Sanidad, A.A.D., director general de Modernización y Calidad de los Servicios del Gobierno de Canarias, G.G.G., subdirector general de Impulso de la Digitalización de la Administración, y F.F.F., asesor técnico del proyecto."

Éxito de adopción, compromiso, retención y funcionamiento.

La prueba arrancó el pasado 29 de junio y se ha desarrollado hasta este pasado 31 de julio, tiempo durante el que se han simulado cuatro oleadas de rebrotes ficticios de COVID-19. Durante su desarrollo, y a pesar de que sólo funcionaba en la isla de La Gomera, más de 60.000 personas descargaron la app en toda España.

El primer objetivo del piloto consistía en evaluar precisamente la adopción de la herramienta, es decir, el número de personas que la descargarían, y se fijó un objetivo de 3.000 participantes para La Gomera, meta que ha sido superada según los datos obtenidos durante la prueba.

Un segundo objetivo consistía en medir la retención, en referencia al número de usuarios que mantuvieron la app activa después de haberla descargado. Los resultados, también satisfactorios, apuntan a un 83% promedio de retención alcanzada.

Además, se analizaba el compromiso de los usuarios en la comunicación de positivos ficticios, lográndose un 61% de comunicaciones activas, de las que el 78% se produjeron en las 24 horas siguientes a haber recibido el código de contagio simulado.
Otro de los objetivos trazados en el piloto fue medir el funcionamiento de la app en el traceo de contactos, consiguiendo una media de 6,4 contactos estrechos de riesgo detectados por positivo simulado confirmado. Esa cifra supone casi doblar la eficiencia actual de los traceadores manuales, que en Canarias detectan una media de 3,5 contactos. (…)

VIGÉSIMO TERCERO: Con fecha 5 de agosto de 2020 se celebra una reunión que tiene por objeto el "Diseño, desarrollo, piloto y evaluación de un sistema que permita la trazabilidad de contactos en relación a la pandemia ocasionada por el Covid-19".

Constan como asistentes:

Persona	SEDIA / CCAA / Mº Sanidad / Minsait
D.D.D.	SEDIA
Dª F.F.F.	SEDIA
G.G.G.	SEDIA
V.V.V.	SEDIA
I.I.I.	Mº Sanidad
W.W.W.	CCAES
X.X.X.	CCAES
M.M.M.	Minsait

Persona	SEDIA / CCAA / Mº Sanidad / Minsait
N.N.N.	Minsait
Ñ.Ñ.Ñ.	Minsait
O.O.O.	Minsait
Y.Y.Y.	Minsait
Q.Q.Q.	Minsait

Acuerdos adoptados:

Se acuerda tener listo para el lunes día 10/08/2020 la app introduciendo los cambios comentados en el documentos anexo facilitando una salida de emergencia en el corto plazo a aquellas CCAA que lo soliciten y seguir avanzando en el desarrollo de las versiones para salida a nivel nacional.

VIGÉSIMO CUARTO: Con fecha 5 de agosto de 2020 se publica en el Boletín Oficial del Estado el Real Decreto 735/2020, de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio de Sanidad, y se modifica el Real Decreto 139/2020, de 28 de enero, por el que se establece la estructura orgánica básica de los departamentos ministeriales.

En el preámbulo del real decreto 735/2020, se dice:

> *"(…) Para poder acometer de manera eficaz estas nuevas medidas, así como con el fin de hacer frente al incremento del volumen de trabajo en el Ministerio de Sanidad a raíz de la pandemia ocasionada por el COVID-19, se hace necesario reforzar la estructura de dicho Departamento. Por ello, mediante el Real Decreto 722/2020, de 31 de julio, por el que se modifica el Real Decreto 2/2020, de 12 de enero, por el que se reestructuran los departamentos ministeriales, se dispuso la creación de una nueva Secretaría de Estado de Sanidad, con el objetivo de fortalecer el ejercicio de las competencias en materia de sanidad reservadas constitucionalmente a la Administración General del Estado.*
>
> *Mediante el presente real decreto se refuerza adicionalmente la estructura del Ministerio de Sanidad, contemplándose la creación de la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud, de la que dependerá la Dirección General de Salud Digital y Sistemas de Información para el Sistema Nacional de Salud, con el objetivo de abordar los proyectos de modernización, mejora y transformación del Sistema Nacional de Salud, a la luz de los nuevos retos derivados de la pandemia ocasionada por el COVID-19, y en particular los relacionados con la salud digital, la interoperabilidad y los servicios en red en el ámbito nacional, europeo e internacional, así como los sistemas de información sanitarios, fomentando la incorporación de las prestaciones de las tecnologías emergentes de última generación, tales como el análisis de datos («big data»), la inteligencia artificial o la analítica predictiva, entre otros, en el ámbito de la salud."*

Asimismo, la Disposición final primera del real decreto 735/2020 dispone:

> *"Modificación del Real Decreto 139/2020, de 28 de enero, por el que se establece la estructura orgánica básica de los departamentos ministeriales.*

Se modifica el artículo 16 del Real Decreto 139/2020, de 28 de enero, por el que se establece la estructura orgánica básica de los departamentos ministeriales, que queda redactado como sigue:

«Artículo 16. Ministerio de Sanidad.

1. El Ministerio de Sanidad se estructura en los siguientes órganos superiores y directivos:

A) La Secretaría de Estado de Sanidad, de la que dependen los siguientes órganos directivos:

1.º La Dirección General de Salud Pública.

2.º La Dirección General de Cartera Común de Servicios del Sistema Nacional de Salud y Farmacia.

3.º La Dirección General de Ordenación Profesional.

4.º La Delegación del Gobierno para el Plan Nacional sobre Drogas, con rango de Dirección General.

B) La Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud, con rango de Subsecretaría, de la que depende la Dirección General de Salud Digital y Sistemas de Información para el Sistema Nacional de Salud.

C) La Subsecretaría de Sanidad, de la que depende la Secretaría General Técnica.

2. Quedan suprimidas la Secretaría General de Sanidad y Consumo y la Secretaría General de Sanidad, así como la Dirección General de Salud Pública, Calidad e Innovación y la Dirección General de Cartera Básica de Servicios del Sistema Nacional de Salud y Farmacia."

Las funciones de la DGSP constan en el artículo 3 del real decreto 735/2020 que dice:

1. La Dirección General de Salud Pública es el órgano que asume las funciones relativas a la sanidad exterior; la promoción de la salud y la prevención de las enfermedades y lesiones; la coordinación de la vigilancia en salud pública; (…).

Se constata que, la previsión que se contenía en el Real Decreto 454/2020, de 10 de marzo, en el artículo 3.2 relativa a que "*Le corresponde la elaboración de los sistemas de información, la gestión de la información y la identificación de la población protegida y el acceso a la información clínica y terapéutica",* ahora es atribuida a la SGSDII en el artículo 7.1 del real decreto 735/2020, que dice:

Artículo 7. La Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud.

1. La Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud es el órgano directivo del Departamento al que corresponde abordar los proyectos de modernización, innovación, mejora y transfor-

mación del Sistema Nacional de Salud a la luz de los nuevos retos derivados de la pandemia por COVID-19, en particular los relacionados con la salud digital y los sistemas de información. Asimismo, le corresponde la realización de actividades tendentes a la traslación de la innovación y avances de la investigación al Sistema Nacional de Salud, sin perjuicio de las competencias atribuidas al Ministerio de Ciencia e Innovación y a las comunidades autónomas. Le corresponde, igualmente, la elaboración de los sistemas de información, la gestión de la información y la identificación de la población protegida y el acceso a la información clínica y terapéutica. Igualmente le compete el control de la información sanitaria, en el ámbito de competencias del Departamento.

Se constatan las siguientes competencias a favor de la SGSDII atribuidas en los apartados d) y j) del artículo 7.4 del real decreto 735/2020:

d) Realizar las actuaciones necesarias para el desarrollo y mantenimiento del Sistema de Información Sanitaria del Sistema Nacional de Salud definido en el capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, garantizando su normalización, comparabilidad, transparencia y accesibilidad dentro del marco legal de protección de datos personales. (…)

j) Coordinar y supervisar la política de protección de datos en cumplimiento de la normativa aplicable en esta materia en el ámbito de las competencias del Departamento.

Se constata que la SGSDII no interviene en el desarrollo del proyecto piloto dado que se crea con el Real Decreto 735/2020, de 4 de agosto.

VIGÉSIMO QUINTO: En la versión inicial de la "Política de Privacidad de la Aplicación Radar COVID" publicada el día 7 de agosto de 2020 junto con la versión 1.0 de la aplicación Radar COVID (versión piloto), consta la siguiente información:

Por favor, lee detenidamente esta política de privacidad para usuarios de la aplicación móvil "Radar COVID" (o la "Aplicación"), donde podrás encontrar toda la información sobre los datos que utilizamos, cómo lo usamos y qué control tienes sobre los mismos.

AVISO IMPORTANTE:

El USUARIO queda avisado de que la utilización de la Aplicación NO CONSTITUYE EN NINGÚN CASO UN SERVICIO DE DIAGNÓSTICO MÉDICO, DE ATENCIÓN DE URGENCIAS O DE PRESCRIPCIÓN DE TRATAMIENTOS FARMACOLÓGICOS, pues la utilización de la Aplicación no podría en ningún caso sustituir la consulta presencial personal frente a un profesional médico debidamente cualificado.

1. ¿Qué es Radar COVID?

Radar COVID es una aplicación para dispositivos móviles de alerta de contagios del virus SARS-CoV-2, cuyo TITULAR es la Secretaría General de Administración Digital, dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital.

Gracias a Radar COVID, aquellos usuarios que se hayan descargado la aplicación y acepten su uso recibirán una notificación en caso de que en los catorce días anteriores a esa notificación hayan estado expuestos a un contacto epidemiológico (a menos de dos metros y más de 15 minutos) con otro usuario (totalmente anónimo) que haya declarado en la aplicación haber dado un resultado positivo en la prueba de COVID 19 (previa acreditación de las autoridades sanitarias). La aplicación le informará exclusivamente sobre el día (dentro de esos catorce anteriores) en que se haya producido la exposición al contacto pero no sobre la identidad del usuario al que haya quedado expuesto (información imposible al ser una aplicación que no solicita, utiliza ni almacena datos de carácter personal de los usuarios) ni la identificación del dispositivo de este, ni sobre el momento o lugar en que la exposición se haya producido.

Recibida una notificación, la aplicación facilitará al usuario expuesto información para la adopción de medidas preventivas y asistenciales, para contribuir con ello a contener la propagación del virus.

El éxito de la aplicación como herramienta que contribuya a la contención de la propagación está directamente vinculado a que los usuarios sean conscientes, y actúen en consecuencia, de que, a pesar de que comunicar a la aplicación que se ha obtenido un resultado positivo en la prueba de COVID 19 (previa acreditación de las autoridades sanitarias) es voluntario, el no comunicarlo y ser un mero receptor de información de terceros usuarios hace que la aplicación pierda su utilidad preventiva no solo para los demás usuarios sino para el resto de la población en general. El carácter completamente anónimo debería animar, sin duda, al ejercicio de esta actuación responsable.

2. ¿Cómo funciona la aplicación?

Una vez que te hayas descargado la aplicación, aceptes las condiciones de uso y la política de privacidad y comiences a utilizarla, tu dispositivo móvil generará cada día un identificador pseudo-aleatorio llamado "clave de exposición temporal" con un tamaño de 16 caracteres (16 bytes o 128 bits) que servirá para derivar los "identificadores efímeros Bluetooth" que son intercambiados con otros teléfonos móviles próximos que también tengan descargada la aplicación RadarCOVID.

Los "identificadores efímeros Bluetooth" son códigos pseudo-aleatorios con un tamaño de 16 caracteres (16 bytes, o 128 bits), que se generan por tu teléfono móvil cada 10-20 minutos, a partir de la "clave de exposición temporal" diaria. Estos códigos no contienen información personal, que permita identificar al teléfono móvil o al usuario del mismo. Estos "identificadores efímeros Bluetooth" son transmitidos por tu teléfono móvil varias veces por segundo a dispositivos cercanos, accesibles a través de Bluetooth Low Energy, produciendo un intercambio de códigos aleatorios entre dispositivos para que puedan ser almacenados por teléfonos próximos que hayan descargado la aplicación. De igual manera, cada cinco minutos, tu teléfono móvil escuchará los identificadores efímeros Bluetooth que son transmitidos por otros teléfonos móviles que tengan la aplicación y los almacenará para calcular si has estado con otro usuario contagiado por COVID-19 a lo largo de los últimos 14 días.

Tu teléfono almacena las claves de exposición temporal que has generado en los últimos 14 días. Recuerda que estas claves se generan aleatoriamente y no sirven para identificar a tu teléfono móvil ni al USUARIO del mismo.

Si has recibido un diagnóstico positivo por COVID-19, puedes introducir voluntariamente en la aplicación el "código de confirmación de un solo uso" que te facilitará tu Servicio Público de Salud y que será validado en nuestro servidor. En ese momento, la aplicación te solicitará tu consentimiento para remitir a nuestro servidor las 14 últimas claves de exposición temporal almacenadas en tu teléfono, por tanto, solo si lo prestas, éstas se enviarán al servidor de la aplicación que, después de verificar la exactitud del código, servirán para componer un listado diario de claves de exposición temporal de personas contagiadas por COVID-19 que son descargados diariamente desde el servidor por todas las aplicaciones Radar COVID que estén en funcionamiento.

La información de estos listados sirve para que en tu propio teléfono se pueda comprobar si has tenido contacto estrecho (menos de dos metros y más de 15 minutos) con personas que han reportado un contagio por COVID-19, sin identificar ni a la persona, ni el lugar de la exposición, ni el dispositivo móvil, ni ningún dato personal tuyo o de la otra persona. Es decir, la aplicación descarga periódicamente las claves de exposición temporal compartidas voluntariamente por los usuarios diagnosticados por COVID-19 del servidor, para compararlas con los códigos aleatorios registrados en los días anteriores como resultado de contactos con otros usuarios. Si se encuentra una coincidencia, la aplicación ejecuta un algoritmo en el dispositivo que, en función de la duración y la distancia estimada del contacto, y de acuerdo con los criterios establecidos por las autoridades sanitarias, decide si se muestra una notificación en el dispositivo del usuario expuesto al riesgo de contagio, advirtiéndole del contacto, comunicándole la fecha del mismo e invitándolo a auto-confinarse, y contactar con las autoridades sanitarias.

Estas claves remitidas al servidor no permiten la identificación directa de los usuarios y son necesarias para garantizar el correcto funcionamiento del sistema de alerta de contagios

3. ¿Qué datos tratamos sobre ti?

Los datos manejados por la aplicación no permiten la identificación directa del usuario o de su dispositivo, y son solo los necesarios para el único fin de informarte de que has estado expuesto a una situación de riesgo de contagio por la COVID-19, así como para facilitar la posible adopción de medidas preventivas y asistenciales.

En ningún caso se rastrearán los movimientos de los USUARIOS, excluyendo así cualquier forma de geolocalización.

Como parte del sistema de alerta de contagios de la COVID-19, se procesarán los siguientes datos para los usuarios que hayan dado positivo por COVID-19 para los fines especificados a continuación:

Las claves de exposición temporal con las que el dispositivo del usuario ha generado los códigos aleatorios enviados (identificadores efímeros Bluetooth), a los dispositivos con los que el usuario ha entrado en contacto, hasta un máximo de 14 días anteriores. Estas claves no guardan relación alguna con la identidad del USUARIO, y se suben al servidor para que puedan ser descargadas por aplicaciones similares en poder de otros usuarios. Con estas claves, mediante un procesamiento que tiene lugar en el teléfono móvil de forma descentralizada, se puede advertir al USUARIO sobre el riesgo de contagio por haber

estado en contacto reciente con una persona que ha sido diagnosticada por COVID-19, sin que la aplicación pueda derivar su identidad o el lugar donde tuvo lugar el contacto.

Un código de confirmación de un solo uso de 12 dígitos facilitado por las autoridades sanitarias en caso de prueba positiva por COVID-19. Este código debe ser informado por el usuario para permitir la carga voluntaria de las claves de exposición al servidor.

Cuestionario voluntario para la recogida de información sobre la experiencia de uso de la aplicación, comprensión de la misma o percepción sobre la privacidad entre otros.

Toda la información se recogerá con fines estrictamente de interés público en el ámbito de la salud pública, y ante la situación de emergencia sanitaria decretada, a fin de proteger y salvaguardar un interés esencial para la vida de las personas, en los términos descritos en esta política de privacidad.

La legislación aplicable se enumera a continuación:

Reglamento (UE) 2016/679, 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).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Ley 14/1986, de 25 de abril, General de Sanidad

Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública.

Ley 33/2011, de 4 de octubre, General de Salud Pública.

Real Decreto 463/2020 de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 que atribuye al Ministro de Sanidad la necesaria competencia en todo el territorio nacional.

Orden Ministerial SND/297/2020 de 27 de marzo, por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de nuevas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19.

4. ¿Cómo obtenemos y de dónde proceden tus datos?

El código de confirmación de positivo por COVID-19 facilitado por el Servicio Público de Salud. Esto permitirá la subida al servidor del sistema de alerta de contagios las claves de exposición temporal con las que el dispositivo del usuario ha generado los códigos aleatorios enviados (identificadores efímeros Bluetooth), a los dispositivos con los que el usuario ha entrado en contacto, hasta un máximo de 14 días anteriores. Estas claves únicamente se suben al servidor con el consentimiento explícito e inequívoco del USUARIO, al haber introducido un código de confirmación de positivo por COVID-19.

5. ¿Para qué y por qué utilizamos tus datos?

La recogida, almacenamiento, modificación, estructuración y en su caso, eliminación, de los datos generados, constituirán operaciones de tratamiento llevadas a cabo por el Titular, con la finalidad de garantizar el correcto funcionamiento de la App, mantener la relación de prestación del servicio con el Usuario, y para la gestión, administración, información, prestación y mejora del servicio.

La información y datos recogidos a través de la Aplicación serán tratados con fines estrictamente de interés público en el ámbito de la salud pública, ante la actual situación de emergencia sanitaria como consecuencia de la pandemia del COVID-19 y la necesidad de su control y propagación, así como para garantizar intereses vitales tuyos o de terceros, de conformidad con la normativa de protección de datos vigente.

A tal efecto, utilizamos tus datos para prestarte el servicio de "Radar COVID" y para que puedas hacer uso de sus funcionalidades de acuerdo con sus condiciones de uso. De conformidad con el Reglamento General de Protección de Datos (RGPD) así como cualquier legislación nacional que resulte aplicable, la Secretaría General de Administración Digital tratará todos los datos generados durante el uso de la App para las siguientes finalidades:

Ofrecerte información sobre contactos considerados de riesgo de exposición a la COVID-19.

Proporcionarte consejos prácticos y recomendaciones de acciones a seguir según se produzcan situaciones de riesgo de cara a la cuarentena o auto-cuarentena.

Este tratamiento se llevará a cabo a través de la funcionalidad de alerta de contagios que permite identificar situaciones de riesgo por haber estado en contacto estrecho con personas usuarias de la aplicación que se encuentran infectadas por la COVID-19. De esta manera se te informará de las medidas que conviene adoptar después.

6. ¿Durante cuánto tiempo conservamos tus datos?

Las claves de exposición temporal y los identificadores efímeros de Bluetooth son almacenados en el dispositivo por un periodo de 14 días, después de los cuales son eliminados.

Asimismo, las claves de exposición temporal que hayan sido comunicadas al servidor por los USUARIOS diagnosticados como positivos por COVID-19 también serán eliminadas del servidor al cabo de 14 días.

En todo caso, ni las claves de exposición temporal ni los identificadores efímeros de Bluetooth contienen datos de carácter personal ni permiten identificador los teléfonos móviles de los usuarios.

7. ¿Quién tiene acceso a tus datos?

Ni la aplicación "Radar COVID" ni el servidor de alerta de contagios almacenan datos personales de ningún tipo.

Los datos gestionados por la aplicación móvil (claves diarias de exposición temporal e identificadores efímeros Bluetooth) se almacenan únicamente en el dispositivo del usuario a los efectos de poder hacer cálculos y derivar informes al USUARIO sobre su riesgo de exposición a la COVID-19.

Solo en el caso de reportar un diagnóstico positivo por COVID-19, las claves de exposición temporal de los últimos 14 días generadas en el dispositivo, y bajo el consentimiento explícito e inequívoco del USUARIO, son subidas al servidor para su difusión al conjunto de USUARIOS de este sistema.

Estas claves no guardan relación alguna con la identidad de los dispositivos móviles ni con datos personales de los USUARIOS de la Aplicación.

8. ¿Cuáles son tus derechos y cómo puedes controlar tus datos?

Dado que la aplicación Radar COVID no almacena datos personales, no son de aplicación los derechos de acceso, rectificación, supresión, limitación, oposición y portabilidad, así como a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos.

En todo caso, tenemos obligación de indicarte que te asiste en todo momento el derecho para presentar una reclamación ante Agencia Española de Protección de Datos (www.aepd.es).

9. ¿Cómo protegemos tus datos?

El sistema Radar COVID no almacena datos personales.

En todo caso, las medidas de seguridad implantadas se corresponden con las previstas en el anexo II (Medidas de seguridad) del 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.

Finalmente, te informamos que tanto el almacenamiento como el resto de las actividades del tratamiento de datos no personales utilizados estarán siempre ubicados dentro de la Unión Europea.

10. ¿Cuál es la legitimación para el tratamiento de tus datos?

Los datos generados se tratarán legítimamente con las siguientes bases legales:

El consentimiento del usuario libre, específico, informado e inequívoco del USUARIO, poniendo a su disposición la presente política de privacidad, que deberá aceptar mediante el marcado de la casilla dispuesta al efecto.

Razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud (artículo 9.2 i) del RGPD), para el tratamiento de los datos de salud (por ejemplo, el estado de una persona contagiada o información sobre síntomas, etc.).

Cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1 e) RGPD).

Fines de archivo de interés público, fines de investigación científica o histórica o fines estadísticos (artículo 9.2 j) RGPD).

El Titular de la Aplicación podrá dar acceso o transmitir los datos a terceros proveedores de servicios, con los que haya suscrito acuerdos de encargo de tratamiento de datos, y que únicamente accedan a dicha información para prestar un servicio en favor y por cuenta del Responsable.

11. ¿Qué tienes que tener especialmente en cuenta al utilizar "Radar COVID"?

Has de tener en cuenta determinados aspectos relativos a la edad mínima de utilización de Aplicación, la calidad de los datos que nos proporcionas, así como la desinstalación de la Aplicación en tu dispositivo móvil.

Edad mínima de utilización: para poder utilizar "Radar COVID" tienes que ser mayor de 18 años o contar con la autorización de tus padres y/o tutores legales. Por tanto, al darte de alta en la Aplicación, garantizas al Titular que eres mayor de dicha edad o, en caso contrario, que cuentas con la mencionada autorización.

Calidad de los datos que nos proporcionas: la información que nos facilites en el uso de los servicios de la Aplicación deberá de ser siempre real, veraz y estar actualizada.

Desinstalación de la Aplicación: en general, puede haber dos situaciones en las que se proceda a la desactivación técnica de la Aplicación en tu dispositivo: 1) que lo realices voluntariamente, y 2) que desde el Titular se proceda a la desactivación técnica de la Aplicación en tu dispositivo (p.ej. en casos en los que detectemos que has incumplido las condiciones de uso de la Aplicación).

12. Política de cookies

Utilizamos solamente cookies técnicas que permiten al usuario la navegación y la utilización de las diferentes opciones o servicios que se ofrecen en la Aplicación como, por ejemplo, acceder a partes de acceso restringido o utilizar elementos de seguridad durante la navegación.

He leído el documento POLÍTICA DE PRIVACIDAD DE LA APLICACIÓN "Radar COVID".

VIGÉSIMO SEXTO*:* En la versión inicial de las "Condiciones de Uso de Radar COVID" consta la siguiente información:

CONDICIONES DE USO DE Radar COVID

AL DESCARGAR Y USAR LA APLICACIÓN MÓVIL "Radar COVID" MANIFIESTAS QUE HAS LEÍDO Y ACEPTAS ESTAS CONDICIONES DE USO Y LA POLÍTICA DE PRIVACIDAD. AQUÍ SE RECOGE TODA LA INFORMACIÓN RELATIVA A TUS DERECHOS Y OBLIGACIONES COMO USUARIO DE ESTA APLICACIÓN.

AVISO IMPORTANTE:

• El USUARIO queda avisado de que la utilización de la Aplicación NO CONSTITUYE EN NINGÚN CASO UN SERVICIO DE DIAGNÓSTICO MÉDICO, DE ATENCIÓN DE URGENCIAS O DE PRESCRIPCIÓN DE TRATAMIENTOS FARMACOLÓGICOS, pues la utilización de la Aplicación no podría en ningún caso sustituir la consulta presencial personal frente a un profesional médico debidamente cualificado.

1. Qué es Radar COVID

Radar COVID es una aplicación que promueve la salud pública mediante un sistema de alerta de contagios por la COVID-19, poniendo a disposición de los

USUARIOS (en adelante, individualmente, el "USUARIO", y conjuntamente los "USUARIOS"), la posibilidad de navegar por la Aplicación, accediendo a los contenidos y servicios de Radar COVID, de acuerdo con las presentes CONDICIONES DE USO.

Radar COVID detecta la intensidad de señales Bluetooth intercambiadas entre dispositivos que tienen esta aplicación activa, mediante el empleo de identificadores aleatorios efímeros, que no guardan relación con la identidad del teléfono móvil empleado o el USUARIO. El dispositivo de cada USUARIO descarga periódicamente las claves Bluetooth de todos los USUARIOS de la aplicación que hayan informado a través de la misma que se les ha diagnosticado COVID-19 (previa acreditación de las autoridades sanitarias), procediendo a determinar si el USUARIO ha establecido contacto de riesgo con alguno de ellos, verificado por las señales Bluetooth intercambiadas. Si es el caso, la aplicación le notifica este hecho, a fin de que pueda para tomar medidas, y contribuir de este modo a evitar que el virus se propague.

2. Uso de Radar COVID

Para la utilización de los servicios de Radar COVID, es requisito necesario que el USUARIO autorice la activación del sistema de comunicaciones Bluetooth de baja energía por parte de la Aplicación, tras la descarga de la misma.

El USUARIO acepta sin reserva el contenido de las presentes CONDICIONES DE USO. En consecuencia, el USUARIO deberá leer detenidamente las mismas antes del acceso y de la utilización de cualquier servicio de Radar COVID bajo su entera responsabilidad.

AVISO IMPORTANTE: La utilización de la Aplicación es gratuita, libre y voluntaria para todos los ciudadanos. Para utilizar Radar COVID no es necesario estar registrado, ni aportar ningún dato personal, identificativo o no identificativo. Al activar la aplicación, el USUARIO acepta:

a) envío de señales Bluetooth emitidas de forma anónima por su dispositivo;

b) la recepción y almacenamiento de señales Bluetooth de aplicaciones compatibles con Radar COVID, que se mantienen de forma anónima y descentralizada en los dispositivos de los USUARIOS durante un periodo no superior a 14 días;

y c) la información ofrecida al USUARIO sobre el posible riesgo de contagio, sin que en ningún momento se refieran datos personales de ningún tipo.

El USUARIO puede informar voluntariamente a la aplicación de un resultado positivo en sus pruebas de COVID-19 mediante el código de confirmación de un solo uso facilitado por las autoridades sanitarias. La validez de este código será cotejada por las autoridades sanitarias para asegurar el correcto funcionamiento de Radar COVID. El USUARIO informará de los resultados de sus pruebas y se le solicitará el consentimiento expreso e inequívoco para compartir las claves generadas diariamente en su dispositivo, y correspondientes a los últimos 14 días. Estas claves son comunicadas a un servidor que las pondrá a

disposición del conjunto de aplicaciones Radar COVID para su descarga. Las claves comunicadas no guardan relación alguna con la identificación del dispositivo o el USUARIO.

No se producirá ninguna discriminación a los potenciales pacientes que requieran servicios sanitarios y no hayan utilizado la aplicación.

3. Seguridad y privacidad

Las medidas de seguridad implantadas se corresponden con las previstas en el anexo II (Medidas de seguridad) del 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.

Te informamos que tus datos serán tratados conforme a lo establecido en la Política de Privacidad de la Aplicación, cuyo contenido íntegro se puede consultar en el siguiente enlace: Política de Privacidad.

Toda la información se tratará con fines estrictamente de interés público en el ámbito de la salud pública, y ante la situación de emergencia sanitaria decretada, a fin de proteger y salvaguardar un interés esencial para la vida de las personas, en los términos descritos en la política de privacidad.

La información de la actividad de los USUARIOS es anónima y en ningún momento se exigirá a los USUARIOS ningún dato personal. En todo momento, el USUARIO puede desactivar el sistema de traza de contactos Bluetooth en la aplicación, así como desinstalar la misma.

4. Cambio del servicio y terminación

Radar COVID siempre está tratando de mejorar el servicio y busca ofrecer funcionalidades adicionales útiles para el USUARIO teniendo siempre presente la preservación de la salud pública. Esto significa que podemos añadir nuevas funciones o mejoras que en ningún caso implicarán el tratamiento de datos personales, así como eliminar algunas de las funciones. Si estas acciones afectan materialmente a los derechos y obligaciones del USUARIO, será informado a través de la Aplicación.

El USUARIO puede dejar de utilizar la aplicación en cualquier momento y por cualquier motivo, desinstalándola de su dispositivo.

5. Titular de la aplicación

La Secretaría General de Administración Digital (SGAD), dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, es la TITULAR de la aplicación Radar COVID.

Radar COVID en su arquitectura emplea el nuevo marco proporcionado por Apple y Google desarrollado a partir del Protocolo de DP-3T de rastreo de proximidad descentralizado para preservar la privacidad.

6. Responsabilidad y obligaciones

Radar COVID se ofrece dedicando los mejores esfuerzos, dado que su calidad y disponibilidad pueden verse afectadas por múltiples factores ajenos al TITULAR como son, entre otros, el volumen de USUARIOS en la ubicación geográfica del USUARIO, limitaciones o restricciones de las redes de terceros operadores o la compatibilidad del dispositivo y sistema operativo utilizado por el USUARIO. Igualmente, los USUARIOS aceptan que el servicio pueda verse interrumpido cuando sea necesario por labores de mantenimiento.

Por todo ello, el TITULAR no será responsable de los problemas de acceso o disponibilidad de Radar COVID y/o sus servicios, ni de los perjuicios que se pudieran causar por ello, cuando éstos procedan de factores ajenos a su ámbito de control. Igualmente, el TITULAR no se hace responsable de los siguientes hechos, ni de fallos, incompatibilidades y/o daños de tus terminales o dispositivos que, en su caso, se pudiesen derivar de la descarga y/o uso de la Aplicación:

- *Actualización, exactitud, exhaustividad, pertinencia, actualidad y fiabilidad de sus contenidos, cualquiera que sea la causa y las dificultades o problemas técnicos o de otra naturaleza en los que tengan su origen dichos hechos.*

- *La calidad, titularidad, legitimidad, adecuación o pertinencia de los materiales, y demás contenidos.*

Como USUARIO de la Aplicación te obligas a:

- *Impedir el acceso de terceras personas no autorizadas a la aplicación desde tu dispositivo.*

- *Notificar al TITULAR con carácter inmediato cualquier indicio de la existencia de una violación en la seguridad en la Aplicación, de usos inapropiados o prohibidos de los servicios prestados desde la misma, o de fallos de seguridad de cualquier índole.*

- *Hacer buen uso de los contenidos, información y servicios prestados desde o a través de la Aplicación, conforme a la ley, la buena fe y a las buenas costumbres generalmente aceptadas, comprometiéndose expresamente a:*

  - *Abstenerse de realizar prácticas o usos de los servicios con fines ilícitos, fraudulentos, lesivos de derechos o intereses del TITULAR o de terceros, infractores de las normas contenidas en el presente documento.*

  - *Abstenerse de realizar cualquier tipo de acción que pudiera inutilizar, sobrecargar o dañar sistemas, equipos o servicios de la Aplicación o accesibles directa o indirectamente a través de esta.*

  - *Respetar los derechos de propiedad intelectual e industrial del TITULAR y de terceros sobre los contenidos, información y servicios prestados desde o a través de la Aplicación, absteniéndose con carácter general de copiar, distribuir, reproducir o comunicar en forma alguna los mismos a terceros, de no me-*

diar autorización expresa y por escrito del TITULAR o de los titulares de dichos derechos.

o No proporcionar información falsa en la Aplicación, siendo el único responsable de la comunicación real y veraz.

o No suplantar la personalidad de un tercero.

El USUARIO de la Aplicación es el único responsable del uso que decida realizar de los servicios de Radar COVID. El incumplimiento de las obligaciones como USUARIO podrá implicar la baja inmediata de la Aplicación y/o sus servicios; todo ello sin derecho a recibir compensación de ningún tipo, y sin perjuicio de las correspondientes acciones legales a que por parte del TITULAR hubiere lugar.

El TITULAR no será responsable en ningún caso de la utilización indebida de Radar COVID y de sus contenidos, siendo el USUARIO el único responsable por los daños y perjuicios que pudieran derivarse de un mal uso de estos o de la infracción de lo dispuesto en las presentes condiciones en que pueda incurrir. El USUARIO se compromete a mantener indemne al TITULAR frente a las reclamaciones o sanciones que pudiera recibir de terceros, ya sean particulares o entidades públicas o privadas, por razón de dichas infracciones, así como frente a los daños y perjuicios de todo tipo que pueda sufrir como consecuencia de las mismas.

En cualquier caso, el TITULAR se reserva, en cualquier momento y sin necesidad de previo aviso, el derecho de modificar o eliminar el contenido, estructura, diseño, servicios y condiciones de acceso y/o uso de esta Aplicación, siempre que lo estime oportuno, siempre que dicho cambio no afecte a los principios y derechos de protección de datos, así como el derecho interpretar las presentes condiciones, en cuantas cuestiones pudiera plantear su aplicación.

Asimismo, queda prohibida la reproducción, distribución, transmisión, adaptación o modificación, por cualquier medio y en cualquier forma, de los contenidos de Radar COVID o sus cursos (textos, diseños, gráficos, informaciones, bases de datos, archivos de sonido y/o imagen, logos y demás elementos de estos sitios), salvo autorización previa de sus legítimos titulares.

La enumeración anterior tiene mero carácter enunciativo y no es, en ningún caso, exclusivo ni excluyente en ninguno de sus puntos. En todos los supuestos, El TITULAR EXCLUYE CUALQUIER RESPONSABILIDAD POR LOS DAÑOS Y PERJUICIOS DE CUALQUIER NATURALEZA DERIVADOS DIRECTA O INDIRECTAMENTE DE LOS MISMOS Y DE CUALESQUIERA OTROS NO ESPECIFICADOS DE ANÁLOGAS CARACTERISTICAS.

El TITUTAR NO OFRECE NINGUNA GARANTÍA, EXPRESA, IMPLÍCITA, LEGAL O VOLUNTARIA.

EL TITULAR EXCLUYE EXPRESAMENTE TODAS LAS GARANTÍAS IMPLÍCITAS, INCLUYENDO, A TÍTULO ENUNCIATIVO, PERO NO LIMITATIVO, CUALQUIER GARANTÍA IMPLÍCITA O SANEAMIENTO DE VICIOS OCUL-

TOS, COMERCIABILIDAD, CALIDAD SATISFACTORIA, TÍTULO, IDONEIDAD DEL PRODUCTO PARA UN PROPÓSITO EN PARTICULAR Y CUALQUIER GARANTÍA O CONDICIÓN DE NO INFRACCIÓN. ESTA EXCLUSIÓN DE RESPONSABILIDAD SÓLO SE APLICARÁ EN LA MEDIDA PERMITIDA POR LA LEY IMPERATIVA APLICABLE.

7. Enlaces

Radar COVID puede incluir dentro de sus contenidos enlaces con sitios pertenecientes y/o gestionados por terceros con el objeto de facilitar el acceso a información y servicios disponibles a través de Internet.

El TITULAR no asume ninguna responsabilidad derivada de la existencia de enlaces entre los contenidos de Radar COVID y contenidos situados fuera de los mismos o de cualquier otra mención de contenidos externos a este sitio, exceptuando aquellas responsabilidades establecidas en la normativa de protección de datos. Tales enlaces o menciones tienen una finalidad exclusivamente informativa y, en ningún caso, implican el apoyo, aprobación, comercialización o relación alguna entre el TITULAR y las personas o entidades autoras y/o gestoras de tales contenidos o titulares de los sitios donde se encuentren, ni garantía alguna del TITULAR por el correcto funcionamiento de los sitios o contenidos enlazados.

En este sentido el USUARIO se obliga a poner la máxima diligencia y prudencia en el caso de acceder o usar contenidos o servicios de los sitios a los que acceda en virtud de los mencionados enlaces.

8. Hiperenlaces

No se admite la reproducción de páginas de Radar COVID mediante hiperenlace desde otra Aplicación móvil o página web, permitiéndose exclusivamente el acceso desde la Aplicación.

En ningún caso se podrá dar a entender que el TITULAR autoriza el hiperenlace o que ha supervisado o asumido de cualquier forma los servicios o contenidos ofrecidos por la web desde la que se produce el hiperenlace.

No se podrán realizar manifestaciones o referencias falsas, incorrectas o inexactas sobre las páginas y servicios del TITULAR.

Se prohíbe explícitamente la creación de cualquier tipo de navegador, programa, "browser" o "border environment" sobre las páginas de Radar COVID.

No se podrán incluir contenidos contrarios a los derechos de terceros, ni contrarios a la moral y las buenas costumbres aceptadas, ni contenidos o informaciones ilícitas, en la página web desde la que se establezca el hiperenlace.

La existencia de un hiperenlace entre una página web y el Radar COVID no implica la existencia de relaciones entre el TITULAR y el propietario de esa página, ni la aceptación y aprobación de sus contenidos y servicios.

9. Ley aplicable y fuero

Las presentes condiciones de uso se regirán e interpretarán en todos y cada uno de sus extremos por la Ley Española. En aquellos casos en los que la normativa vigente no prevea la obligación de someterse a un fuero o legislación determinado, el TITULAR y los USUARIOS, con renuncia a cualquier otro fuero que pudiera corresponderles, se someten a los juzgados y tribunales de Madrid capital (España).

10. Información corporativa y contacto

Dirección: Calle de Manuel Cortina, 2, 28010 Madrid

El soporte al USUARIO en caso de incidencias y/o reclamaciones será principalmente online y atendido a la mayor brevedad: soporte.radarcovid@covid19.gob.es

VIGÉSIMO SÉPTIMO: El 12 de agosto de 2020 se elabora por la SEDIA, y según afirma la propia SEDIA, el primer documento de EIPD respecto del proyecto piloto Radar Covid, *"cuando se tomó la decisión de que se adaptase el proyecto piloto para su despliegue a nivel nacional*".

En dicho documento se afirma la existencia de tratamientos de datos de carácter personal:

"*Por tanto, en los casos en que, a primera vista, la información no permite singularizar a una persona determinada, esta aún puede ser identificable, porque esa información puede ser combinada con otros datos, tanto si el responsable de su tratamiento tiene conocimiento de ellos como si no, que permitan distinguir a esa persona de otras.*

A pesar de que tradicionalmente los datos pseudonimizados eran considerados datos anónimos, en la actualidad la pseudonimización ya no se considera un método de anonimización, pues la persona es todavía identificable, aunque sea de forma indirecta. Así, actualmente se considera que los datos pseudonimizados son todavía datos de carácter personal y están sujetos a la normativa sobre protección de datos de carácter personal.

En conclusión, en este tratamiento, a pesar de que los usuarios no puedan ser identificados directamente, podrían llegar a ser identificables, realizándose mapas de relaciones entre personas, mediante reidentificación por localización implícita llegando, incluso, a poder identificar la identidad de los contagiados. Debe tenerse en cuenta, en este sentido, que el tratamiento de la información no solo afecta al usuario de la aplicación sino también a la de todos los terceros con los que ha estado en contacto.

Una vez dicho lo anterior, partiendo por tanto de que a la actividad de tratamiento en cuestión le aplica la normativa vigente sobre privacidad y protección de datos, y teniendo en cuenta la categoría de datos que podrían llegar a identificar a los usuarios, se procede a analizar la necesidad de realizar una EIPD".

En cuanto a los roles de "Responsables, corresponsables y encargados del tratamiento" dispone:

"Por ello, y en virtud de lo dispuesto en el artículo 27.3, los responsables del tratamiento serán las comunidades autónomas, las ciudades de Ceuta y Melilla y el Ministerio de Sanidad, 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.

En este caso el titular de la aplicación es la Secretaría General de Administración Digital dependiente del Ministerio de Asuntos Económicos y Transformación Digital, que también se constituye como Responsable del Tratamiento.

La aplicación ha sido desarrollada a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA)".

Respecto de los datos personales tratados confirma los siguientes:

"De esta forma, los datos generados o a los que accede la aplicación, son los siguientes:

· La aplicación genera datos de proximidad (claves de exposición temporal con las que el dispositivo del usuario ha generado los códigos aleatorios o Identificador de proximidad rodante - RPI), que son datos generados mediante el intercambio de señales de Bluetooth de baja energía (BLE) entre dispositivos dentro de una distancia relevante desde el punto de vista epidemiológico y durante un tiempo relevante también desde el punto de vista epidemiológico. Estos datos se comunicarán a las autoridades sanitarias únicamente cuando se haya confirmado que un usuario en cuestión está infectado de COVID-19 y a condición de que la persona opte por que así se haga, es decir, de manera voluntaria.

· Dato mediante el que el usuario es advertido previamente de un contacto de riesgo. Estos datos permiten estimar cuántos usuarios son advertidos por la aplicación de un riesgo potencial de contagio, sin poder rastrear su identidad, y le permite al Servicio Nacional de Salud preparar las iniciativas y los recursos necesarios para atender a los usuarios que han recibido la notificación.

· El día en que el usuario desarrolló síntomas compatibles con COVID-19.

· Código (QR) proporcionado por las autoridades sanitarias para permitir al usuario activar una alerta de advertencia. Este número de 12 cifras será proporcionado por las autoridades sanitarias, que lo enviarán después de dar positivo. Este número no deja de ser la "confirmación" que efectivamente el usuario ha dado positivo y no se trata de un usuario aleatorio intentando enviar alertas falsas.

· La dirección IP que utiliza el dispositivo para conectarse a Internet. En este sentido cabe traer a colación la Sentencia del Tribunal Supremo de 3 de octubre de 2014, en cuyo Fundamento de Derecho número cuatro establece que «no cabe duda que, a partir de la dirección IP puede identificarse directa o indirectamente la identidad del interesado, ya que los proveedores de acceso a internet tienen constancia de los nombres, teléfono y otros datos identificativos de los usuarios a los que han asignado las particulares direcciones IP». La Sentencia confirma que las direcciones IP son datos personales ya que contie-

nen información concerniente a personas identificadas o identificables.

(…)

Por tanto, como consecuencia de lo anterior, cualquier sistema de seguimiento de proximidad que verifique una base de datos pública de claves de diagnóstico contra identificadores cambiantes de proximidad (rolling proximity identifiers-RPID) en el dispositivo de un usuario deja abierta la posibilidad de que los contactos de una persona infectada descubran cuál de las personas que encontraron es infectado. Además, el hecho de que los usuarios infectados compartan públicamente sus claves de diagnóstico una vez al día, en lugar de sus RPID cada pocos minutos, expone a esas personas a ataques de enlace.

Por ello, hay que prestar especial atención a esta probabilidad ya que en el caso de que un usuario de la aplicación pudiera ser identificado, la privacidad quedaría enormemente amenazada, pudiendo resultar afectados todo tipo de datos personales como:

· Datos de salud,

· Localización,

· Contactos,

· Correo electrónico,

· Registro de llamadas,

· SMS y mensajería instantánea,

· Identidad del interesado,

· Identidad del teléfono (es decir, nombre del teléfono)

· Historial de navegación,

· Credenciales de autenticación para los servicios de la sociedad de la información (en particular los servicios con características sociales)

· Fotografías y vídeos

· Datos biométricos (por ejemplo, modelos de reconocimiento facial y huellas dactilares)".

Respecto de la finalidad del tratamiento, lo determinan, ligándolo a las funcionalidades de la aplicación:

"Cada una de las distintas funcionalidades de la aplicación obedece a determinados fines:

· La finalidad principal de la App es informar a las personas que hayan estado muy cerca de alguien que resulte ser un portador confirmado del virus, a fin de romper las cadenas de transmisión lo antes posible. De esta manera, la aplicación permite identificar a las personas que han estado en contacto con alguien infectado por la COVID-19 e informarles de las medidas que conviene adoptar después, como someterse a autocuarentena o a las pruebas correspondientes.

· Para ello la App mantiene los contactos de las personas que utilizan la aplicación y que pueden haber estado expuestas a la infección de la COVID-19.

· Cuando una persona da positivo en el test de COVID-19 y decida compartir li-

bremente este dato, la App alerta a aquellas otras personas que podrían haber sido infectadas y con las que se haya tenido contacto los últimos 14 días. Para ello, esta persona deberá compartir un número de 12 cifras que será proporcionado por las autoridades sanitarias. El móvil realiza una comprobación de si los ID aleatorios coinciden con alguno que haya sido marcado como positivo.

· Se determina el día en que el usuario desarrolló síntomas compatibles con COVID-19 y fecha de contacto con personas infectadas".

Del estudio del ciclo de vida de los datos se indica que la captura de los datos se produce con el *"Acceso a información almacenada en el dispositivo móvil en el momento de la instalación de la App*".

VIGÉSIMO OCTAVO: Con fecha 19 de agosto de 2020 el Consejo Interterritorial del Sistema Nacional de Salud, firma un "Acuerdo de uso de la aplicación "Radar COVID", en fase de pruebas, por parte de las Comunidades Autónomas y Ciudades Autónomas" que dice:

Para contribuir a estas tareas de búsqueda activa de contactos estrechos de casos confirmados, desde la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA), se ha desarrollado, en coordinación con otros miembros de la UE y la red de eHealth, una herramienta digital para complementar las tareas de búsqueda manual de contactos que llevan a cabo los correspondientes servicios de las comunidades y ciudades autónomas. (…)
Durante el mes de julio de 2020, la Secretaría General de Administración Digital, órgano directivo dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial, llevó a cabo con éxito un proyecto piloto para comprobar el funcionamiento de esta aplicación en la isla de la Gomera. (…)
El presente Acuerdo temporal permite establecer los términos de uso por parte de las comunidades y ciudades autónomas de la aplicación "RADAR COVID" durante dicha fase de pruebas, hasta la fecha de total operatividad de la misma, que se producirá mediante la adhesión a la aplicación a través de los oportunos convenios bilaterales de la Secretaría de Estado de Digitalización e Inteligencia Artificial con las diferentes comunidades y ciudades autónomas.

En el punto 5 se dice:

5. En relación con el tratamiento de datos de carácter personal, y en aplicación del régimen previsto 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, durante la vigencia de este Acuerdo, el responsable del tratamiento será el Ministerio de Sanidad y, en su respectivo territorio, cada una de las comunidades y ciudades autónomas que se vayan incorporando durante la fase de pruebas al uso de la aplicación, ostentando plenamente sus competencias en materia sanitaria. El encargado del tratamiento será, en ambos casos, la Secretaría de Estado de Digitalización e Inteligencia Artificial.

VIGÉSIMO NOVENO: Consta el Documento técnico "Procedimiento de implementación de la App Radar COVID como complemento a los sistemas manuales de identificación de contactos" en su versión de 14 de agosto de 2020, coordinado por:

- Centro de Coordinación de Alertas y Emergencias Sanitarias.
- Dirección General de Salud Pública, Calidad e Innovación.

TRIGÉSIMO: A nivel nacional, la puesta en servicio de la App Radar COVID se produce en fecha 19 de agosto de 2020.

TRIGÉSIMO PRIMERO: Con fecha 26 de agosto de 2020 se celebra la reunión para determinar la situación del proyecto y los próximos pasos. Los asistentes son:

Persona	SEDIA / CCAA / Mº Sanidad / Minsait
D.D.D.	SEDIA
F.F.F.	SEDIA
Z.Z.Z.	SEDIA
V.V.V.	SEDIA
M.M.M.	Minsait
P.P.P.	Minsait
Q.Q.Q.	Minsait

TRIGÉSIMO SEGUNDO: Consta una primera versión del documento "Análisis de Riesgos Servicio Radar Covid19" fechado en agosto de 2020, elaborado por MINTSAIT an INDRA COMPANY.

TRIGÉSIMO TERCERO: Consta una segunda versión del documento "Análisis de Riesgos Servicio Radar Covid19" fechado en septiembre de 2020, elaborado por MINTSAIT an INDRA COMPANY.

El principal objetivo del Análisis de Riesgos es determinar el nivel de riesgo al que están expuestos los activos del Servicio Radar Covid19, teniendo en cuenta las amenazas a las que están expuestos y el nivel de eficacia de los controles implantados actualmente para protegerlos. El Análisis de Riesgos está basado en la información aportada por los responsables técnicos de INDRA y los responsables del desarrollo, puesta en marcha e implantación de la Aplicación Radar Covid19, quienes conocen la infraestructura y que, por tanto, pueden conocer el grado de implantación de cada una de las medidas de seguridad del Anexo II del Esquema Nacional de Seguridad. Por otra parte, el presente documento se ha elaborado con la información recabada hasta su fecha de edición, por lo que, salvo indicación expresa, los cambios realizados después de esta fecha no se verán reflejados en el mismo. Como se ha comentado anteriormente, el nivel del riesgo se puede clasificar en una escala de 0 a 10, siendo el valor 0 el riesgo despreciable y el valor 10 el riesgo extremadamente crítico. Teniendo en cuenta dicha escala, y tomando como métrica para el nivel de riesgo el mayor valor de riesgo identificado en un activo, el resultado del Análisis de Riesgos determina un Nivel de Riesgo Actual = {2,6}. Atendiendo a los niveles mínimos de madurez requeridos por el Esquema Nacional de Seguridad y tomando para el riesgo objetivo la misma métrica que se ha tomado para el riesgo residual, es decir, el mayor valor de riesgo identificado en un activo, el objetivo que se propone alcanzar en el proceso de mitigación de riesgos quedaría establecido en un Nivel de Riesgo Objetivo = {1,8}.

Se recomienda abordar un conjunto de acciones para mejorar las medidas de se-

guridad existentes actualmente, con el objeto de ajustar el nivel de riesgo del Servicio Radar Covid19 a un nivel BAJO. Estas acciones se han focalizado en las medidas de seguridad que pueden minimizar las amenazas que aportan un nivel de riesgo MEDIO en el presente Análisis de Riesgos. Estas acciones permitirán alcanzar el nivel de Riesgo Objetivo propuesto, ya que aumentarían el grado de madurez de las medidas de seguridad Mp.info.4 Firma electrónica y Op.acc.5 Mecanismos de autenticación.

Las acciones propuestas en este caso son:

- *Utilizar certificados cualificados para la firma digital que se utiliza en el servicio de verificación de los positivos.*

- *Verificar que los elementos criptográficos hardware del AWS Multi-Factor Authentication (MFA) utilizan algoritmos y parámetros acreditados por el CCN. Además se recomienda revisar el mecanismo de control de acceso a la Base de Datos PostgreSQL para concluir que cumple con los requisitos de nivel alto.*

TRIGÉSIMO CUARTO Con fecha 9 de septiembre de 2020 el METD publica esta nota de prensa:

"La aplicación móvil RadarCOVID completa su implantación en trece comunidades autónomas, que abarcan el 70% de la población, y libera su código. (…)

A falta de esa necesaria integración, la aplicación está activa y funcionando en todo el territorio nacional desde el pasado mes de agosto. Eso implica que el terminal ya almacena los identificadores anónimos de los otros terminales con los que se ha estado en contacto de riesgo durante los últimos siete días.

Por eso, y aunque la implementación técnica esté en proceso en algunas comunidades autónomas, es útil tener ya instalada la aplicación para que ese proceso de registro vaya teniendo lugar y poder estar así protegidos desde el primer momento en el que se pone en marcha. Más de 3,7 millones de usuarios han descargado ya la aplicación, protegiéndose y protegiendo a sus personas cercanas contra posibles cadenas de contagio.

Liberación del código

Además, se ha dado cumplimiento a uno de los compromisos adquiridos con el inicio del desarrollo de la aplicación: la liberación de su código.

Se trata de un ejercicio de transparencia para que el funcionamiento de la aplicación pueda ser auditado de forma abierta y directa por parte de la ciudadanía. *(…)*

Con la intención de dar a conocer el funcionamiento de la aplicación y resolver las dudas y cuestiones que la ciudadanía comparte a través de las redes sociales, la Secretaría de Estado de Digitalización e IA ha puesto en marcha dos cuentas específicas para la aplicación. Así, desde la cuenta @AppRadarCOVID, disponible tanto en Twitter como en Instagram, se irá compartiendo información puntual sobre las novedades respecto a la app y se dará respuesta a las preguntas más fre-

cuentes que haga llegar la ciudadanía."

TRIGÉSIMO QUINTO: Consta el Documento técnico "Procedimiento de implementación de la App Radar COVID como complemento a los sistemas manuales de identificación de contactos" en su versión de 15 de septiembre de 2020, coordinado por:

- Centro de Coordinación de Alertas y Emergencias Sanitarias.
- Dirección General de Salud Pública, Calidad e Innovación.

TRIGÉSIMO SEXTO: Constan dos versiones más de la Evaluación de impacto:

En la segunda versión, fechada en septiembre de 2020, se dice:

"Por ello, y en virtud de lo dispuesto en el artículo 27.3, los responsables del tratamiento serán las comunidades autónomas, las ciudades de Ceuta y Melilla y el Ministerio de Sanidad, 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 COVID Radar 10 categorías especiales de datos y que dichos tratamientos serán realizados por administraciones públicas obligadas al cumplimiento del Esquema Nacional de Seguridad.

En este caso el titular de la aplicación es la Secretaría General de Administración Digital dependiente del Ministerio de Asuntos Económicos y Transformación Digital, que también se constituye como Responsable del Tratamiento".

En la tercera versión, se dice:

"Por ello, y en virtud de lo dispuesto en el artículo 27.3, los responsables del tratamiento serán las comunidades autónomas, las ciudades de Ceuta y Melilla y el Ministerio de Sanidad, 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 Radar COVID 10 categorías especiales de datos y que dichos tratamientos serán realizados por administraciones públicas obligadas al cumplimiento del Esquema Nacional de Seguridad.

El responsable de tratamiento es la Dirección General de Salud Pública, dependiente del Ministerio de Sanidad.

El encargado de tratamiento es la Secretaría General de Administración Digital, dependiente del Ministerio de Asuntos Económicos y Transformación Digital, que ha desarrollado la Aplicación."

Asimismo, en la primera versión de la Evaluación de impacto se indica respecto de su finalidad que *"El presente documento tiene como objetivo exponer los resultados del Análisis de Riesgos realizado al Servicio Radar Covid19 respecto al Esquema Nacional de Seguridad"*.

Aseveran que "*La aplicación no solicita ningún dato de carácter personal, ni requiere crear usuario (sin login ni datos personales). La aplicación utiliza claves anónimas e intercambia identificadores aleatorios, que están en constante cambio. El personal implicado en la aplicación conoce la tipología de la información y, lo más importante, la Política de Seguridad*".

Conforme a lo anterior y al contenido de esta, la evaluación de impacto se limita a examinar el cumplimiento del ENS, sin entrar en un posible análisis de riesgos o evaluación de impacto de protección de datos.

TRIGÉSIMO SÉPTIMO: En la versión definitiva de la "Política de Privacidad de la Aplicación Radar COVID" publicada en octubre de 2020, consta la siguiente información:

> *POLÍTICA DE PRIVACIDAD DE LA APLICACIÓN Radar COVID*
>
> *Por favor, lee detenidamente esta política de privacidad para usuarios de la aplicación móvil "Radar COVID" (o la "Aplicación"), donde podrás encontrar toda la información sobre los datos que utilizamos, cómo lo usamos y qué control tienes sobre los mismos.*
>
> *AVISO IMPORTANTE:*
>
> *El USUARIO queda avisado de que la utilización de la Aplicación NO CONSTITUYE EN NINGÚN CASO UN SERVICIO DE DIAGNÓSTICO MÉDICO, DE ATENCIÓN DE URGENCIAS O DE PRESCRIPCIÓN DE TRATAMIENTOS FARMACOLÓGICOS, pues la utilización de la Aplicación no podría en ningún caso sustituir la consulta presencial personal frente a un profesional médico debidamente cualificado.*
>
> *1. ¿Qué es Radar COVID?*
>
> *Radar COVID es una aplicación para dispositivos móviles de alerta de contagios del virus SARS-CoV-2, cuyo TITULAR es la Secretaría General de Administración Digital, dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital.*
>
> *Gracias a Radar COVID, aquellos usuarios que se hayan descargado la aplicación y acepten su uso recibirán una notificación en caso de que en los catorce días anteriores a esa notificación hayan estado expuestos a un contacto epidemiológico (a menos de dos metros y más de 15 minutos) con otro usuario (totalmente anónimo) que haya declarado en la aplicación haber dado un resultado positivo en la prueba de COVID 19 (previa acreditación de las autoridades sanitarias). La aplicación le informará exclusivamente sobre el día (dentro de esos catorce anteriores) en que se haya producido la exposición al contacto pero no sobre la identidad del usuario al que haya quedado expuesto (información imposible al ser una aplicación que no solicita, utiliza ni almacena datos de carácter personal de los usuarios) ni la identificación del dispositivo de este, ni sobre el momento o lugar en que la exposición se haya producido.*
>
> *Recibida una notificación, la aplicación facilitará al usuario expuesto información para la adopción de medidas preventivas y asistenciales, para contribuir con ello a contener la propagación del virus.*

El éxito de la aplicación como herramienta que contribuya a la contención de la propagación está directamente vinculado a que los usuarios sean conscientes, y actúen en consecuencia, de que, a pesar de que comunicar a la aplicación que se ha obtenido un resultado positivo en la prueba de COVID 19 (previa acreditación de las autoridades sanitarias) es voluntario, el no comunicarlo y ser un mero receptor de información de terceros usuarios hace que la aplicación pierda su utilidad preventiva no solo para los demás usuarios sino para el resto de la población en general. El carácter completamente anónimo debería animar, sin duda, al ejercicio de esta actuación responsable.

2. ¿Cómo funciona la aplicación?

Una vez que te hayas descargado la aplicación, aceptes las condiciones de uso y la política de privacidad y comiences a utilizarla, tu dispositivo móvil generará cada día un identificador aleatorio llamado "clave de exposición temporal" con un tamaño de 16 caracteres (16 bytes o 128 bits) que servirá para derivar los "identificadores efímeros Bluetooth" que son intercambiados con otros teléfonos móviles próximos que también tengan descargada la aplicación Radar COVID y activado su Bluetooth.

Los "identificadores efímeros Bluetooth" son códigos aleatorios con un tamaño de 16 caracteres (16 bytes, o 128 bits), que se generan por tu teléfono móvil cada 10-20 minutos, a partir de la "clave de exposición temporal" diaria. Estos códigos no contienen información personal, que permita identificar al teléfono móvil o al usuario del mismo. Estos "identificadores efímeros Bluetooth" son transmitidos por tu teléfono móvil varias veces por segundo a dispositivos cercanos, accesibles a través de Bluetooth de baja energía (BLE, Bluetooth Low Energy), produciendo un intercambio de códigos aleatorios entre dispositivos para que puedan ser almacenados por teléfonos próximos que hayan descargado la aplicación. De igual manera, cada cinco minutos, tu teléfono móvil escuchará los identificadores efímeros Bluetooth que son transmitidos por otros teléfonos móviles que tengan la aplicación y los almacenará para determinar si has estado con otro usuario contagiado por COVID-19 a lo largo de los últimos 14 días que haya comunicado un positivo.

Tu teléfono almacena las claves de exposición temporal que has generado en los últimos 14 días. Recuerda que estas claves se generan aleatoriamente y no sirven para identificar a tu teléfono móvil ni al USUARIO del mismo.

Si has recibido un diagnóstico positivo por COVID-19, puedes introducir voluntariamente en la aplicación el "código de confirmación de un solo uso" que te facilitará tu Servicio Público de Salud y que será validado en el servidor de la SGAD. En ese momento, la aplicación te solicitará tu consentimiento para remitir a nuestro servidor hasta un máximo de las 14 últimas claves de exposición temporal almacenadas en tu teléfono, por tanto, solo si lo prestas, éstas se enviarán al servidor de la SGAD que, después de verificar la exactitud del código, servirán para componer un listado diario de claves de exposición temporal de personas contagiadas por COVID-19 que son descargados diariamente desde el servidor por todas las aplicaciones Radar COVID que estén en funcionamiento.

La información de estos listados sirve para que en tu propio teléfono se pueda comprobar si has tenido contacto estrecho (menos de dos metros y más de 15 minutos) con personas que han reportado un contagio por COVID-19, sin iden-

tificar ni a la persona, ni el lugar de la exposición, ni el dispositivo móvil, ni ningún dato personal tuyo o de la otra persona. Es decir, la aplicación descarga periódicamente las claves de exposición temporal compartidas voluntariamente por los usuarios diagnosticados por COVID-19 del servidor, para compararlas con los códigos aleatorios registrados en los días anteriores como resultado de contactos con otros usuarios. Si se encuentra una coincidencia, la aplicación ejecuta un algoritmo en el dispositivo que, en función de la duración y la distancia estimada del contacto, y de acuerdo con los criterios establecidos por las autoridades sanitarias, evalúa el riesgo de exposición al virus SARS-CoV-2 y en su caso muestra una notificación advirtiendo del contacto de riesgo al usuario, comunicándole la fecha del mismo e invitándolo a auto-confinarse y contactar con las autoridades sanitarias.

Estas claves remitidas al servidor no permiten la identificación directa de los usuarios y son necesarias para garantizar el correcto funcionamiento del sistema de alerta de contactos de riesgo.

3. ¿Quiénes son los responsables del tratamiento de tus datos como usuario de "Radar COVID"?

Esta aplicación tiene como responsables de tratamiento tanto al Ministerio de Sanidad, como a las Comunidades Autónomas. Así mismo, la Secretaría General de Administración Digital ejerce como encargada del tratamiento.

A nivel nacional, el responsable del tratamiento de tus datos como usuario de "Radar COVID" es:

Como parte del sistema de alerta de contagios de la COVID-19, se procesarán los siguientes datos para los usuarios que hayan dado positivo por COVID-19 para los fines especificados a continuación:

Nombre: Ministerio de Sanidad.

Dirección: Paseo del Prado 18-20, 28014 Madrid

La Secretaría General de Administración Digital, en calidad de titular de la aplicación y en base al encargo del tratamiento encomendado por el Ministerio de Sanidad, efectuará las siguientes operaciones del tratamiento:

Generación de códigos para la comunicación de positivos en la aplicación Radar COVID.

Recepción de la información remitida por los usuarios cuando comunican un positivo. Esta información incluye:

Las claves de exposición diaria hasta un máximo de 14 días. El número exacto de claves comunicadas dependerá de la fecha de inicio de síntomas o fecha de diagnóstico que se informa en la aplicación.

La preferencia o no por comunicar estas claves de exposición diaria al nodo europeo de interoperabilidad entre aplicaciones de rastreo de contactos.

Composición de un listado actualizado de claves de exposición temporal que son puestas a disposición para su descarga por parte de las aplicaciones Radar COVID.

En relación al nodo europeo de interoperabilidad de contactos (EFGS).

Recepción diaria de los listados de claves de exposición temporal generados por los servidores nacionales de los Estados Miembros adheridos en su caso al proyecto.

Remisión diaria al nodo EFGS de un listado de claves de exposición temporal remitidas por los usuarios de Radar COVID que han consentido explícitamente compartir esta información con el resto de Estados Miembros adheridos al proyecto.

Las Comunidades Autónomas adheridas al uso de la aplicación son, así mismo, responsables del tratamiento, llevando a cabo las siguientes operaciones de tratamiento:

Solicitud al servidor Radar COVID de generación de códigos de confirmación de positivo.

Entrega de estos códigos a las personas diagnosticadas positivas por pruebas PCR.

El encargado del tratamiento y titular de la aplicación es la Secretaría General de Administración Digital, órgano directivo de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, en virtud al Acuerdo entre el Ministerio de Asuntos Económicos y Transformación Digital (Secretaría de Estado de Digitalización e Inteligencia Artificial) y el Ministerio de Sanidad acerca de la aplicación "Radar COVID".

4. ¿Qué datos tratamos sobre ti?

Los datos manejados por la aplicación no permiten la identificación directa del usuario o de su dispositivo, y son solo los necesarios para el único fin de informarte de que has estado expuesto a una situación de riesgo de contagio por la COVID-19, así como para facilitar la posible adopción de medidas preventivas y asistenciales.

En ningún caso se rastrearán los movimientos de los USUARIOS, excluyendo así cualquier forma de geolocalización.

No se almacenará ni tratará la dirección IP de los USUARIOS.

No se almacenarán los códigos de confirmación de positivo junto con otros datos personales de los usuarios.

Como parte del sistema de alerta de contactos de riesgo de la COVID-19, se procesarán los siguientes datos para los usuarios que hayan dado positivo por COVID-19 para los fines especificados a continuación:

Las claves de exposición temporal con las que el dispositivo del usuario ha generado los códigos aleatorios enviados (identificadores efímeros Bluetooth), a los dispositivos con los que el usuario ha entrado en contacto, hasta un máximo de 14 días anteriores. Estas claves no guardan relación alguna con la identidad del USUARIO, y se suben al servidor para que puedan ser descargadas por aplicaciones Radar COVID en poder de otros usuarios. Con estas claves, mediante un procesamiento que tiene lugar en el teléfono móvil de forma descentralizada, se puede advertir al USUARIO sobre el riesgo de contagio por haber estado en contacto reciente con una persona que ha sido diagnosticada por COVID-19, sin que la aplicación pueda derivar su identidad o el lugar don-

de tuvo lugar el contacto.

Un código de confirmación de un solo uso de 12 dígitos facilitado por las autoridades sanitarias al USUARIO en caso de prueba positiva por COVID-19. Este código debe ser introducido a continuación por el usuario en la aplicación para permitir la carga voluntaria al servidor de las claves de exposición temporal.

El consentimiento del usuario, si aplica, para la remisión de claves de exposición temporal al nodo europeo de interoperabilidad de aplicaciones de rastreo de contactos.

El aviso de notificación de exposición, a efectos de recoger una estadística anónima y agregada del volumen de notificaciones que produce el sistema a través del rastreo de contactos. Estos datos permiten estimar cuántos usuarios han sido alertados por la Aplicación, de un riesgo potencial de infección, sin poder rastrear su identidad.

Toda la información se recogerá con fines estrictamente de interés público en el ámbito de la salud pública, y ante la situación de emergencia sanitaria decretada, a fin de proteger y salvaguardar un interés esencial para la vida de las personas, en los términos descritos en esta política de privacidad, y atendiendo a los artículos 6.1.a), 9.2.a), 6.1.c), 6.1.d), 6.1.e), 9.2.c), 9.2.h) y 9.2.i)

La legislación aplicable se enumera a continuación:

Reglamento (UE) 2016/679, 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).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública.

Ley 33/2011, de 4 de octubre, General de Salud Pública.

Ley 14/1986, de 25 de abril, General de Sanidad.

Real Decreto ley 21/2020, de 9 de junio, de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por el COVID-19.

Acuerdo de 9 de octubre de 2020, entre el Ministerio de Asuntos Económicos y Transformación Digital (Secretaría de Estado de Digitalización e Inteligencia Artificial) y el Ministerio de Sanidad acerca de la aplicación "Radar COVID".

5. ¿Cómo obtenemos y de dónde proceden tus datos?

El código de confirmación de positivo por COVID-19 facilitado por el Servicio Público de Salud. Esto permitirá la subida al servidor de las claves de exposición temporal con las que el dispositivo del usuario ha generado los códigos aleatorios enviados (identificadores efímeros Bluetooth) a los dispositivos con los que el usuario ha entrado en contacto, hasta un máximo de 14 días anteriores. Estas claves únicamente se suben al servidor con el consentimiento explícito e inequívoco del USUARIO, al haber introducido un código de confirmación de positivo por COVID-19.

El aviso de notificación de exposición es facilitado por la aplicación de forma anónima a los efectos de componer una estadística agregada del volumen de usuarios que han sido notificados.

6. ¿Para qué y por qué utilizamos tus datos?

La recogida, almacenamiento, modificación, estructuración y en su caso, eliminación, de los datos generados, constituirán operaciones de tratamiento llevadas a cabo por el Titular, con la finalidad de garantizar el correcto funcionamiento de la App, mantener la relación de prestación del servicio con el Usuario, y para la gestión, administración, información, prestación y mejora del servicio.

La información y datos recogidos a través de la Aplicación serán tratados con fines estrictamente de interés público en el ámbito de la salud pública, ante la actual situación de emergencia sanitaria como consecuencia de la pandemia del COVID-19 y la necesidad de su control y propagación, así como para garantizar intereses vitales tuyos o de terceros, de conformidad con la normativa de protección de datos vigente.

A tal efecto, utilizamos tus datos para prestarte el servicio de "Radar COVID" y para que puedas hacer uso de sus funcionalidades de acuerdo con sus condiciones de uso. De conformidad con el Reglamento General de Protección de Datos (RGPD) así como cualquier legislación nacional que resulte aplicable, la Secretaría General de Administración Digital tratará todos los datos generados durante el uso de la App para las siguientes finalidades:

Ofrecerte información sobre contactos considerados de riesgo de exposición a la COVID-19.

Proporcionarte consejos prácticos y recomendaciones de acciones a seguir según se produzcan situaciones de riesgo de cara a la cuarentena o auto-cuarentena.

Se utilizarán los datos siempre y sólo de forma anonimizada para fines estadísticos y epidemiológicos.

Este tratamiento se llevará a cabo a través de la funcionalidad de alerta de contagios que permite identificar situaciones de riesgo por haber estado en contacto estrecho con personas usuarias de la aplicación que se encuentran infectadas por la COVID-19. De esta manera se te informará de las medidas que conviene adoptar después.

7. ¿Durante cuánto tiempo conservamos tus datos?

Las claves de exposición temporal y los identificadores efímeros de Bluetooth son almacenados en el dispositivo por un periodo de 14 días, después de los cuales son eliminados.

Asimismo, las claves de exposición temporal que hayan sido comunicadas al servidor por los USUARIOS diagnosticados como positivos por COVID-19 también serán eliminadas del servidor al cabo de 14 días.

En todo caso, ni las claves de exposición temporal ni los identificadores efímeros de Bluetooth contienen datos de carácter personal ni permiten identificador los teléfonos móviles de los usuarios.

El aviso de notificación de exposición se agrega en el indicador de avisos diarios comunicados, siendo descartado para cualquier otro uso.

8. ¿Quién tiene acceso a tus datos?

Los datos gestionados por la aplicación móvil (claves diarias de exposición temporal e identificadores efímeros Bluetooth) se almacenan únicamente en el dispositivo del usuario a los efectos de poder hacer cálculos y avisar al USUARIO sobre su riesgo de exposición a la COVID-19.

Solo en el caso de reportar un diagnóstico positivo por COVID-19, las claves de exposición temporal de los últimos 14 días generadas en el dispositivo, y bajo el consentimiento explícito e inequívoco del USUARIO, son subidas al servidor para su difusión al conjunto de USUARIOS de este sistema.

Estas claves no guardan relación alguna con la identidad de los dispositivos móviles ni con datos personales de los USUARIOS de la Aplicación.

Los avisos de notificación de exposición comunicados solo se utilizan para la generación de datos estadísticos agregados y anónimos.

9. ¿Cuáles son tus derechos y cómo puedes controlar tus datos?

La normativa vigente te otorga una serie de derechos en relación con los datos e información que tratamos sobre ti. Concretamente, los derechos de acceso, rectificación, supresión, limitación y oposición.

Puedes consultar el alcance y detalle completo de los mismos en la página web de la Agencia Española de Protección de Datos (AEPD) aquí.

Con carácter general, podrás ejercitar todos estos derechos en cualquier momento y de forma gratuita. Puedes dirigirte a los Responsables de Tratamiento por vía electrónica, bien Ministerio de Sanidad o Comunidad Autónoma de residencia. En el caso del Ministerio de Sanidad, puede hacerlo a través de este formulario, o presencialmente a través de la red de oficinas de asistencia en materia de registros utilizando este modelo de solicitud (versión editable e imprimible).

Asimismo, te asiste en todo momento el derecho para presentar una reclamación ante Agencia Española de Protección de Datos.

10. ¿Cómo protegemos tus datos?

Los Responsables, así como la SGAD en condición de encargada del tratamiento, garantizan la seguridad, el secreto y la confidencialidad de tus datos, comunicaciones e información personal y han adoptado las más exigentes y robustas medidas de seguridad y medios técnicos para evitar su pérdida, mal uso o su acceso sin tu autorización. Las medidas de seguridad implantadas se corresponden con las previstas en el anexo II (Medidas de seguridad) del 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.

Finalmente, te informamos que tanto el almacenamiento como el resto de las actividades del tratamiento de datos no personales utilizados estarán siempre ubicados dentro de la Unión Europea.

11. ¿Qué tienes que tener especialmente en cuenta al utilizar "Radar COVID"?

Has de tener en cuenta determinados aspectos relativos a la edad mínima de utilización de Aplicación, la calidad de los datos que nos proporcionas, así como la desinstalación de la Aplicación en tu dispositivo móvil.

Edad mínima de utilización: para poder utilizar "Radar COVID" tienes que ser mayor de 18 años o contar con la autorización de tus padres y/o tutores legales. Por tanto, al darte de alta en la Aplicación, garantizas al Titular que eres mayor de dicha edad o, en caso contrario, que cuentas con la mencionada autorización.

Calidad de los datos que nos proporcionas: la información que nos facilites en el uso de los servicios de la Aplicación deberá de ser siempre real, veraz y estar actualizada.

Desinstalación de la Aplicación: en general, puedes desinstalar la aplicación en tu dispositivo en cualquier momento. Este proceso elimina de tu teléfono móvil el historial de códigos recibidos desde otros teléfonos móviles para las funciones de alerta de contactos estrechos.

12. Transferencia de datos a países de la Unión Europea

Radar COVID participa en la plataforma de integración de aplicaciones de la unión europea, de manera que se compartirán las claves positivas con terceros países de la UE y viceversa.

Cuando el dispositivo del usuario descarga las claves positivas para analizar posibles contactos estrechos, descargará también las claves positivas de terceros países adheridos al proyecto europeo.

Esto permitirá identificar posibles contactos estrechos tanto si el usuario ha estado visitando alguno de estos países como si ha estado en contacto estrecho con un visitante procedente de estos países.

Cuando el usuario introduce un código de confirmación de diagnóstico positivo por COVID-19, se solicitará el consentimiento del usuario libre, específico, informado e inequívoco para compartir sus claves infectadas con terceros países a través de la plataforma de interoperabilidad europea facilitando el rastreo digital de posibles contactos estrechos. La comunicación de tus claves infectadas a la red de países europeos adheridos a este proyecto es completamente voluntaria.

No se efectuarán transferencias de datos fuera de la Unión Europea

13. Política de cookies

Utilizamos solamente cookies técnicas que permiten al usuario la navegación y la utilización de las diferentes opciones o servicios que se ofrecen en la Aplicación como, por ejemplo, acceder a partes de acceso restringido o utilizar elementos de seguridad durante la navegación.

He leído el documento POLÍTICA DE PRIVACIDAD DE LA APLICACIÓN "Radar COVID".

TRIGÉSIMO OCTAVO: En la versión final de las "Condiciones de Uso de Radar COVID" consta la siguiente información:

CONDICIONES DE USO DE Radar COVID

AL DESCARGAR Y USAR LA APLICACIÓN MÓVIL "Radar COVID" MANIFIESTAS QUE HAS LEÍDO Y ACEPTAS ESTAS CONDICIONES DE USO Y LA POLÍTICA DE PRIVACIDAD. AQUÍ SE RECOGE TODA LA INFORMACIÓN RELATIVA A TUS DERECHOS Y OBLIGACIONES COMO USUARIO DE ESTA APLICACIÓN.

AVISO IMPORTANTE:

El USUARIO queda avisado de que la utilización de la Aplicación NO CONSTITUYE EN NINGÚN CASO UN SERVICIO DE DIAGNÓSTICO MÉDICO, DE ATENCIÓN DE URGENCIAS O DE PRESCRIPCIÓN DE TRATAMIENTOS FARMACOLÓGICOS, pues la utilización de la Aplicación no podría en ningún caso sustituir la consulta presencial personal frente a un profesional médico debidamente cualificado.

1. Qué es Radar COVID

Radar COVID es una aplicación que promueve la salud pública mediante un sistema de alerta de contactos de riesgo en relación a la COVID-19, poniendo a disposición de los USUARIOS (en adelante, individualmente, el "USUARIO", y conjuntamente los "USUARIOS"), la posibilidad de navegar por la Aplicación, accediendo a los contenidos y servicios de Radar COVID, de acuerdo con las presentes CONDICIONES DE USO.

Radar COVID detecta la intensidad de señales Bluetooth intercambiadas entre dispositivos que tienen esta aplicación activa, mediante el empleo de identificadores aleatorios efímeros, que no guardan relación con la identidad del teléfono móvil empleado o el USUARIO. El dispositivo de cada USUARIO descarga periódicamente las claves Bluetooth de todos los USUARIOS de la aplicación que hayan informado a través de la misma que se les ha diagnosticado COVID-19 (previa acreditación de las autoridades sanitarias), procediendo a determinar si el USUARIO ha establecido contacto de riesgo con alguno de ellos, verificado por las señales Bluetooth intercambiadas. Si es el caso, la aplicación le notifica este hecho, a fin de que pueda para tomar medidas, y contribuir de este modo a evitar que el virus se propague.

Radar COVID en su arquitectura emplea el Sistema de Notificación de Exposiciones (SNE) proporcionado por Apple y Google, y desarrollado a partir del Protocolo de DP-3T de rastreo de proximidad descentralizado para preservar la privacidad.

2. Uso de Radar COVID

Para la utilización de los servicios de Radar COVID, es requisito necesario que el USUARIO autorice la activación del sistema de comunicaciones Bluetooth de baja energía (BLE, Bluetooth Low Energy) por parte de la Aplicación, tras la descarga de la misma.

El USUARIO acepta sin reserva el contenido de las presentes CONDICIONES DE USO. En consecuencia, el USUARIO deberá leer detenidamente las mismas antes del acceso y de la utilización de cualquier servicio de Radar COVID bajo su entera responsabilidad.

AVISO IMPORTANTE: La utilización de la Aplicación es gratuita, libre y voluntaria para todos los ciudadanos. Para utilizar Radar COVID no es necesario estar registrado, ni aportar ningún dato personal, identificativo o no identificativo.

Al activar la aplicación, el USUARIO acepta:

a) envío de señales Bluetooth emitidas de forma anónima por su dispositivo;

b) la recepción y almacenamiento de señales Bluetooth de aplicaciones compatibles con Radar COVID, que se mantienen de forma anónima y descentralizada en los dispositivos de los USUARIOS durante un periodo no superior a 14 días;

c) la información ofrecida al USUARIO sobre el posible riesgo de contagio, sin que en ningún momento se refieran datos personales de ningún tipo.

d) recibir claves positivas de terceros países de la Unión Europea a través de la plataforma de interoperabilidad de la unión europea (EFGS);

e) bajo consentimiento explícito, el envío de claves positivas que serán compartidas con terceros países de la Unión Europea a través de la plataforma de interoperabilidad de la unión europea (EFGS).

El USUARIO puede informar voluntariamente a la aplicación de un resultado positivo en sus pruebas de COVID-19 mediante el código de confirmación de un solo uso facilitado por las autoridades sanitarias. La validez de este código será cotejada por la aplicación para asegurar el correcto funcionamiento de Radar COVID. El USUARIO informará de los resultados de sus pruebas y se le solicitará el consentimiento expreso e inequívoco para compartir las claves generadas diariamente en su dispositivo, y correspondientes a los últimos 14 días. Estas claves son comunicadas a un servidor que las pondrá a disposición del conjunto de aplicaciones Radar COVID para su descarga. Las claves comunicadas no guardan relación alguna con la identificación del dispositivo o el USUARIO.

3. Seguridad y privacidad

Las medidas de seguridad implantadas se corresponden con las previstas en el anexo II (Medidas de seguridad) del 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.

Te informamos que tus datos serán tratados conforme a lo establecido en la Política de Privacidad de la Aplicación, cuyo contenido íntegro se puede consultar en el siguiente enlace: Política de Privacidad.

Toda la información se tratará con fines estrictamente de interés público en el ámbito de la salud pública, y ante la situación de emergencia sanitaria decretada, a fin de proteger y salvaguardar un interés esencial para la vida de las personas, en los términos descritos en la política de privacidad.

La información de la actividad de los USUARIOS es anónima y en ningún momento se exigirá a los USUARIOS ningún dato personal. En todo momento, el USUARIO puede desactivar el sistema de traza de contactos Bluetooth en la aplicación, así como desinstalar la Aplicación.

4. Cambio del servicio y terminación

Radar COVID siempre está tratando de mejorar el servicio y busca ofrecer funcionalidades adicionales útiles para el USUARIO teniendo siempre presente la preservación de la salud pública. Esto significa que podemos añadir nuevas

funciones o mejoras, así como eliminar algunas de las funciones. Si estas nuevas funciones o mejoras afectan materialmente a los derechos y obligaciones del USUARIO, será informado a través de la Aplicación para que adopte las decisiones oportunas sobre la continuación de su uso.

El USUARIO puede dejar de utilizar la aplicación en cualquier momento y por cualquier motivo, desinstalándola de su dispositivo.

5. Titular de la aplicación

La Secretaría General de Administración Digital (SGAD), dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, es el órgano TITULAR de la aplicación.

6. Responsabilidad y obligaciones

Radar COVID se ofrece dedicando los mejores esfuerzos, dado que su calidad y disponibilidad pueden verse afectadas por múltiples factores ajenos al TITULAR como son, entre otros, el volumen de otros USUARIOS en la ubicación geográfica del USUARIO, limitaciones o restricciones de las redes de terceros operadores o la compatibilidad del dispositivo y sistema operativo utilizado por el USUARIO. Igualmente, los USUARIOS aceptan que el servicio pueda verse interrumpido cuando sea necesario por labores de mantenimiento.

Por todo ello, el TITULAR no será responsable de los problemas de acceso o disponibilidad de Radar COVID y/o de sus servicios, ni de los perjuicios que se pudieran causar por ello, cuando éstos procedan de factores ajenos a su ámbito de control.

Igualmente, el TITULAR no se hace responsable de los siguientes hechos, ni de fallos, incompatibilidades y/o daños de tus terminales o dispositivos que, en su caso, se pudiesen derivar de la descarga y/o uso de la Aplicación:

Actualización, exactitud, exhaustividad, pertinencia, actualidad y fiabilidad de sus contenidos, cualquiera que sea la causa y las dificultades o problemas técnicos o de otra naturaleza en los que tengan su origen dichos hechos.

La calidad, titularidad, legitimidad, adecuación o pertinencia de los materiales, y demás contenidos.

Como USUARIO de la Aplicación te obligas a:

Impedir el acceso de terceras personas no autorizadas a la aplicación desde tu dispositivo.

Notificar al TITULAR con carácter inmediato cualquier indicio de la existencia de una violación en la seguridad en la Aplicación, de usos inapropiados o prohibidos de los servicios prestados desde la misma, o de fallos de seguridad de cualquier índole.

Hacer buen uso de los contenidos, información y servicios prestados desde o a través de la Aplicación, conforme a la ley, la buena fe y a las buenas costumbres generalmente aceptadas, comprometiéndose expresamente a:

Abstenerse de realizar prácticas o usos de los servicios con fines ilícitos, fraudulentos, lesivos de derechos o intereses del TITULAR o de terceros, infractores de las normas contenidas en el presente documento.

Abstenerse de realizar cualquier tipo de acción que pudiera inutilizar, sobrecargar o dañar sistemas, equipos o servicios de la Aplicación o accesibles directa o indirectamente a través de esta.

Respetar los derechos de propiedad intelectual e industrial del TITULAR y de terceros sobre los contenidos, información y servicios prestados desde o a través de la Aplicación, absteniéndose con carácter general de copiar, distribuir, reproducir o comunicar en forma alguna los mismos a terceros, de no mediar autorización expresa y por escrito del TITULAR o de los titulares de dichos derechos.

No proporcionar información falsa en la Aplicación, siendo el único responsable de la comunicación real y veraz.

No suplantar la personalidad de un tercero.

El USUARIO de la Aplicación es el único responsable del uso que decida realizar de los servicios de Radar COVID.

El TITULAR no será responsable en ningún caso de la utilización indebida de Radar COVID y de sus contenidos, siendo el USUARIO el único responsable por los daños y perjuicios que pudieran derivarse de un mal uso de estos o de la infracción de lo dispuesto en las presentes condiciones en que pueda incurrir. El USUARIO se compromete a mantener indemne al TITULAR frente a las reclamaciones o sanciones que pudiera recibir de terceros, ya sean particulares o entidades públicas o privadas, por razón de dichas infracciones, así como frente a los daños y perjuicios de todo tipo que pueda sufrir como consecuencia de las mismas.

En cualquier caso, el TITULAR se reserva, en cualquier momento y sin necesidad de previo aviso, el derecho de modificar o eliminar el contenido, estructura, diseño, servicios y condiciones de acceso y/o uso de esta Aplicación, siempre que dicho cambio no afecte a los principios y derechos de protección de datos, así como el derecho interpretar las presentes condiciones, en cuantas cuestiones pudiera plantear su aplicación.

Asimismo, queda prohibida la reproducción, distribución, transmisión, adaptación o modificación, por cualquier medio y en cualquier forma, de los contenidos de Radar COVID o sus cursos (textos, diseños, gráficos, informaciones, bases de datos, archivos de sonido y/o imagen, logos y demás elementos de estos sitios), salvo las permitidas por la licencia de liberación de código abierto bajo la que se ha publicado el sistema.

La enumeración anterior tiene mero carácter enunciativo y no es, en ningún caso, exclusivo ni excluyente en ninguno de sus puntos. En todos los supuestos, El TITULAR EXCLUYE CUALQUIER RESPONSABILIDAD POR LOS DAÑOS Y PERJUICIOS DE CUALQUIER NATURALEZA DERIVADOS DIRECTA O INDIRECTAMENTE DE LOS MISMOS Y DE CUALESQUIERA OTROS NO ESPECIFICADOS DE ANÁLOGAS CARACTERISTICAS.

El TITULAR NO OFRECE NINGUNA GARANTÍA, EXPRESA, IMPLÍCITA, LEGAL O VOLUNTARIA.

EL TITULAR EXCLUYE EXPRESAMENTE TODAS LAS GARANTÍAS IMPLÍCITAS, INCLUYENDO, A TÍTULO ENUNCIATIVO, PERO NO LIMITATIVO, CUALQUIER GARANTÍA IMPLÍCITA O SANEAMIENTO DE VICIOS OCUL-

TOS, COMERCIABILIDAD, CALIDAD SATISFACTORIA, TÍTULO, IDONEIDAD DEL PRODUCTO PARA UN PROPÓSITO EN PARTICULAR Y CUALQUIER GARANTÍA O CONDICIÓN DE NO INFRACCIÓN. ESTA EXCLUSIÓN DE RESPONSABILIDAD SÓLO SE APLICARÁ EN LA MEDIDA PERMITIDA POR LA LEY IMPERATIVA APLICABLE.

7. Enlaces

Radar COVID puede incluir dentro de sus contenidos enlaces con sitios pertenecientes y/o gestionados por terceros con el objeto de facilitar el acceso a información y servicios disponibles a través de Internet.

El TITULAR no asume ninguna responsabilidad derivada de la existencia de enlaces entre los contenidos de Radar COVID y contenidos situados fuera de los mismos o de cualquier otra mención de contenidos externos, exceptuando aquellas responsabilidades establecidas en la normativa de protección de datos. Tales enlaces o menciones tienen una finalidad exclusivamente informativa y, en ningún caso, implican el apoyo, aprobación, comercialización o relación alguna entre el TITULAR y las personas o entidades autoras y/o gestoras de tales contenidos o titulares de los sitios donde se encuentren, ni garantía alguna del TITULAR por el correcto funcionamiento de los sitios o contenidos enlazados.

En este sentido el USUARIO se obliga a poner la máxima diligencia y prudencia en el caso de acceder o usar contenidos o servicios de los sitios a los que acceda en virtud de los mencionados enlaces.

8. Hiperenlaces

No se admite la reproducción de páginas de Radar COVID mediante hiperenlace desde otra Aplicación móvil o página web, permitiéndose exclusivamente el acceso desde la Aplicación.

En ningún caso se podrá dar a entender que el TITULAR autoriza el hiperenlace o que ha supervisado o asumido de cualquier forma los servicios o contenidos ofrecidos por la web desde la que se produce el hiperenlace.

No se podrán realizar manifestaciones o referencias falsas, incorrectas o inexactas sobre las páginas y servicios del TITULAR.

Se prohíbe explícitamente la creación de cualquier tipo de navegador, programa, "browser" o "border environment" sobre las páginas de Radar COVID.

No se podrán incluir contenidos contrarios a los derechos de terceros, ni contrarios a la moral y las buenas costumbres aceptadas, ni contenidos o informaciones ilícitas, en la página web desde la que se establezca el hiperenlace.

La existencia de un hiperenlace entre una página web y el Radar COVID no implica la existencia de relaciones entre el TITULAR y el propietario de esa página, ni la aceptación y aprobación de sus contenidos y servicios.

9. Ley aplicable y fuero

Las presentes condiciones de uso se regirán e interpretarán en todos y cada uno de sus extremos por la legislación española. En aquellos casos en los que la normativa vigente no prevea la obligación de someterse a un fuero o legislación determinado, el TITULAR y los USUARIOS, con renuncia a cualquier otro

fuero que pudiera corresponderles, se someten a los juzgados y tribunales de Madrid capital (España).

10. Información corporativa y contacto

Dirección: Calle de Manuel Cortina, 2, 28010 Madrid

TRIGÉSIMO NOVENO: Con fecha 15 de octubre de 2020 se publica en el BOE la "Resolución de 13 de octubre de 2020, de la Subsecretaría, por la que se publica el Acuerdo entre el Ministerio de Asuntos Económicos y Transformación Digital y el Ministerio de Sanidad, acerca de la aplicación "Radar COVID"". Con fecha 10/10/2020 entra en vigor dicha resolución.

El Acuerdo se suscribe entre el Secretario General de Administración Digital, por delegación de la SEDIA, y el Secretario General de Salud Digital, Información e Innovación del Sistema Nacional de Salud, por delegación del MSND.

En este se señalan las competencias de los intervinientes:

"*Segundo.- Que de acuerdo con lo previsto en el artículo 7.1 del Real Decreto 735/2020, de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio de Sanidad, la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud (en adelante, SGSDII) es el órgano directivo del Ministerio de Sanidad al que, bajo la superior dirección de la persona titular del Departamento, corresponde abordar los proyectos de modernización, innovación, mejora y transformación del Sistema Nacional de Salud.*

Tercero. Que, de acuerdo con lo previsto en el artículo 8.2.a) del Real Decreto 735/2020, de 4 de agosto, la Dirección General de Salud Digital y Sistemas de Información para el Sistema Nacional de Salud es el órgano directivo dependiente de la Secretaría General de Salud Digital a quien corresponde el diseño, desarrollo e implantación de los servicios electrónicos comunes del Sistema Nacional de Salud, las aplicaciones informáticas y de salud digital del Ministerio de Sanidad, así como los portales sectoriales y horizontales de dicho Departamento, garantizando su integración y homogeneidad

Cuarto.- Que de acuerdo con lo previsto en el Real Decreto 403/2020, de 25 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Asuntos Económicos y Transformación Digital, corresponde a la Secretaría General de Administración Digital (en adelante SGAD), órgano directivo de la Secretaría de Estado de Digitalización e Inteligencia Artificial, la dirección, coordinación y ejecución de las competencias atribuidas a la Secretaría de Estado en materia de transformación digital de la administración".

En el "EXPONEN" Sexto dice:

"*Que en aplicación de dichos principios, desde el mes de mayo de 2020, la SGAD ha venido desarrollando, con el conocimiento y la conformidad del Ministerio de Sanidad, una aplicación para la trazabilidad de contactos en relación a la pandemia ocasionada por la COVID-19 denominada «Radar COVID. Durante el mes de julio de 2020, con la conformidad de la Dirección General de Salud Pública, Calidad e Innovación del Ministerio de Sanidad, la SGAD llevó a cabo con éxito el pro-*

yecto piloto de la misma, cuyo éxito garantiza la viabilidad de la solución propuesta para el rastreo de contactos estrechos"

En el "EXPONEN" Noveno dice:

"Que, hasta el momento, el Ministerio de Sanidad ha venido colaborando con la SGAD, titular de la aplicación «Radar COVID», en los procesos de ajuste funcional de la misma desde la perspectiva de salud pública, coordinando los protocolos de manejo epidemiológico de casos detectados a través de la aplicación, y favoreciendo la incorporación progresiva de las comunidades y ciudades autónomas a su utilización en fase de pruebas con datos reales según el mencionado Acuerdo de 19 de agosto de 2020."

La primera de las cláusulas dice:

Primera. Objeto. Es objeto del presente Acuerdo:

a) Delegar en la Secretaría General de Administración Digital (en adelante, SGAD) del Ministerio de Asuntos Económicos y Transformación Digital, todas las competencias de diseño, desarrollo, implantación y evolución de la aplicación «Radar COVID» que correspondan a la Dirección General de Salud Digital y Sistemas de Información para el Sistema Nacional de Salud en virtud de lo previsto en el artículo 8.2.a) del Real Decreto 735/2020, de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio de Sanidad, la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud. La Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud ha aprobado previamente la delegación de todas estas competencias en la SGAD de acuerdo con lo previsto en el artículo 9.1 de la Ley 40/2015, de 1 de octubre.

b) Delegar en la SGAD la competencia del Ministro de Sanidad para suscribir con las comunidades y ciudades autónomas los convenios de colaboración para la adhesión de estas al uso de la aplicación «Radar COVID», de acuerdo con lo previsto en el Capítulo VI del Título Preliminar de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. sin perjuicio del apoyo que para facilitar su tramitación le prestará la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud.

La segunda de las cláusulas dice:

Segunda. Obligaciones de las partes con relación a la delegación de competencias prevista en la letra a) de la cláusula primera:

1. Con la firma del presente Acuerdo, con relación a la delegación de competencias prevista en la letra a) de la cláusula primera la SGAD se compromete al cumplimiento de las siguientes obligaciones:

a) La contratación del mantenimiento evolutivo, correctivo, adaptativo y perfectivo del sistema «Radar COVID» con cargo a sus créditos presupuestarios.

b) La publicación en abierto del código fuente del sistema «Radar COVID».

c) El soporte a la operación del sistema y la gestión de la infraestructura asociada.

d) El soporte y atención a usuarios y comunidades y ciudades autónomas en relación con los aspectos técnicos de este sistema.

e) Cualesquiera otras obligaciones necesarias para el correcto funcionamiento de la aplicación y, en especial su integración con el sistema europeo de intercambio de contactos, incluyendo la solicitud formal de adhesión al sistema.

2. Las decisiones en relación con la evolución de la Aplicación se adoptarán de común acuerdo entre las partes.

3. Con relación a la delegación de competencias prevista en la letra a) de la cláusula primera de este Acuerdo, corresponden a la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud, además de sus obligaciones como Responsable del tratamiento de datos de carácter personal, y su Dirección General de Salud Digital y Sistemas de Información para el Sistema Nacional de Salud, las siguientes obligaciones:

a) El seguimiento del diseño e implementación del sistema «Radar COVID».

b) La recepción de los datos que obren en poder de la SGAD (relacionados con su descarga activa, uso, códigos utilizados, etc) para el adecuado seguimiento epidemiológico de la Pandemia en España, así como su relación con otros países europeos.

c) El impulso de las medidas necesarias para su correcta aplicación dentro del ámbito de competencias de la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud, así como el impulso de los acuerdos que fuera necesario adoptar al respecto en el Consejo Interterritorial del Sistema Nacional de Salud.

d) El análisis del cumplimiento de objetivos y, en su caso, la propuesta de reformulación de procedimientos e indicadores para ajustarlos a necesidades sobrevenidas.

e) Cualesquiera otras obligaciones necesarias para el correcto funcionamiento de la aplicación.

La tercera de las cláusulas en el apartado 1 y 2 dice:

1. En los Convenios de colaboración que la SGAD subscriba por delegación del Ministro de Sanidad para la adhesión de las comunidades y ciudades autónomas al uso de la aplicación «Radar COVID», la SGAD se comprometerá al cumplimiento de las siguientes obligaciones:

a) La puesta a disposición del uso de la Aplicación conforme a lo previsto en el Convenio.

b) La distribución a las consejerías competentes en materia de sanidad de los códigos positivos necesarios para que los usuarios de la Aplicación con test PCR positivo los introduzcan en la misma, garantizando así la inexistencia de falsos positivos en el sistema.

c) La adopción de las medidas de seguridad precisas para proteger la información contenida en la aplicación y los sistemas asociados a soluciones tecnológicas objeto de dicho Convenio.

d) La asunción del compromiso de no reidentificación de los interesados.

e) La asunción del compromiso de no almacenamiento de códigos o elementos que pudieran llegar a permitir la reidentificación de las personas, incluyendo direcciones IP.

f) El establecimiento de plazos de limitación y supresión de las informaciones obtenidas, incluidos los logs del aplicativo, como parte del ciclo de vida del dato, previa aprobación del Ministerio de Sanidad en su condición de responsable del tratamiento.

g) La asunción del compromiso de no llevar a cabo el procesamiento unilateral de los datos, dando lugar a tratamientos u operaciones de tratamiento diferentes a las establecidas en el convenio o similares que no hubieran sido previstas en dicho convenio.

h) La asunción del compromiso de no llevar a cabo la toma de decisiones automatizadas u otras decisiones que pudieran afectar a los interesados.

i) El establecimiento, junto con la consejería competente en materia de sanidad de la comunidad o ciudad autónoma de que se trate, del detalle de quién pone fin al ciclo de vida del tratamiento de datos personales y términos en los que debería llevarse a cabo la eliminación definitiva de toda información, junto con el compromiso de ambas partes de no mantener datos más allá del acuerdo del fin del ciclo de vida del tratamiento.

j) Cualesquiera otras obligaciones necesarias para el buen fin de la aplicación que la SGAD pueda llevar a cabo en su ámbito competencial.

2. En los mencionados Convenios de colaboración, el Ministerio de Sanidad y la Consejería competente en materia de sanidad de la comunidad o ciudad autónoma de que se trate figurarán como responsables del tratamiento de datos de carácter personal y la SGAD como encargado del tratamiento, a los efectos previstos en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y demás normativa de aplicación en materia de protección de datos.

3. Con relación a la delegación de competencias prevista en la letra b) de la cláusula primera de este Acuerdo, corresponden a la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud, en su condición de Responsable del tratamiento de datos de carácter personal, dar las indicaciones necesarias a la SGAD en su condición de encargado del tratamiento.

Asimismo, corresponden a la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud y su Dirección General de Salud Digital y Sistemas de Información para el Sistema Nacional de Salud las siguientes obligaciones:

a) La colaboración con la SGAD y las consejerías de las comunidades y ciudades autónomas competentes en la materia en todas las acciones necesarias para la correcta implantación y desarrollo del sistema «Radar COVID».

b) Velar por el correcto funcionamiento del sistema «Radar COVID», en particular en lo referente a la defensa de los derechos de los interesados.

c) El seguimiento permanente de los resultados del sistema «Radar COVID» para trasladarlos a las autoridades sanitarias de las distintas Administraciones

Públicas.

d) El impulso de las medidas necesarias para su correcta desarrollo y ejecución dentro del ámbito de competencias de la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud, así como el impulso de los acuerdos que fuera necesario adoptar al respecto en el Consejo Interterritorial del Sistema Nacional de Salud.

e) Cualesquiera otras obligaciones necesarias para el buen fin de la aplicación que puedan abordarse desde las competencias de la dicha Secretaría General.

La cláusula décima dice:

Décima. Régimen de protección de datos, seguridad y confidencialidad.

1. El régimen de protección de datos de carácter personal en las actuaciones que se desarrollen en ejecución del presente Acuerdo será el previsto en el Reglamento general de protección de datos y en la Ley Orgánica 3/2018, de 5 de diciembre, y demás normativa de aplicación en materia de protección de datos.

2. Las partes velarán por el cumplimiento del 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.

3. Toda la información facilitada por las partes y toda la información generada como consecuencia de la ejecución del presente Acuerdo, tendrá el tratamiento de confidencial, sin perjuicio de la información que sea de dominio público, no pudiendo ser divulgada o facilitada a terceros, ni utilizada para un fin distinto del previsto en este documento, sin el acuerdo unánime de las partes.

4. La obligación de confidencialidad para las partes se extenderá indefinidamente aunque el Acuerdo se hubiera extinguido. Todo ello sin perjuicio de la eventual autorización de las partes o en su caso, de que dicha información pasara a ser considerada como de dominio público.

CUADRAGÉSIMO: Con fecha 22 de octubre de 2020 el METD publica esta nota de prensa:

"Las principales operadoras de telefonía se comprometen a no repercutir el consumo de datos de la app RadarCOVID a sus usuarios. (…)

La secretaria de Estado de Digitalización e Inteligencia Artificial, Carmen Artigas, ha mantenido esta mañana un encuentro con representantes de las principales operadoras de telefonía del país con el objetivo de establecer vías de colaboración para la difusión de la aplicación móvil de traceo de contactos RadarCOVID.

La reunión se enmarca dentro de una serie de encuentros sectoriales con distintos actores, instituciones y empresas para explorar posibles modelos de apoyo para la expansión e implantación entre la ciudadanía de esta herramienta digital."

CUADRAGÉSIMO PRIMERO: La App Radar COVID consta inscrita en el Registro de actividades de tratamiento (RAT) del MSND, SGSDII, en los siguientes términos:

RESPONSABLE:

SECRETARÍA GENERAL DE SALUD DIGITAL, INFORMACIÓN E INNOVACIÓN DEL SISTEMA NACIONAL DE SALUD. Paseo del Prado, 18. 20. Madrid 28071.

sgsdii@sanidad.gob.es

DELEGADA DE PROTECCION DE DATOS Titular de la Inspección General de Servicios del Ministerio. delegadoprotecciondatos@mscbs.es

FINES DEL TRATAMIENTO:

El tratamiento tiene por finalidad facilitar la trazabilidad de contactos en relación a la pandemia ocasionada por la COVID-19 mediante alertas al usuario.

BASE JURÍDICA DEL TRATAMIENTO:

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

• Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

• Ley 14/1986, de 25 de abril, General de Sanidad

•Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública.

• Ley 33/2011, de 4 de octubre, General de Salud Pública.

• Real Decreto 463/2020 de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID.19 que atribuye al Ministro de Sanidad la necesaria competencia en todo el territorio nacional.

• Orden Ministerial SND/297/2020 de 27 de marzo, por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de nuevas actuaciones.

CATEGORIAS DE INTERESADOS

Personas que voluntariamente se han descargado la aplicación móvil, han sido diagnosticadas como caso positivo en COVID y han remitido el código facilitado por los servicios de salud de las CCAAs en la aplicación.

CATEGORIAS DE DATOS PERSONALES:

Los datos manejados por la aplicación no permiten la identificación directa del usuario o de su dispositivo ni su geolocalización.

Como parte del sistema de alerta de contagios de la COVID-19, se procesarán los siguientes datos para los usuarios que hayan dado positivo por COVID.19 para los fines especificados a continuación:

o Las claves de exposición temporal con las que el dispositivo del usuario ha generado los códigos aleatorios enviados (identificadores efímeros Bluetooth), a los dispositivos con los que el usuario ha entrado en contacto, hasta un máximo de 14 días anteriores.

o Un código de confirmación de un solo uso de 12 dígitos facilitado por las autoridades sanitarias en caso de prueba positiva por COVID.19.

Cuestionario voluntario para la recogida de información sobre la experiencia de uso

de la aplicación, comprensión de la misma o percepción sobre la privacidad, entre otros.

CATEGORIAS DE DESTINATARIOS:

Usuario de la aplicación.

TRANSFERENCIAS INTERNACIONALES:

No previstas, salvo obligación legal.

PLAZO DE SUPRESIÓN

Las claves de exposición temporal y los identificadores efímeros de Bluetooth son almacenados en el dispositivo por un periodo de 14 días, después de los cuales son eliminados.

Asimismo, las claves de exposición temporal que hayan sido comunicadas al servidor por los USUARIOS diagnosticados como positivos por COVID-19 también serán eliminadas del servidor al cabo de 14 días.

MEDIDAS TECNICAS Y ORGANIZATIVAS DE SEGURIDAD:

Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del 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 y que se encuentran descritas en los documentos que conforman la Política de protección de datos y seguridad de la información del Ministerio.

CUADRAGÉSIMO SEGUNDO: No consta acreditado que la SEDIA recabara el asesoramiento del delegado de protección de datos del METD, al realizar la evaluación de impacto relativa a la protección de datos.

CUADRAGÉSIMO TERCERO: Con fecha 9 de septiembre de 2020 se produce la publicación en abierto del código fuente del sistema «Radar COVID»:

radar-covid-android – Aplicación RadarCOVID para Android - 9 Sept 2020 – GitHub - RadarCOVID/radar-covid-android at 67a4506cc43a20062e87aebd5caa6be2ea0f6482

radar-covid-ios – Aplicación iOS para RadarCOVID – 9 Sept 2020 – GitHub - RadarCOVID/radar-covid-ios at 118d6239fc42e369db83e0f2555b62d3e72fc1be

radar-covid-backend-dp3t-server – Servidor DPT3 - 9 Sept 2020 – GitHub - RadarCOVID/radar-covid-backend-dp3t-server at 2ea39a5e03ad3da1ff4c7f6567be6b778fb79c7d

CUADRAGÉSIMO CUARTO: En el escrito de respuesta al requerimiento de fecha 26 de octubre de 2020, notificado a la SEDIA, se confirma la existencia de una vulnerabilidad que es corregida en la subida correspondiente al 8 de octubre, para las siguientes versiones de la aplicación:

1. Android, versión 1.0.9

2. Apple, versión 1.0.8

Se confirma que a fecha de 8 de octubre, se habían declarado un total de 3.059 códigos a nivel nacional, si bien es cierto que a fecha de la publicación del código fuente (9/sep), ya se habían reportado un total de 574 códigos.

CUADRAGÉSIMO QUINTO: En enero de 2022 se continua facilitando la siguiente in-

formación en las “Preguntas frecuentes” del sitio web: https://radarcovid.gob.es/faq-datos-personales-y-privacidad:

¿Cómo se protege mi privacidad?

Durante todo el proceso de diseño y desarrollo de Radar COVID, la protección de tu privacidad ha sido una prioridad.

Aquí tienes una lista de algunas de las medidas con las que Radar COVID protege tus datos:

- *La aplicación no recopila ningún dato que permita rastrear tu identidad. Por ejemplo, no te preguntará y no podrá conocer tu nombre, apellidos, dirección, número de teléfono o dirección de correo electrónico.*
- *La aplicación no recopila ningún dato de geolocalización, incluidos los del GPS. Además, tampoco realiza ningún seguimiento de tus desplazamientos.*
- *El código de Bluetooth Low Energy (de baja energía) que se transmite a través de la aplicación se genera aleatoriamente y no contiene ninguna información sobre tu smartphone ni sobre ti.*
- *Además, este código cambia varias veces cada hora para proteger aún más tu privacidad.*
- *Los datos que se guardan en tu teléfono móvil están cifrados.*
- *Las conexiones entre la aplicación y el servidor están cifradas.*
- *Todos los datos, tanto los que se guardan en el dispositivo (códigos intercambiados con otros teléfonos móviles) son eliminados al cabo de 14 días.*
- *Asimismo, los datos recogidos en el servidor, procedentes de los teléfonos móviles donde se ha reportado un diagnóstico positivo por COVID-19, son eliminados al cabo de 14 días.*
- *Ningún dato almacenado en los teléfonos móviles o en el servidor permite la identificación ni del propio dispositivo móvil ni del usuario del mismo*

¿Radar COVID comparte o vende mis datos?

Radar COVID no recoge datos personales de ningún tipo. Solo almacena en los dispositivos móviles información sobre los códigos provenientes de otros teléfonos móviles que han estado en proximidad con tu teléfono. Estos códigos no permiten identificar ni al dispositivo ni a su usuario.

El servidor con el que se comunican las aplicaciones en caso de reportarse un diagnóstico positivo por la COVID-19, solo almacena los códigos que ha generado el teléfono de la persona infectada, en los últimos 14 días. De nuevo, estos códigos son aleatorios y no permiten identificar ni al dispositivo móvil ni al usuario.

Por todo lo anterior, Radar COVID no maneja información susceptible de ser vendida o utilizada para ningún objetivo comercial, incluyendo la creación de perfiles con fines publicitarios. Este proyecto no tiene ningún ánimo de lucro, siendo creado exclusivamente para ayudar a combatir la epidemia. No se descarta el análisis de datos agregados sobre volumen de descargas de la aplicación, volumen de usuarios contagiados, u otros indicadores anónimos y agre-

gados, para proyectos de investigación científica.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control y según lo establecido en los artículos 47, 48, 64.2 y 68.1 de la LOPDGDD, la directora de la AEPD es competente para iniciar y resolver este procedimiento.

II

El artículo 63.2 de la LOPDGDD determina que: *"Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."*

III

Se imputa a la SEDIA la comisión de varias infracciones por vulneración de los artículos: 5.1.a), 5.2, 12, 13, 25, 28.3 y 28.10 y 35 del RGPD.

Las infracciones están tipificadas en los artículos 83.5.a), 83.5.b) y 83.4.a) del RGPD y son calificadas, a los solos efectos de determinar los plazos de prescripción, en los artículos 72.1.a) y h) y 73.d), k), m) y t) de la LOPDGDD.

El artículo 83.5.a) y b) del RGPD indica:

> *"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:*
>
> *a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;*
>
> *b) los derechos de los interesados a tenor de los artículos 12 a 22;*

A este respecto, la LOPDGDD, en su artículo 71 establece que *"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica".*

A efectos del plazo de prescripción, el artículo 72 de la LOPDGDD indica:

> *"Artículo 72. Infracciones consideradas muy graves.*
>
> *1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:*
>
> *a) El tratamiento de datos personales vulnerando los principios y garantías esta-*

blecidos en el artículo 5 del Reglamento (UE) 2016/679.

(…)

h) La omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en los artículos 13 y 14 del Reglamento (UE) 2016/679 y 12 de esta ley orgánica."

Por su parte, el artículo 83.4.a) del RGPD indica:

"4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía: a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;"

A efectos del plazo de prescripción, el artículo 73 de la LOPDGDD indica:

"Artículo 73. Infracciones consideradas graves. En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

(…)

d) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño, así como la no integración de las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25 del Reglamento (UE) 2016/679. (…)

k) Encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679. (…)

m) La infracción por un encargado del tratamiento de lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica, al determinar los fines y los medios del tratamiento, conforme a lo dispuesto en el artículo 28.10 del citado reglamento. (…)

t) El tratamiento de datos personales sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible."

Asimismo, el artículo 83.7 del RGPD dice:

Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro.

En este sentido, la LOPDGDD en su artículo 77, bajo el epígrafe "Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento", establece lo siguiente:

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

(…)

c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.

(…)

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación. Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción. Cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica".

En resumen, la LOPDGDD no faculta a imponer multas administrativas, sino una sanción de apercibimiento, es decir, sin efecto económico alguno.

IV

En relación con las alegaciones aducidas a la propuesta de resolución se procede a

dar respuesta a las mismas según el orden expuesto por la SEDIA:

I. ANTECEDENTES

Ciertamente, con fecha 26 de febrero de 2021, en virtud de los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 del RGPD, y de conformidad con lo establecido en el artículo 67 de la LOPDGDD, la SGID emitió un informe de actuaciones previas de investigación y con fecha 21 de mayo de 2021, la AEPD acordó el inicio del expediente sancionador.

En cuanto al inicio de las actuaciones previas de investigación, la Sentencia de la Audiencia Nacional (SAN), 4988/2007, 17 de octubre de 2007, justifica la conveniencia de las actuaciones previas de investigación en relación con los procedimientos sancionadores afirmando que:

> "*Se trata de que por la gravedad y trascendencia que entraña el ejercicio de la potestad sancionadora, pues el status jurídico de quien se halla sometido a un expediente sancionador, por esta sola circunstancia, puede encontrarse negativamente afectado, resulta necesario que la decisión de incoar el procedimiento sancionador sea fundada y este asentada en sólidas razones que exijan dicha incoación.*
>
> *Es decir, con la finalidad de permitir a la Administración conocer los hechos previsiblemente infractores, las circunstancias concurrentes y las personas intervinientes, se permite a la misma practicar dichas actuaciones de investigación o indagación previas, en cuanto sean necesarias y oportunas para verificar, hasta que punto, existe base racional para entender producido el hecho infractor, e imputárselo a persona determinada."*

El artículo 67 de la LOPDGDD establece que:

> "*Antes de la adopción del acuerdo de inicio de procedimiento, y una vez admitida a trámite la reclamación si la hubiese, la Agencia Española de Protección de Datos podrá llevar a cabo actuaciones previas de investigación a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento. La Agencia Española de Protección de Datos actuará en todo caso cuando sea precisa la investigación de tratamientos que implique un tráfico masivo de datos personales*".

Hay que señalar que el artículo 53 de la LOPDGDD determina el "Alcance de la actividad de investigación":

> *"1. Quienes desarrollen la actividad de investigación podrán recabar las informaciones precisas para el cumplimiento de sus funciones, realizar inspecciones, requerir la exhibición o el envío de los documentos y datos necesarios, examinarlos en el lugar en que se encuentren depositados o en donde se lleven a cabo los tratamientos, obtener copia de ellos, inspeccionar los equipos físicos y lógicos y requerir la ejecución de tratamientos y programas o procedimientos de gestión y soporte del tratamiento sujetos a investigación. (…)"*

Así las cosas, y teniendo en cuenta las consideraciones expuestas, la Agencia puede realizar las investigaciones que considere oportunas independientemente de que se haya presentado alguna reclamación o no, tras lo que puede decidir iniciar de oficio un procedimiento sancionador (artículo 68 de la LOPDGDD).

En relación con las alegaciones formuladas por la SEDIA, hemos de manifestar que la AEPD en el ejercicio de sus competencias, conforme le confieren los artículos 57 y 58 del RGPD en el que se establecen sus funciones y poderes respectivamente, solicitó a la SEDIA la información que consideró oportuna para aclarar los hechos controvertidos y determinar las actuaciones efectuadas por la SEDIA, en concreto respecto al rol ejercido en relación con el tratamiento de datos personales a través de la aplicación.

II. ALEGACIONES.

Las alegaciones formuladas a las actuaciones previas de investigación, al acuerdo de inicio y durante el periodo de prueba, fueron contestadas en la propuesta de resolución de fecha 26 de enero de 2022.

A) Respecto de las ALEGACIONES DE CARÁCTER GENERAL:

Alude a RADAR COVID como una herramienta adicional y al Real Decreto 463/2020, de 14 de marzo. Aduce que, en ese contexto, la SEDIA, como encargada de tratamiento, actuó conforme a las indicaciones dadas en todo momento por el MSND, como autoridad delegada del Gobierno en materia de salud pública y responsable del tratamiento. Razona que, aunque estas indicaciones no se plasmaron conforme exige la normativa, se debió a que el estado de alarma dificultó la formalización de los instrumentos habituales previstos en la legislación para estos supuestos en circunstancias normales. Alude a las reuniones celebradas a las que asistieron representantes del MSND, de la SEDIA y de la empresa adjudicataria del contrato de emergencia, en las que se tomaban las decisiones necesarias para avanzar en el desarrollo del piloto y de la aplicación.

En este sentido, de la práctica de la prueba y en relación con las reuniones celebradas y que constan en los hechos probados, no se ha acreditado la existencia de ninguna indicación “instrucción” por parte del MSND que dé cobertura a las actuaciones desarrolladas por la SEDIA. Tampoco en la carta referenciada de 9 de junio de 2020, dando el visto bueno para el desarrollo de la aplicación móvil. Y respecto de toda la comunicación y contactos que dice haber mantenido con el MSND tampoco aporta prueba alguna, ni tan siquiera un correo electrónico.

En todo caso, estas “indicaciones” a las que alude, no son suficientes para articular la relación entre responsable y encargado del tratamiento, relación que no puede ser considerada como una mera formalidad administrativa o como un intercambio de opiniones, sino como un medio para procurar la defensa y la protección del Derecho Fundamental a la protección de datos de carácter personal, máxime cuando la relación se establece entre los órganos de una misma Administración Pública o entre distintas Administraciones Públicas a quienes corresponde “*promover las condiciones para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas; remover los obstáculos que impidan o dificulten su plenitud y facilitar la participación de todos los ciudadanos en la vida política, económica, cultural y social*”, ar-

tículo 9.2 de la Constitución Española.

En conclusión, no se ha acreditado la existencia de las instrucciones recibidas del responsable del tratamiento, en los términos anteriormente descritos, desconociéndose su contenido, ámbito, asuntos, fechas en las que fueron suministradas, ni cuál ha sido la actuación, respuesta y reporte suministrado por la SEDIA, consecuencia de estas.

En todo caso, aún cuando hubieran acreditado comunicaciones informales entre las partes para suministrar instrucciones, hemos de significar que el artículo 28.1.a) del RGPD impone que las instrucciones que rigen la relación entre responsables y encargados del tratamiento se encuentren documentadas. Y es que, las instrucciones a las que hace mención el RGPD no dejan de ser documentos internos con efectos en la relación entre el responsable y el encargado del tratamiento en el marco de un contrato de encargado del tratamiento; contrato de encargado de tratamiento u otro acto jurídico que no existe en el presente supuesto.

Por consiguiente, no queda acreditado por parte de la SEDIA que actuase siguiendo las instrucciones del MSND.

B) Respecto de las ALEGACIONES ESPECÍFICAS:

B.1 Respecto al tratamiento de datos de carácter personal.

Alude a que, el derecho a la protección de datos no es absoluto e invoca el artículo 3 del Código Civil. Aduce que, la exigencia y aplicación de la normativa de protección de datos en unas circunstancias tan especiales y atípicas, debe ser equilibrada y ponderada y que, la Agencia no puede actuar como si el estado de alarma no hubiese existido.

En este sentido, el derecho fundamental a la protección de datos no se suspende por la mera declaración de un estado de alarma, sino que esta suspensión queda limitada a los supuestos de declaración del estado de excepción o de sitio, según establece el artículo 55.1 de la CE. En el estado de alarma sólo puede condicionarse el ejercicio de los derechos, pero no suspenderlos.

En este supuesto concreto, se declaró el estado de alarma, lo que no supuso, en ningún caso la suspensión de los derechos fundamentales.

Además, la propia normativa de protección de datos personales (RGPD) contiene las salvaguardas y reglas necesarias para permitir legítimamente los tratamientos de datos personales en situaciones, como la que aconteció, en que existía una emergencia sanitaria de alcance general.

También aduce que los datos no eran reales (eran de prueba), que los códigos de contagiados para su introducción en la App eran falsos y que cuando la App se abrió en La Gomera al público, las personas no podían introducir datos reales de estar infectados. En concreto, esta alegación será objeto de análisis en el FD V de esta Resolución.

Invoca la licitud del tratamiento y se remite al Informe de la AEPD 17/2020, de 12 de

marzo, destacando la base relativa a los artículos 6.1.d) y 6.1.e) del RGPD. Efectivamente, el tratamiento de los datos debe basarse en una causa lícita (artículo 6 RGPD) y debe ser transparente para los afectados (artículos 13 y 14 del RGPD). Por tanto, la falta de información o transparencia supone un incumplimiento de los principios de protección de datos. Este aspecto será analizado en el FD IX de esta Resolución.

B.2 Respecto al rol de la SGAD en el tratamiento de datos

1º. La etapa en la que se hace el proyecto piloto.

Alude de nuevo al visto bueno recibido en fecha 9 de junio de 2020 por parte de la Dirección General de Salud Pública (sic) del MSND donde se considera como responsable del tratamiento de los datos del piloto a la autoridad sanitaria de la Comunidad en que se fuera a llevar a cabo. Analizaremos estos hechos en el FD VII de esta Resolución.

Respecto a la siguiente afirmación realizada por la SEDIA: *"Quedando la SEDIA como encargada del tratamiento de los datos y resultados*", nada se dice al respecto en el mandato recibido en fecha 9 de junio de 2020.

Coincide esta Agencia en que ha quedado acreditada la participación de la DGSP, antes DIRECCIÓN GENERAL DE SALUD PÚBLICA, CALIDAD E INNOVACION, en las reuniones semanales del piloto para la conformación de los fines y medios del proyecto. De igual modo, la misma afirmación puede realizarse respecto a la participación de la SEDIA.

Y, aunque los datos relativos a la salud manejados en el piloto fueran datos simulados de infección (datos no reales), se trataron datos personales, cuestión que será desarrollada en el FD V de esta Resolución.

2º.- La etapa en la que se pone en marcha la aplicación en fase de pruebas y posteriormente la aplicación definitiva.

Alude al Acuerdo del Consejo Interterritorial del Sistema Nacional de Salud, de 19 de agosto de 2020, que permitió que las CCAA pudieran asumir temporalmente, hasta la firma de los convenios, la gestión de los códigos de diagnóstico positivo y a la hoja de ruta presentada por el Presidente del Gobierno para hacer frente al ascenso de la "segunda curva epidemiológica", que entre otras medidas citó, el refuerzo de los medios digitales de rastreo, solicitando a los ciudadanos el uso de RADAR COVID. Aduce que, en el Acuerdo, de 9 de octubre de 2020, que faculta a la SGAD para la suscripción de Convenios con Comunidades y Ciudades Autónomas, se especifica lo siguiente: "*en los mencionados Convenios de colaboración, el Ministerio de Sanidad y la Consejería competente en materia de sanidad de la Comunidad o Ciudad Autónoma de que se trate figurarán como responsables del tratamiento de datos de carácter personal y* ***la SGAD como encargado del tratamiento*****.**" Y especifica parte de las atribuciones que según su condición, competen a unos y a otros.

Nada nuevo aporta esta alegación que ya fue objeto de un pormenorizado análisis en la propuesta de resolución (FD VII) y que de nuevo será rebatida en el FD VII de esta Resolución.

No coincide la AEPD con la afirmación realizada por la SEDIA respecto a que haya quedado plenamente acreditado que en todo momento y de acuerdo con los instrumentos jurídicamente vinculantes, la SGAD actuase única y exclusivamente como encargada del tratamiento, pues no es hasta que se celebra el acuerdo de Acuerdo del Consejo Interterritorial del Sistema Nacional de Salud, de 19 de agosto de 2020, cuando, por primera vez, se le reconoce esta condición.

Por añadidura, según el hecho probado vigésimo séptimo, la primera versión de la EIPD, de 12 de agosto de 2020, en cuanto a los roles de "Responsables, corresponsables y encargados del tratamiento" disponía:

> *En este caso el **titular de la aplicación es la Secretaría General de Administración Digital** dependiente del Ministerio de Asuntos Económicos y Transformación Digital, **que también se constituye como Responsable del Tratamiento**.*
>
> *La aplicación ha sido desarrollada a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA).*

Por otra parte, la SEDIA ha facilitado dos enlaces que dirigen a dos documentos del MSND:

> 1. Estrategia de detección precoz, vigilancia y control de covid-19.
>
> 2. Procedimiento de implementación de la app Radar COVID como complemento a los sistemas manuales de identificación de contactos, coordinado por el Centro de Coordinación de Alertas y Emergencias Sanitarias, Dirección General de Salud Pública, Calidad e Innovación y aprobado por la Ponencia de Alertas y Planes de Preparación y Respuesta.

E insiste en que, en todo momento, tanto en el desarrollo del piloto, como en el uso de RADAR COVID en pruebas por las CCAA, y en su uso, superada dicha fase de pruebas, estaban definidos los roles de responsable y encargado de tratamiento, y remite de nuevo, a la carta de 9 de junio de 2020, al Acuerdo del Consejo Interterritorial y al Acuerdo publicado en el BOE el 15 de octubre.

En relación con este argumento, nos remitimos a lo anteriormente expuesto. La SEDIA no aparece como encargada del tratamiento hasta que se produce el Acuerdo del Consejo Interterritorial. El RGPD enumera los elementos que deben establecerse en el contrato o acto jurídico (artículo 28.3 RGPD). No obstante, el acuerdo del Consejo Interterritorial únicamente disponía: *El encargado del tratamiento será, en ambos casos, la Secretaría de Estado de Digitalización e Inteligencia Artificial*. Es decir, no estipuló, ninguna otra información más específica y concreta sobre cómo se cumplirían los requisitos del acuerdo. Con posterioridad, a partir del Acuerdo publicado en el BOE el 15 de octubre, la que aparecerá como encargada del tratamiento será la SGAD.

En definitiva, la SEDIA, aparece como encargada del tratamiento a partir del Acuerdo del Consejo Interterritorial y ejerce esta condición hasta que se produce la celebración de los correspondientes convenios con las CCAA, en los que asumirá la condición de encargada del tratamiento, la SGAD.

En cuanto a la disconformidad de la SEDIA con alguna de las afirmaciones realizadas por la Agencia respecto a las Notas de Prensa del METD, por cuanto no atribuyen competencia alguna, esta cuestión no es discutida por la Agencia.

El artículo 2.1 de la Ley 50/1997, de 27 de noviembre, del Gobierno dispone: El Presidente dirige la acción del Gobierno y coordina las funciones de los demás miembros del mismo, sin perjuicio de la competencia y responsabilidad directa de los Ministros en su gestión.

Asimismo, el artículo 3.1.d) de la Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado, aplicable a los miembros del Gobierno y los Secretarios de Estado, dispone la observancia del principio de transparencia y responsabilidad en los siguientes términos: adoptarán sus decisiones de forma transparente y serán responsables de las consecuencias derivadas de su adopción.

Por otra parte, la LRJSP, en el artículo 3.1.c) dispone que las Administraciones Públicas deben respetar en su actuación y relaciones una serie de principios, entre ellos, la transparencia de la actuación administrativa.

Asimismo, la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, en el artículo 26 bajo el epígrafe "Principios de buen gobierno", dispone que las personas comprendidas en su ámbito de aplicación (miembros del gobierno, Secretarios de Estado, resto de altos cargos de la AGE, etc.) adecuarán su actividad a los "Principios de actuación", entre ellos, el previsto en el apartado 7º que se refiere al desempeño de sus funciones con transparencia.

En suma, las notas de prensa, más allá de ser consideradas según afirma la SEDIA, como "*simples anuncios que realizó el METD para informar a la ciudadanía y los medios de comunicación, de actividades que estaban proyectadas o en curso de realización*", difundieron información por parte del METD, facilitando el conocimiento por la ciudadanía de la información relativa al rastreo de contactos y las decisiones adoptadas al respecto.

Son por tanto, una prueba más, de la actividad desarrollada por la SEDIA en relación con la aplicación Radar COVID.

En cuanto a que fue el Gobierno el que impulsó la creación de esta aplicación e instó a la población al uso de RADAR COVID, hay que señalar que, el artículo 97 de la Constitución atribuye al Gobierno funciones políticas y ejecutivas, un binomio que tiene su reflejo en toda acción de gobierno y que se proyecta, también, sobre la relación comunicativa que en un sistema democrático existe entre gobernantes y gobernados.

El Gobierno es, indudablemente, sujeto y objeto de información y valoración política; pero, en cuanto responsable último de la Administración General del Estado (en lo sucesivo, AGE) y en razón, precisamente, de la función ejecutiva que constitucionalmente se le encomienda, es emisor de una serie de mensajes dirigidos a los ciudadanos que se engloban bajo la denominación genérica de campañas institucionales de publicidad y de comunicación, según se recoge en la exposición de motivos de la Ley

29/2005, de 29 de diciembre, de Publicidad y Comunicación Institucional.

La SEDIA rechaza la interpretación de la Agencia sobre su papel de cara a la ciudadanía, y alega que, simplemente contribuyó, en colaboración con todo el Gobierno, a aportar soluciones en el ámbito de sus competencias de impulso de la digitalización de las administraciones públicas (y todo ello, sin tener en cuenta la existencia de categorías jurídicas como las de responsable y encargado del tratamiento de protección de datos difícilmente aprehensibles para el común de los destinatarios).

Pues bien, las categorías jurídicas a las que se refiere son conceptos jurídicos determinados en el artículo 4.7) y 4.8) del RGPD y desempeñan un papel crucial en la aplicación del RGPD, puesto que determinan quién responde del cumplimiento de las distintas normas relativas a la protección de datos y cómo pueden los interesados ejercer sus derechos en la práctica.

Respecto a que, por el hecho de colaborar, impulsar y tener un papel relevante en intentar convencer a la población del uso de RADAR COVID y ofrecer explicaciones de las características de la aplicación en los medios de comunicación, no puede llevar a la conclusión de que se esté desarrollando otro papel diferente al asignado en los documentos reiteradamente señalados, nos remitimos a lo dispuesto en las Directrices 07/2020 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» en el RGPD, que en el apartado 25 dice:

> *"En ausencia de responsabilidad por el tratamiento derivada de disposiciones legales, la calificación de una parte como «responsable del tratamiento» debe establecerse sobre la base de una evaluación de las circunstancias de hecho en que tiene lugar el tratamiento. Para alcanzar una conclusión acerca de si un ente concreto ejerce una influencia determinante en relación con el tratamiento de los datos personales en cuestión, deben tenerse en cuenta todas las circunstancias de hecho pertinentes."*

Y las circunstancias de hecho nos remiten al mismo punto de partida. Es decir, al tratamiento de datos personales por parte de la SEDIA durante la ejecución del proyecto piloto, sin contar con un contrato u otro acto jurídico que la vinculase con la Dirección General de Salud Pública, Calidad e Innovación, conforme exige la normativa vigente.

En este sentido, el apartado 102 de las Directrices 07/2020, dice:

> *"Además, el contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros debe vincular al encargado frente al responsable; esto es, debe imponer al encargado obligaciones vinculantes en virtud del Derecho de la Unión o de los Estados miembros. También debe establecer las obligaciones del encargado. En la mayor parte de los casos, existirá un contrato, pero el Reglamento también hace referencia a «otro acto jurídico», como una norma nacional (de Derecho primario o derivado) u otro instrumento jurídico. Si el acto jurídico no incluye todo el contenido mínimo requerido, debe complementarse con un contrato u otro acto jurídico que incluya los elementos que falten."*

B.3 Respecto al rol de INDRA

Alude a que la SEDIA, en su condición de encargado del tratamiento, contó desde el primer momento, con la autorización del MSND, como responsable del tratamiento, para la contratación de INDRA, que, contaba con las garantías suficientes para garantizar la aplicación del RGPD.

Respecto a esta alegación, cabe señalar que en la propuesta de resolución no se imputa la infracción del artículo 28.1 del RGPD.

B.4 Respecto a las Evaluaciones de Impacto

Insiste en que, si bien la EIPD publicada en septiembre 2020 fue la versión 1.1, ya existía una versión 1.0 con anterioridad al 19 de agosto de 2020. La EIPD facilitada a la AEPD fue la versión 1.1 pues es la que se publicó, coincidiendo con el despliegue en septiembre 2020 de una versión de la aplicación, con soporte de lenguas cooficiales.

Aduce que, durante el periodo que va del 19 de agosto hasta la publicación en septiembre 2020, se debatió internamente sobre la conveniencia o no de su publicación. Invoca la personalidad jurídica única de la AGE; añade que, ostenta la condición de responsable y de encargado del tratamiento a través de órganos distintos y no viene publicando ni la EIPD, ni los Análisis de Riesgos sobre las que se basan, de los sistemas que desarrolla.

Razona que la SGAD recabó criterio al delegado de protección de datos del METD. Su criterio fue que, con carácter general, no debían publicarse estos documentos.

En todo caso, finalmente publicó la EIPD y el Análisis de Riesgos en septiembre de 2020.

Por otra parte, cuestiona el criterio de la AEPD, página 189 de la propuesta de resolución, que califica de “más reprochable” la falta de realización de la EIPD en el momento oportuno e insiste en que en ese momento, durante el proyecto piloto, se utilizaron datos simulados, y aunque se hizo en un momento posterior a la puesta en funcionamiento del piloto, se hizo con anterioridad al momento en que la aplicación iba a manejar datos de salud de los usuarios.

En este sentido, la EIPD es una herramienta de carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas.

De hecho, otra de las circunstancias que identifican a la SEDIA como responsable del tratamiento, es que, a través de la SGAD, fue el órgano del METD, encargado de celebrar el “Acuerdo de contratación” que tuvo por objeto la contratación de los servicios de diseño, desarrollo, piloto y evaluación de un sistema que permita la trazabilidad de contactos en relación a la pandemia ocasionada por la COVID-1, aspecto que desarrollamos en el FD VIII. Confirma este hecho, el “Pliego de condiciones para el diseño, desarrollo, piloto y evaluación de un sistema que permita el rastreo de contactos en relación con la pandemia ocasionada por la COVID-19” de fecha 10 y 12 de junio de

2020, que exige/encarga una serie de entregables, entre ellos, la EIPD.

B.5 Respecto a las condiciones de uso y política de privacidad

Alude a que, la primera versión de la App (piloto) sirvió a efectos de comprobar aspectos como la usabilidad, percepción de privacidad, y eficacia de la solución en un entorno simulado.

También incluía un aviso sobre la participación voluntaria en una experiencia piloto con datos ficticios de alerta de contagios de la COVID-19 en la isla de La Gomera.

Añade que los documentos se han ido revisando y actualizando con el ánimo de mejorar su contenido y facilitar su lectura y comprensión, haciendo uso de su facultad de responsabilidad proactiva.

Y que con cada actualización del aplicativo se solicitaba de nuevo el consentimiento expreso de los usuarios.

Respecto a los responsables del tratamiento se remite a la Política de Privacidad actual (https://radarcovid.gob.es/politica-de-privacidad) que establece como responsables del tratamiento al MSND y CCAA, y como encargado del tratamiento a la SGAD.

Justifica el incremento de las 700 palabras con las explicaciones más extensas, así como la ampliación a nuevos usos de la aplicación, o la interoperabilidad con las aplicaciones de rastreo de contactos de la Unión Europea, que ha conllevado su actualización, con el fin de aportar transparencia e información a los usuarios.

Recuerda que, las Condiciones de Uso y Política de Privacidad han estado siempre accesibles para los interesados, tanto desde la aplicación móvil, como desde la web http://radarcovid.gob.es.

Añade que no ha recibido ninguna queja del delegado de protección de datos del MSND y que en el apartado de Preguntas frecuentes del sitio web: https://radarcovid.-gob.es/faq-datos-personales-y-privacidad, se recoge determinada información.

Pues bien, es cierto que recoge la información que aduce, que además, se visibiliza con 16 viñetas, cuando en realidad son 9 los aspectos que informa. El RGPD detalla la información que debe facilitarse al interesado en la fase inicial del tratamiento, en el artículo 13, que contemplan las categorías de la información que ha de suministrarse a los interesados cuando los datos se obtengan de este. Esta información tiene el carácter de básica (artículo 11.1 LOPDGDD) y debe facilitarse en forma concisa, transparente, inteligible y de fácil acceso.

De los hechos probados, se extrae la conclusión de que, la transparencia de la información facilitada a lo largo de las distintas fases de implementación del proyecto piloto y de la aplicación Radar COVID, ha sido confusa, prolija y contradictoria, observada desde las distintas fuentes que emanaba.

De hecho, en febrero de 2022, todavía siguen sin informarse los datos de contacto del delegado de protección de datos (en lo sucesivo, DPD).

Una de las claves para poder garantizar la privacidad es poder demostrarla, verificando que el tratamiento es acorde a la información facilitada. La transparencia de datos

se asienta como pilar para demostrar la diligencia y la responsabilidad proactiva ante la autoridad de control y como medida de confianza ante los sujetos cuyos datos son tratados. Tal y como establece el considerando 39 del RGPD, para la personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados.

Por último, otras de las circunstancias de hecho que identifican a la SEDIA como responsable del tratamiento, es que, se identificó a la SGAD como titular de la aplicación, y fue esta la que definió el contenido de las Condiciones de Uso y la Política de Privacidad de la aplicación. Recordemos que es el responsable del tratamiento el que debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto (considerando 78 RGPD).

B.6 Respecto a las vulnerabilidades detectadas

Razona que se juzgó muy remoto el escenario en el que podía explotarse la vulnerabilidad, con un tercero con capacidad suficiente de espiar las redes de comunicaciones y de cruzar la información remitida por RADAR COVID, que permitieran establecer una relación entre la identidad del usuario y su condición médica de positivo por COVID-19.

Aduce que ese juicio se mostró acertado, pues no se ha detectado ni se tiene constancia de que esta teórica vulnerabilidad haya sido explotada o aprovechada y que no existe ningún sistema informático 100% seguro, y por ello, se optó, una vez ponderadas estas circunstancias, por continuar el desarrollo.

El hecho de que la vulnerabilidad fuera corregida no supone que la infracción no se cometiera.

Cualquier aplicación que vaya a utilizar datos personales debe ser concebida y diseñada desde cero identificando, a priori, los posibles riesgos a los derechos y libertades de los interesados y minimizarlos para que no lleguen a concretarse en daños.

Cabe traer a colación, de nuevo, a los “Antecedentes” del “Pliego de condiciones para el diseño, desarrollo, piloto y evaluación de un sistema que permita el rastreo de contactos en relación con la pandemia ocasionada por la COVID-19” de fecha 10 y 12 de junio de 2020, que decía lo siguiente:

> “*Siendo de interés general para el Gobierno de la Nación dar respuesta al objetivo común de contribuir a la gestión de la situación de crisis sanitaria ocasionada por el COVID-19, la* ***Secretaría de Estado de Digitalización e Inteligencia Artificial*** *del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría General de Administración Digital (SGAD en adelante),* ***desarrollará un conjunto de actividades para la definición y construcción de un sistema*** *que permita el rastreo de contactos estrechos (de forma segura y anónima para el usuario) y su posterior evaluación a través de un piloto*
>
> *En relación a las tecnologías habilitadoras para el rastreo de contactos, hay que reseñar que Apple y Google, empresas que manejan los sistemas operativos instalados en la práctica totalidad de dispositivos móviles a nivel mundial,*

anunciaron el pasado 10 de abril de 2020 una alianza para crear un sistema interoperable, integrado en los sistemas operativos iOS y Android, para el seguimiento de contactos, que no utiliza geolocalización sino Bluetooth de baja energía (Bluetooth LE o BLE), para identificar dispositivos presentes a una distancia próxima.

El enfoque de Apple/Google está basado en el protocolo DP-3T, que preserva la privacidad mediante el empleo de identificadores efímeros sobre los que no es posible realizar ingeniería inversa para obtener datos personales del propietario del dispositivo. Apple y Google liberaron el kit para desarrolladores (SDK, https://apple.com/covid19/contracttracing) el pasado 20 de mayo, lo que permite a los distintos Estados desarrollar soluciones de rastreo de contactos sobre las nuevas funciones incorporadas en sus sistemas operativos, siempre bajo la tutela de las autoridades sanitarias nacionales.

El Sistema que se desarrollará mediante este contrato hará uso de este SDK, *sobre el que se construirá una aplicación móvil que permita activar el sistema de rastreo de contactos; que en conexión con las autoridades sanitarias pueda recibir un código de confirmación de positivo en COVID-19; y que mediante una plataforma servidora (backend) con la que se comunica la aplicación móvil se pueda alertar a las personas con las que se ha tenido un contacto estrecho en fechas recientes.*

Este hecho apunta una vez más, a que la SEDIA, determinó parte de los medios esenciales del tratamiento al decidir utilizar tecnología Bluetooth siguiendo el modelo descentralizado basado en el protocolo DP-3T.

En este sentido, las Directrices 07/2020 en su apartado 40 indican:

Por lo que respecta a la determinación de los medios, cabe distinguir entre los medios esenciales y los no esenciales. ***Los medios esenciales se reservan tradicionalmente y de forma inherente al responsable del tratamiento****. Estos deben ser determinados obligatoriamente por el responsable del tratamiento aunque la determinación de los medios no esenciales también puede dejarse en manos de él. Los medios esenciales son medios estrechamente ligados al fin y el alcance del tratamiento, como el tipo de datos personales tratados («¿qué datos se tratarán?»), la duración del tratamiento («¿cuánto tiempo se tratarán?»), las categorías de destinatarios («¿quién tendrá acceso a los datos?») y las categorías de interesados («¿a quién pertenecen los datos personales tratados?»). Además de estar relacionados con el fin del tratamiento, los medios esenciales se encuentran estrechamente vinculados a la cuestión de si el tratamiento es lícito, necesario y proporcionado.*

III. CONCLUSIÓN DEL ESCRITO DE ALEGACIONES

Alude la SEDIA a que es consciente que puede haber discrepancias en los criterios sobre las actuaciones en las que se ha concretado el trabajo de puesta en marcha de una aplicación necesaria en el contexto de pandemia, con un estado de emergencia declarado. Añade que siempre ha actuado con responsabilidad proactiva colaborando con la AEPD en todo lo solicitado.

De hecho, alega que solicitó informe a la AEPD en el momento en que estaba prevista la extensión de la aplicación a las CCAA en agosto de 2020, momento en el que habría sido muy valiosa la aportación de la AEPD, pero el inicio de las actuaciones previas, determinó, a juicio de la AEPD, la imposibilidad de contar con este informe.

Insiste en que la situación de emergencia y la declaración el estado de alarma alteró el orden jurídico ordinario y el modo de actuar habitual de la Administración.

La situación excepcional determinó una modulación en los procedimientos de la administración y exigió actuar con celeridad para así poder llegar a tiempo y que la aplicación cumpliera con sus fines.

Se hicieron las evaluaciones pertinentes, los análisis que permitió la premura con que hubo de desarrollarse la aplicación y se actuó siempre con la finalidad última de ejercer una responsabilidad proactiva para permitir un adecuado respeto a la protección de datos de carácter personal.

En definitiva, conforme a las argumentaciones y razonamientos anteriores, la SEDIA considera que no ha lugar a sanción de apercibimiento, porque no ha existido un incumplimiento flagrante, consciente y deliberado de la normativa de protección de datos y de todos los artículos que se citan en la propuesta de resolución del expediente sancionador.

Respecto a las conclusiones alcanzadas por la SEDIA cabe señalar lo siguiente:

La normativa de protección de datos personales, en tanto que dirigida a salvaguardar un derecho fundamental, se aplicó en su integridad durante el estado de alarma declarado, dado que no produjo la suspensión de derecho fundamental alguno, siendo la postura adoptada por esta Agencia de estrecha colaboración con todas las autoridades públicas que han solicitado su asesoramiento previo durante la pandemia, singularmente con el Ministerio de Sanidad, habiendo ofrecido la AEPD su colaboración en distintas ocasiones a la SEDIA, vía email, en fechas 7 y 8 de mayo de 2020, interesándose por el grupo de trabajo en el que participaba la SEDIA para coordinar con las CCAA el despliegue de la aplicación.

Tanto es así, que con fecha 7 de abril de 2020, la AEPD informó a petición de la Directora del Gabinete de la SEDIA, sobre el Convenio tipo con las Comunidades Autónomas para el desarrollo de la aplicación “APP” coronavirus. Sobre dicho Convenio también se emitió el informe 030/2020, de fecha 6 de abril de 2020. Todos estos informes se solicitaron con carácter previo al desarrollo de las aplicaciones, sin que existiesen actuaciones previas iniciadas por esta Agencia.

Por otro lado, la SEDIA alega que solicitó informe a la AEPD en el momento en que estaba prevista la extensión de la aplicación a las CCAA en agosto de 2020, momento en el que habría sido muy valiosa la aportación de la AEPD, pero el inicio de las actuaciones previas, determinó, a juicio de la AEPD, la imposibilidad de contar con este informe. Como bien sabe la SEDIA, sí que se le suministraron observaciones al borrador de “Convenio entre la Secretaría de Estado de Digitalización e Inteligencia Artificial y la Consejería de Sanidad de la Comunidad Autónoma de….sobre la adhesión al uso de la aplicación RADAR COVID19”, tal y como ella admite en el escrito de 1 de sep-

tiembre de 2020 en el que contestan a un requerimiento de información de 18 de agosto de 2020 (notificado el día 29 del mismo mes y año). No obstante, debe matizarse que dichas observaciones realizadas por el Gabinete Jurídico, no se refieren al objeto de este procedimiento sancionador, sino que están relacionadas únicamente con el borrador del convenio precitado.

Finalmente, en cuanto a la alegada situación de emergencia, por razón del principio de legalidad, de acuerdo con el artículo 9 de la Constitución Española, los ciudadanos y los poderes públicos están sujetos a la Constitución y al resto del ordenamiento, sin que existiera, como se ha indicado, una suspensión del derecho fundamental a la protección de datos personales, tal y como tempranamente indicó esta Agencia en su informe 17/2020.

IV. CONSIDERACIONES COMPLEMENTARIAS

En cuanto a la solicitud de la práctica de la prueba consistente en la puesta a disposición de la SGAD de la siguiente documentación que se considera fundamental para el ejercicio de la defensa en el procedimiento sancionador:

> a) Propuesta de resolución del Instructor/a en relación con el procedimiento abierto contra el MSND, a fin de apreciar el criterio de la AEPD en relación con la actividad desarrollada por dicho departamento que aunque goza de la misma personalidad jurídica que la SEDIA, es tratada por la AEPD como un ente distinto.
>
> b) Informes íntegros del Gabinete Jurídico de la AEPD citados que se citan en el Fundamento de Derecho Noveno (17/2020 y 32/2020) de la Propuesta de Resolución, para poder apreciarlo en su conjunto y aceptarlo o rebatirlo según sea su criterio.

Debe desestimarse la solicitud de práctica de prueba realizada por la SEDIA en su escrito de alegaciones -también solicitada en oficio a parte-, y ello en la medida que, la SEDIA, no formuló proposición de prueba alguna en el momento procedimental pertinente, a saber, su escrito de alegaciones presentado en fecha 22 de noviembre de 2021.

Es preciso subrayar, que en el curso del procedimiento, la SEDIA ya se benefició de un período extraordinario de prueba por un plazo de diez días adicionales a los 30 inicialmente concedidos. Es decir, la práctica de prueba abarcó el periodo máximo permitido por la LPACAP (artículo 77.2).

Por otra parte, aunque la SEDIA y el MSND actúen para el cumplimiento de sus fines bajo el paraguas de la personalidad jurídica única de la AGE, ésta se organiza en Presidencia del Gobierno y en Ministerios, comprendiendo a cada uno de ellos uno o varios sectores funcionalmente homogéneos de actividad administrativa (artículo 57.1 LRJSP).

A su vez, cada Departamento Ministerial dispone de una estructura de órganos superiores y directivos prevista en el Real Decreto 139/2020, de 28 de enero, que asumen un determinado haz de competencias que será analizado en el FD VII.

La Sentencia del Tribunal Supremo (STS) 5298/1994, de 9 de julio de 1994, indica:

> *"…la potestad sancionadora de la Administración goza de la misma naturaleza que la potestad penal, por lo que en consecuencia, las directrices estructurales del ilícito administrativo tienden también, como en el ilícito penal, a conseguir la individualización de la responsabilidad, vedando cualquier intento de construir una responsabilidad objetiva o basada en la simple relación con una cosa, por consiguiente en el ámbito de la* ***responsabilidad administrativa*** *no basta con que la conducta sea antijurídica y típica, sino que también es necesario que sea culpable, esto es, consecuencia de una acción u omisión* ***imputable a su autor*** *por malicia o imprudencia, negligencia o ignorancia inexcusable (STC, Sala del artículo 61 de la Ley Orgánica del Poder Judicial, de 6 de noviembre de 1990)"*

Por esta razón, aún actuando la SEDIA con personalidad jurídica única, según el principio de responsabilidad previsto en el artículo 28 de la LRJSP:

> "Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa."

No obstante, el modo de atribución de responsabilidad a las personas jurídicas no se corresponde con las formas de culpabilidad dolosas o imprudentes que son imputables a la conducta humana. De modo que en el caso de infracciones cometidas por personas jurídicas, aunque haya de concurrir el elemento de la culpabilidad, éste se aplica necesariamente de forma distinta a como se hace respecto de las personas físicas.

Según la STC 246/1991 " (...) esta construcción distinta de la imputabilidad de la autoría de la infracción a la persona jurídica nace de la propia naturaleza de ficción jurídica a la que responden estos sujetos. Falta en ellos el elemento volitivo en sentido estricto, pero no la capacidad de infringir las normas a las que están sometidos.

Capacidad de infracción y, por ende, reprochabilidad directa que deriva del bien jurídico protegido por la norma que se infringe y la necesidad de que dicha protección sea realmente eficaz y por el riesgo que, en consecuencia, debe asumir la persona jurídica que está sujeta al cumplimiento de dicha norma" (en este sentido STS de 24 de noviembre de 2011, Rec 258/2009).

A lo expuesto debe añadirse, siguiendo la sentencia de 23 de enero de 1998, parcialmente trascrita en las SSTS de 9 de octubre de 2009, Rec 5285/2005, y de 23 de octubre de 2010, Rec 1067/2006, que "aunque la culpabilidad de la conducta debe también ser objeto de prueba, debe considerarse en orden a la asunción de la correspondiente carga, que ordinariamente los elementos volitivos y cognoscitivos necesarios para apreciar aquélla forman parte de la conducta típica probada, y que su exclusión requiere que se acredite la ausencia de tales elementos, o en su vertiente normativa, que se ha empleado la diligencia que era exigible por quien aduce su inexistencia; no basta, en suma, para la exculpación frente a un comportamiento típicamente antijurídico la invocación de la ausencia de culpa".

Respecto a los informes íntegros del Gabinete Jurídico que solicita, el informe 032/2020 fue enviado a la SEDIA el martes, 7 de abril de 2020 a las 22:56 vía correo

electrónico e iba dirigido a:

A.A.B. <EMAIL.1>;***

Z.Z.Z. <EMAIL.2>***

Con relación al informe 17/2020, está disponible en la página web de la AEPD: https://www.aepd.es/es/documento/2020-0017.pdf.

Por las consideraciones expuestas se desestiman las alegaciones aducidas.

V

Radar COVID es una aplicación para dispositivos móviles que promueve la salud pública mediante un sistema de alerta de contagios por la COVID-19.

La Decisión de Ejecución (UE) 2020/1023 de la Comisión de 15 de julio de 2020, que modifica la Decisión de Ejecución (UE) 2019/1765, en lo concerniente al intercambio transfronterizo de datos entre las aplicaciones móviles nacionales de rastreo de contactos y advertencia para combatir la pandemia de COVID-19, define en el artículo 1 los siguientes conceptos:

h) "rastreo de contactos" o "localización de contactos": las medidas aplicadas para seguir el rastro de las personas que han estado expuestas a una fuente de amenaza transfronteriza grave para la salud, en el sentido del artículo 3, letra c), de la Decisión nº 1082/2013/UE del Parlamento Europeo y del Consejo (*);

i) "aplicación móvil nacional de rastreo de contactos y advertencia": una aplicación informática aprobada a nivel nacional que funciona en dispositivos inteligentes, en particular teléfonos inteligentes, está normalmente diseñada para una interacción específica y de amplio alcance con recursos web y trata datos de proximidad y otra información contextual recogida por muchos de los sensores que se encuentran en los dispositivos inteligentes, con el fin de rastrear los contactos con personas infectadas por el SARS-CoV-2 y de advertir a las personas que pueden haber estado expuestas al SARS-CoV-2; estas aplicaciones móviles pueden detectar la presencia de otros dispositivos que utilizan Bluetooth e intercambiar información con servidores finales (backend) a través de internet;

k) "clave": el identificador efímero único relacionado con un usuario de la aplicación que informa de que está infectado por el SARS-CoV-2, o de que puede haber estado expuesto al SARS-CoV-2;

Asimismo, el artículo 4 del RGPD recoge las siguientes definiciones:

> *1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;*

2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".

5) «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

15) «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

Así las cosas, considerando las definiciones expuestas, se ha constatado que, la aplicación Radar COVID, puesta en funcionamiento en distintas fases, ha realizado tratamientos de los datos personales de los usuarios.

Así resulta de los hechos probados, tras confirmarse en la práctica de la prueba, que a la finalización del piloto se habían conseguido más de 58.000 descargas totales, en concreto 58.652 según se indica en el documento "Seguimiento 24.07.2020".

Tal y como se reconoce por la SEDIA: "*Si bien en un primer momento se planteó la posibilidad de controlar el acceso a la descarga de la aplicación exclusivamente al público objetivo del piloto, residentes, trabajadores o visitantes de San Sebastián de la Gomera, se decidió finalmente dejarla abierta debido a 3 factores clave:*

• *Complejidad de implementación.*

• *Impacto negativo en la usabilidad por parte de los ciudadanos al tener que introducir códigos de acceso para la descarga.*

• *Incorporar un factor ajeno al propio funcionamiento de la aplicación en el supuesto despliegue nacional."*

Igualmente, se ha constatado que se recopiló información agregada de los usuarios de la aplicación, tanto de las personas que se la descargaban, como de las personas que asumían el papel de casos positivos o recibían notificaciones de alerta de riesgo de contagio.

Según las cifras de población resultantes de la revisión de los padrones municipales referida al 1 de enero de 2020, con efectos desde el 31 de diciembre de 2020, publicada en el Real Decreto 1147/2020, de 15 de diciembre, por el que se declaran oficiales las cifras de población resultantes de la revisión del Padrón municipal referidas al 1 de enero de 2020, la isla de La Gomera, tenía una población de 21.678 vecinos. En concreto, San Sebastián de La Gomera, municipio donde se desarrolla el proyecto piloto, tenía una población de 7.779 habitantes según los datos registrados en el INE. Es decir, el número de descargas totales de la aplicación durante el proyecto piloto rebasó la

cantidad de 58.000 descargas, superando con creces el número de vecinos censados en la isla, lo que supone que la aplicación se descargó por un número de usuarios muy superior al inicialmente previsto, localizados en distintos puntos de la geografía nacional.

En cuanto al concepto de datos personales, hemos de realizar un par de precisiones.

En primer lugar, el concepto de "información" previsto en el artículo 4 del RGPD ha de entenderse extensivamente, tal y como estable la STJUE de 20 de diciembre de 2017, en el asunto C-434/16, Peter Nowak y Data Protection Commissioner, "*evidencia el objetivo del legislador de la Unión de atribuir a este concepto un significado muy amplio, que no se ciñe a los datos confidenciales o relacionados con la intimidad, sino que puede abarcar todo género de información, tanto objetiva como subjetiva, en forma de opiniones o apreciaciones, siempre que sean «sobre» la persona en cuestión".*

Segundo, que está ampliamente asentado un concepto vasto de dato de carácter personal, que incluye la identificación de una persona física de forma directa o indirecta. En este sentido, la STJUE de 19 de octubre de 2016, en el asunto C-582/14, Patrick Breyer y Bundesrepublik Deutschland, dispone de forma clara que *"El uso por el legislador de la Unión del término «indirectamente» muestra que, para calificar una información de dato personal, no es necesario que dicha información permita, por sí sola, identificar al interesado".*

En el ámbito nacional citaremos por todas la SAN de 8 de marzo de 2002 en la que se indica que *"para que exista un dato de carácter personal (en contraposición con dato disociado) no es imprescindible una plena coincidencia entre el dato y una persona concreta, sino que es suficiente con que tal identificación pueda efectuarse sin esfuerzos desproporcionados" y "para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona".*

A tales efectos, hemos de tomar en consideración el Dictamen del Grupo de Trabajo del artículo 29, hoy sustituido por el CEPD, 4/2007 sobre el concepto de datos personales, en el que se afirma que "*se puede considerar «identificada» a una persona física cuando, dentro de un grupo de personas, se la «distingue» de todos los demás miembros del grupo*".

El considerando 26 del RGPD previene una serie de criterios para decretar si una persona física es o no identificable: *"Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos".*

Hay que destacar, que en la primera evaluación de impacto aportada por la SEDIA, fechada en septiembre de 2020, se determinan cuáles son los *datos "generados o a los*

que accede la aplicación", entre los que se recogen datos personales.

Una primera categoría, se identifica con el concepto de "Datos personales" previsto en el artículo 4.1 del RGPD, dentro de la cual incluimos los datos de proximidad, o la dirección IP, que utiliza el dispositivo para conectarse a Internet.

Los datos de proximidad son datos mediante a los que se localiza a un sujeto y son, per se, datos personales. Así se pone de manifiesto en las Directrices del CEPD 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-19.

La dirección IP también es un dato de carácter personal. Esta cuestión se encuentra plenamente resuelta, citando al efecto, y, por todos, los informes 327/2003 o 213/2004 del Gabinete Jurídico de la AEPD en los que se concluye que *"aunque no siempre sea posible para todos los agentes de Internet identificar a un usuario a partir de datos tratados en la Red, desde esta Agencia de Protección de Datos se parte de la idea de que la posibilidad de identificar a un usuario de Internet existe en muchos casos y, por lo tanto, las direcciones IP tanto fijas como dinámicas, con independencia del tipo de acceso, se consideran datos de carácter personal resultando de aplicación la normativa sobre protección de datos".*

La jurisprudencia del Tribunal Supremo también ha sido prolija en el reconocimiento de la IP como dato de carácter personal y no sólo en la jurisdicción contencioso-administrativa, por todas, STS 16/2014, de 30 de enero (rec. 824/2013).

No podemos dejar de citar la Sentencia de la Sala de lo Contencioso Administrativo de la Audiencia Nacional de 1 de septiembre de 2011 (rec. 625/2009) en la que se establece que la dirección IP es un dato de carácter personal, entendiendo que "*El criterio de la identificabilidad es básico para entender que la dirección IP debe ser considerada como dato personal y, por lo tanto, se encuentra sometida a las mismas garantías que resultan de lo previsto para cualquier clase de dato personal en relación a su tratamiento […] Aplicando estos criterios, resulta que debemos concluir que lo que pretende la recurrente en relación a las direcciones IP de los usuarios de las redes P2P entra claramente en el concepto de tratamiento de datos y obligará, por lo tanto, a la aplicación de los criterios y exigencias generales del concepto de tratamiento de datos.*"

Igualmente se contiene esta prescripción en la STJUE de 19 de octubre de 2016, en el asunto C-582/14), Patrick Breyer y Bundesrepublik Deutschland, al aseverarse que la IP es un dato de carácter personal para el proveedor de servicios: *"el artículo 2, letra a), de la Directiva 95/46 debe interpretarse en el sentido de que una dirección IP dinámica registrada por un proveedor de servicios de medios en línea con ocasión de la consulta por una persona de un sitio de Internet que ese proveedor hace accesible al público constituye respecto a dicho proveedor un dato personal, en el sentido de la citada disposición, cuando éste disponga de medios legales que le permitan identificar a la persona interesada gracias a la información adicional de que dispone el proveedor de acceso a Internet de dicha persona".*

Sin olvidarnos que el propio Grupo del Artículo 29 significa que "*El Grupo de trabajo considera las direcciones IP como datos sobre una persona identificable. En ese senti-*

do ha declarado que «los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP, pues registran sistemáticamente en un fichero la fecha, la hora, la duración y la dirección IP dinámica asignada al usuario de Internet. Lo mismo puede decirse de los proveedores de servicios de Internet que mantienen un fichero registro en el servidor HTTP. En estos casos, no cabe duda de que se puede hablar de datos de carácter personal en el sentido de la letra a) del artículo 2 de la Directiva»", Dictamen del Grupo de Trabajo del artículo 29, 4/2007 sobre el concepto de datos personales.

Hay que traer a colación el considerando 26 del RGPD que informa: "*Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. (…)"*

Estas aplicaciones almacenan y tratan datos que, aunque sometidos a procedimientos de encriptación y medidas de salvaguarda, siguen vinculados a personas específicas.

De hecho, sostener que los usuarios no son identificables, cuando la finalidad del tratamiento es precisamente identificarlos, sería una contradicción flagrante.

De modo que, existió tratamiento de datos y aunque los datos referidos no permitían la identificación directa del usuario o de su dispositivo, sí que permitían su identificación indirecta.

Una segunda categoría de dato personal, la identificamos con los "Datos relativos a la salud" prevista en el artículo 4.15 del RGPD. Tal es el caso del código de confirmación de un solo uso de 12 dígitos facilitado por las autoridades sanitarias en caso de prueba positiva por COVID, o el dato mediante el que el usuario es advertido previamente de un contacto de riesgo, así como el día en que el usuario desarrolló síntomas compatibles con COVID-19.

En estos casos, nos encontramos ante una categoría especial de datos personales (artículo 9.1 RGPD) a la que es aplicable el principio de prohibición de tratamiento, salvo que concurra alguna de las circunstancias previstas en su apartado 2. Por tanto, incorporan un peligro innato, y deben someterse a un estándar de protección más elevado.

El considerando 51 dispone, sobre las categorías especiales de datos personales, que "*Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. […] Tales datos personales no deben ser trata-*

dos, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento, habida cuenta de que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del presente Reglamento al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Además de los requisitos específicos de ese tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento. Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales".

Pues bien, como adelantábamos en el acuerdo de inicio y en la propuesta de resolución hubo datos personales implicados en el tratamiento analizado.

Así, en la práctica de prueba la SEDIA determinó lo que denominó "*datos potencialmente personales que trata la aplicación",*

> *"· Generación de códigos para la comunicación de positivos en la aplicación Radar COVID.*
>
> > *o Código de confirmación de positivo. Estos códigos, de 12 cifras, son generados por el servidor Radar COVID mediante algoritmos pseudoaleatorios, y puestos a disposición de las autoridades sanitarias de las comunidades autónomas, para su reparto entre los casos confirmados de COVID-19 en su territorio. Este número no deja de ser la "confirmación" de que efectivamente el usuario ha dado positivo, y no se trata de un usuario malintencionado que desea desencadenar alertas falsas. Estos códigos tienen una vigencia máxima de un mes, a partir del cual son eliminados del servidor y no pueden ser utilizados para la confirmación de positivos. Así mismo, si un usuario introduce un código de confirmación válido, una vez validado en el servidor, también se elimina.*
>
> *· Recepción de la información remitida por los usuarios cuando comunican un positivo. Las claves de exposición diaria hasta un máximo de 14 días. El número exacto de claves comunicadas dependerá de la fecha de inicio de síntomas o fecha de diagnóstico que se informa en la aplicación.*
>
> > *o Dirección IP del usuario. En la medida en que las aplicaciones Radar COVID establecen contacto con el servidor, tanto para la descarga diaria de claves de exposición temporal, como para la comunicación de casos confirmados, el servidor está en disposición de conocer la dirección IP utilizada por el teléfono móvil para establecer dicha comunicación. En todo caso, esta dirección IP se descarta, no almacenándose a ningún efecto.*
> >
> > *o Comunicación de positivo. En el proceso de comunicación de casos confirmados, también se solicita al usuario que indique el día en el que desarrolló síntomas compatibles con COVID-19. Esta información permite filtrar en el servidor de Radar COVID, según el criterio del Ministerio de Sanidad, las claves de exposición temporal que son añadidas a la relación diaria de claves a disposición de las aplicaciones. Típicamente*

se añadirán la de algunos días inmediatamente anteriores al desarrollo de síntomas, y hasta el día en que se reporta el positivo. Esta fecha se descarta después de ser utilizada por el servidor para determinar las claves de exposición temporal que deben ser incorporadas a la lista de difusión.

o Claves de exposición temporal. La aplicación genera estas claves, a razón de una por día, con las que se derivan los identificadores de proximidad rodantes (RPI), que se intercambian entre teléfonos móviles mediante señales Bluetooth de baja energía (BLE). Estas claves de exposición temporal se almacenan durante un máximo de 14 días, siendo eliminadas a continuación.

En el caso de que el usuario confirme un caso positivo por COVID-19 desde su aplicación, las claves de exposición temporal se comunicarán al servidor de Radar COVID para su composición dentro de un listado diario que puede ser descargado por el conjunto de teléfonos con la aplicación Radar COVID activa.

o Identificadores rodantes de proximidad*. A partir de las claves de exposición temporal, el teléfono móvil genera cada 10 minutos aproximadamente un identificador rodante de proximidad, que es intercambiado con otros teléfonos móviles vía señales BLE. Estos identificadores se almacenan en los teléfonos receptores, y no se comunican a ningún servidor en ningún momento. Servirán para identificar contactos estrechos. Se eliminan al cabo de 14 días.*

· Composición de un listado actualizado de claves de exposición temporal que son puestas a disposición para su descarga por parte de las aplicaciones Radar COVID.

o Listado de claves de exposición temporal. Una vez al día, el servidor Radar COVID compone una lista de claves de exposición temporal, compuesta por todas las claves que han sido comunicadas desde las aplicaciones Radar COVID cuyos usuarios han reportado un caso confirmado de COVID-19. Este listado está a disposición de las aplicaciones Radar COVID, que se conectan diariamente al servidor para descargar dicho listado. Con las claves de exposición descargadas, y cruzándolas con los identificadores rodantes de proximidad almacenados en el teléfono móvil, se puede deducir de acuerdo al protocolo DP3-T si el usuario de este teléfono ha estado a menos de dos metros, durante más de 15 minutos, en los últimos 14 días, con una persona que haya comunicado un caso confirmado por COVID-19. Si es el caso, la aplicación Radar COVID avisará al usuario de esta situación de riesgo, invitándolo a auto confinarse y ponerse en contacto con las autoridades sanitarias. El servidor mantiene listados diarios de claves de exposición temporal por un máximo de 14 días. Los listados con más antigüedad son eliminados del sistema.

Tras ello, la SEDIA aseveró que: "*Como se viene afirmando, los datos recopilados y generados por la aplicación no permiten, por defecto, la identificación directa del usuario o de su dispositivo. Sin embargo, y ateniéndonos al Considerando 30 del Reglamento Europeo de Protección de Datos, los usuarios podrían llegar a ser identificables mediante la asociación a algún identificador en línea facilitado por el dispositivo u otro*

tipo de herramientas o protocolos”.

Asimismo, lo admite la SEDIA abiertamente en la EIPD de agosto de 2020 incluyendo entre los datos personales tratados, entre otros, como los datos de proximidad, la dirección IP: “*La dirección IP que utiliza el dispositivo para conectarse a Internet. En este sentido cabe traer a colación la Sentencia del Tribunal Supremo de 3 de octubre de 2014, en cuyo Fundamento de Derecho número cuatro establece que «no cabe duda que, a partir de la dirección IP puede identificarse directa o indirectamente la identidad del interesado, ya que los proveedores de acceso a internet tienen constancia de los nombres, teléfono y otros datos identificativos de los usuarios a los que han asignado las particulares direcciones IP». La Sentencia confirma que las direcciones IP son datos personales ya que contienen información concerniente a personas identificadas o identificables “.*

Las EIPD de septiembre de 2020 contiene idéntica previsión según consta el informe de actuaciones previas.

No obstante lo anterior, en la EIPD de septiembre de 2020 consta que: “*La aplicación no solicita ningún dato de carácter personal, ni requiere crear usuario (sin login ni datos personales). La aplicación utiliza claves anónimas e intercambia identificadores aleatorios, que están en constante cambio. El personal implicado en la aplicación conoce la tipología de la información y, lo más importante, la Política de Seguridad*”.

Esta afirmación no contradice lo que se deduce de los hechos probados, pues el hecho de que la aplicación no solicitase datos personales que tuvieran que suministrarse por los usuarios, ni se les pidiera su nombre, número de teléfono o correo electrónico para poder crear un registro, no significa que no existiera un tratamiento de otros datos personales.

Que se tratasen datos personales pseudonimizados, tal y como también afirman, implica que hay tratamiento de datos personales.

Asimismo, el hecho de que en el proyecto piloto se trabajase con datos simulados de salud (falsos positivos) tal y como asevera la SEDIA en las alegaciones a la propuesta de resolución, no obsta para que sí se produjera el tratamiento de otros de los datos personales referenciados con anterioridad, máxime cuando los voluntarios se descargaron la aplicación en sus propios dispositivos móviles y desde los mismos reportaron los positivos.

Además, ha existido tratamiento de datos personales. Amén de los datos personales antes referidos y tratados en el proyecto piloto, la misma EIPD de agosto de 2020 concreta al examinar *“todo el ciclo de vida y el flujo de los datos personales a través del tratamiento y todos los actores y elementos que intervienen durante las actividades de tratamiento desde su inicio hasta su fin*” respecto de la fase del ciclo de vida de los datos en que se produce la captura de los mismos que se produce con el “*Acceso a información almacenada en el dispositivo móvil en el momento de la instalación de la App”,* por parte de los usuarios del dispositivo móvil.

Esto significa que con la instalación de la aplicación ya se produce un tratamiento de datos personales.

Hay que destacar, en este momento, que el proyecto piloto no fue cerrado sólo a los voluntarios en el mismo, sino abierto a cualquiera que quisiera descargarse la aplicación.

La propia SEDIA afirma en el trámite de prueba que se producen los siguientes tratamientos, en concreto y tal y como consta en la política de privacidad de la aplicación,

> "*La Secretaría General de Administración Digital, en calidad de titular de la aplicación y en base al encargo del tratamiento encomendado por el Ministerio de Sanidad, efectuará las siguientes operaciones del tratamiento:*
>
> *· Generación de códigos para la comunicación de positivos en la aplicación Radar COVID.*
>
> *· Recepción de la información remitida por los usuarios cuando comunican un positivo. Las claves de exposición diaria hasta un máximo de 14 días. El número exacto de claves comunicadas dependerá de la fecha de inicio de síntomas o fecha de diagnóstico que se informa en la aplicación.*
>
> *· Composición de un listado actualizado de claves de exposición temporal que son puestas a disposición para su descarga por parte de las aplicaciones Radar COVID".*

Determinada, por lo tanto, la existencia de un tratamiento de datos resulta prioritario determinar el papel desempeñado por la SEDIA respecto a la aplicación Radar COVID, especialmente durante el proyecto piloto, que ha conllevado el tratamiento de datos personales. Para ello, examinaremos los conceptos de responsable y encargado del tratamiento, a los efectos de dilucidar, si la SEDIA adecuó su actuación a la posición que conforme al RGPD le correspondía.

VI

El RGPD introduce explícitamente el principio de responsabilidad (artículo 5.2 RGPD), es decir, el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 del artículo 5 y ha de ser capaz de demostrarlo "responsabilidad proactiva".

En este sentido, el artículo 5 del RGPD bajo el epígrafe "Principios relativos al tratamiento" dispone:

> *"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»).”

Asimismo, el artículo 24 del RGPD bajo el epígrafe “Responsabilidad del responsable del tratamiento” dispone:

“1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.
2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos. (…)”

Por su parte, el artículo 25 del RGPD bajo el epígrafe “Protección de datos desde el diseño y por defecto” dispone:

“1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas

apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas. (…)"

Asimismo, la LOPDGDD en el artículo 28.1 señala que:

"Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable."

En consecuencia, debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el RGPD, incluida la eficacia de las medidas (RGPD considerando 74).

En síntesis, este principio exige una actitud consciente, diligente, comprometida y proactiva por parte del responsable frente a todos los tratamientos de datos personales que lleve a cabo.

VII

Continuemos la fundamentación jurídica determinando y diferenciando los conceptos de responsable y encargados del tratamiento.

Respecto al concepto de "Responsable del tratamiento", se encuentra previsto en el artículo 4.7 del RGPD:

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros".

El concepto de "Encargado del tratamiento" se encuentra definido en el apartado 7 del citado artículo:

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

El Informe 0064/2020 del Gabinete Jurídico de la AEPD ha expresado con rotundidad que: "*El RGPD ha supuesto un cambio de paradigma al abordar la regulación del derecho a la protección de datos personales, que pasa a fundamentarse en el principio de «accountability» o «responsabilidad proactiva» tal y como ha señalado reiterada-*

mente la AEPD (Informe 17/2019, entre otros muchos) y se recoge en la Exposición de motivos de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)".

Sigue diciendo el citado informe que: *"…los criterios sobre cómo atribuir los diferentes roles siguen siendo los mismos (apartado 11), reitera que se trata de conceptos funcionales, que tienen por objeto asignar responsabilidades de acuerdo con los roles reales de las partes (apartado 12), lo que implica que en la mayoría de los supuestos deba atenderse a las circunstancias del caso concreto (case by case) atendiendo a sus actividades reales en lugar de la designación formal de un actor como "responsable" o "encargado" (por ejemplo, en un contrato), así como de conceptos autónomos, cuya interpretación debe realizarse al amparo de la normativa europea sobre protección de datos personales (apartado 13), y teniendo en cuenta (apartado 24) que la necesidad de una evaluación fáctica también significa que el papel de un responsable del tratamiento no se deriva de la naturaleza de una entidad que está procesando datos sino de sus actividades concretas en un contexto específico…".*

Los conceptos de responsable y encargado de tratamiento no son formales, sino funcionales y deben atender al caso concreto.

Por ello, debemos fijarnos en la esfera de dirección control u ordenación que el responsable puede ejercer sobre el tratamiento de los datos de carácter personal que obran en su poder en virtud de aquella causa y que estaría enteramente vedado al encargado del tratamiento, tal y como se expresa en el Informe 287/2006 del Gabinete Jurídico de la AEPD, de 20 de junio de 2006.

El responsable del tratamiento lo es desde el momento que decide los fines y los medios del tratamiento, no perdiendo tal condición el hecho de dejar cierto margen de actuación al encargado del tratamiento.

Así se expresa indubitadamente en las Directrices 07/2020: "*El responsable del tratamiento determina los fines y medios del tratamiento; esto es, el porqué y el cómo del tratamiento. Debe decidir tanto sobre los fines como sobre los medios. Sin embargo, algunos aspectos más prácticos del propio tratamiento (los «medios no esenciales») pueden dejarse en manos del encargado del tratamiento. Para ser considerado responsable del tratamiento, no es necesario disponer de un acceso real a los datos que se estén tratando".*

Determinar quién decide los medios y los fines del tratamiento de datos es crucial para establecer quién es responsable del cumplimiento de las normas de protección de datos personales, y en particular quién debería facilitar información a las personas que descargan la aplicación acerca del tratamiento de sus datos personales, cuáles van a ser sus derechos, quién va a ser responsable en caso de violación de la seguridad de los datos personales, etc.

Pues bien, fijados los conceptos de responsable y encargado del tratamiento, así como las obligaciones del primero derivadas de la responsabilidad proactiva, hemos de significar la peculiar situación de las Administraciones Públicas, dónde el responsable del tratamiento es aquel órgano administrativo que tenga atribuidas competencias por una norma jurídica, para cuyo ejercicio sea preciso realizar tratamientos de datos de carácter personal. Si no se ostenta la competencia para realizar una determinada actividad, tampoco se tiene para llevar a cabo los tratamientos que de la misma se de-

rivarían. La competencia determinará, por tanto, la legitimación para realizar el tratamiento. Y todo ello, partiendo de la premisa de que, frente a lo que sucede en el ámbito privado, en el que se puede hacer todo lo que no está prohibido, las Administraciones Públicas solo pueden acometer lo que el ordenamiento jurídico les permite, con sometimiento pleno a la Ley y al Derecho (artículos 9.1 y 103.1 de la Constitución española).

Así se recoge en el artículo 8 de la LRJSP, cuando se dispone que "*la competencia es irrenunciable y se ejercerá por los órganos administrativos que la tengan atribuida como propia, salvo los casos de delegación o avocación, cuando se efectúen en los términos previstos en ésta u otras leyes".*

El apartado segundo del artículo 8.1 de la LRJSP añade que "*La delegación de competencias, las encomiendas de gestión, la delegación de firma y la suplencia no suponen alteración de la titularidad de la competencia, aunque sí de los elementos determinantes de su ejercicio que en cada caso se prevén*", de tal forma que se establecen mecanismos para asignar, en su caso, el ejercicio de las competencias a otros órganos administrativos.

En concreto, y respecto de la delegación de competencias regulada en el artículo 9 del LRJSP deberá publicarse en los boletines o diarios oficiales, procurando la seguridad jurídica que debe garantizarse a los ciudadanos, que deben de conocer, en todo momento, quién es el órgano administrativo titular de una competencia y quién la está ejerciendo en nombre del órgano delegante.

En el marco de una delegación de competencias, el órgano administrativo en quien se residencia la titularidad de esta no pierde su condición de responsable de tratamiento por delegar su ejercicio en otro órgano administrativo. Y no sólo porque las resoluciones administrativas que se adopten por delegación indicarán expresamente esta circunstancia y se considerarán dictadas por el órgano delegante, sino porque mantiene el control sobre el tratamiento de los datos pues puede revocar la delegación en cualquier momento o avocar un asunto cuando concurran circunstancias que lo hagan conveniente.

El órgano competente, que ostenta la titularidad, decide que otro ejerza la competencia (incluyendo en tal ejercicio cierto margen de maniobra al órgano delegado en el tratamiento de los datos) sin perder el control. El órgano delegante, que es el responsable del tratamiento, cuando dispone que otro órgano ejerza las competencias está resolviendo sobre los fines y los medios del tratamiento.

De igual forma, si se produce una encomienda de gestión en los términos del artículo 11 de la LRJSP tampoco supone cesión de la titularidad de la competencia ni de los elementos sustantivos de su ejercicio.

Ostentar la competencia por parte de un órgano administrativo es una cuestión capital, pues su ausencia puede ser determinante de nulidad de pleno derecho o anulabilidad.

Dicho lo anterior, conforme a las alegaciones formuladas por la SEDIA a lo largo del procedimiento sancionador, y para el mejor esclarecimiento de lo acontecido, podemos dividir el tratamiento relativo al establecimiento, desarrollo e implementación de la aplicación Radar COVID en dos periodos temporales.

El primero se produce desde el momento en que se dispone la posibilidad de utilizar una aplicación con la finalidad de determinar la trazabilidad de los contactos, que incluye el proyecto piloto Radar COVID, hasta que se celebra el "Acuerdo de uso de la apli-

cación “Radar COVID”, en fase de pruebas, por parte de las Comunidades Autónomas y Ciudades Autónomas” de 19 de agosto de 2020 del Consejo Interterritorial del Sistema Nacional de Salud. El segundo periodo se inicia con la vigencia del Acuerdo de 19 de agosto de 2020. Según disponía la cláusula 6:

> *6. Este Acuerdo mantendrá su vigencia únicamente durante la fase de pruebas de la utilización de la aplicación “RADAR COVID” y, en todo caso, hasta la firma de los convenios bilaterales de adhesión definitiva pare el uso de la aplicación.*

Pues bien, se diferencia entre ambos periodos porque, como explicaremos a continuación, en el primero la SEDIA detenta la condición de responsable del tratamiento y en el segundo la SEDIA es designada formalmente como encargada del tratamiento, todo ello en relación con la aplicación Radar COVID.

Así, y respecto de este segundo periodo indicaremos que la actuación de la SEDIA como responsable del tratamiento no se dilata en el tiempo, sino que opera un cambio en su condición. En concreto, a partir del “Acuerdo de uso de la aplicación “Radar COVID”, en fase de pruebas, por parte de las Comunidades Autónomas y Ciudades Autónomas” de 19 de agosto de 2020 el Consejo Interterritorial del Sistema Nacional de Salud, conforme a lo recogido en el hecho probado vigésimo octavo, donde se indica que: *El encargado del tratamiento será, en ambos casos, la Secretaría de Estado de Digitalización e Inteligencia Artificial*

También con posterioridad, la Resolución de 13 de octubre de 2020, en la Clausula Tercera, apartado 2 y 3, se reconoce a la SGAD como encargada del tratamiento, respecto de las *“Obligaciones de las partes con relación a la delegación de competencias prevista en la letra b) de la cláusula primera”* conforme al hecho probado trigésimo noveno. Y a la *Secretaría General de Salud Digital, e Innovación del Sistema Nacional de Salud, en su condición de Responsable del tratamiento, dar las indicaciones necesarias a la SGAD en su condición de encargado del tratamiento*.

Recordemos que el artículo 9.1 de la LRJSP, prevé la delegación del ejercicio de las competencias, cuestión distinta a lo que implica ostentar la titularidad de la competencia.

Igualmente, en la Política de Privacidad se producen modificaciones respecto a la versión inicial.

La versión final introduce un “Punto 3” que responde a la cuestión: *¿Quiénes son los responsables del tratamiento de tus datos como usuario de “Radar COVID”?,* e informa lo siguiente:

> *“A nivel nacional, el responsable del tratamiento de tus datos como usuario de “Radar COVID” es: (…)*
>
> *Nombre: Ministerio de Sanidad.*
>
> *Dirección: Paseo del Prado 18-20, 28014 Madrid*
>
> *La Secretaría General de Administración Digital, en calidad de titular de la aplica-*

ción y en base al encargo del tratamiento encomendado por el Ministerio de Sanidad, efectuará las siguientes operaciones del tratamiento:

- *Generación de códigos para la comunicación de positivos en la aplicación Radar COVID.*
- *Recepción de la información remitida por los usuarios cuando comunican un positivo. Esta información incluye:*
- *Las claves de exposición diaria hasta un máximo de 14 días. El número exacto de claves comunicadas dependerá de la fecha de inicio de síntomas o fecha de diagnóstico que se informa en la aplicación.*
- *La preferencia o no por comunicar estas claves de exposición diaria al nodo europeo de interoperabilidad entre aplicaciones de rastreo de contactos.*
- *Composición de un listado actualizado de claves de exposición temporal que son puestas a disposición para su descarga por parte de las aplicaciones Radar COVID.*
- *En relación al nodo europeo de interoperabilidad de contactos (EFGS)*
- *Recepción diaria de los listados de claves de exposición temporal generados por los servidores nacionales de los Estados Miembros adheridos en su caso al proyecto.*
- *Remisión diaria al nodo EFGS de un listado de claves de exposición temporal remitidas por los usuarios de Radar COVID que han consentido explícitamente compartir esta información con el resto de Estados Miembros adheridos al proyecto. (…)"*

Dejando atrás este segundo periodo, nos centraremos ahora en el primero para determinar quién era el responsable del tratamiento respecto del tratamiento de datos personales en relación con la realización del proyecto piloto Radar COVID.

Fijémonos ahora en el ámbito competencial en relación con el tratamiento efectuado para determinar quién es el responsable del tratamiento. A priori, parece que son las autoridades sanitarias nacionales.

Habida cuenta de la sensibilidad de los datos personales y la finalidad del tratamiento de los datos, la Comisión considera que las aplicaciones deberían estar diseñadas de tal manera que las autoridades sanitarias nacionales (o las entidades que realicen una misión que se lleva a cabo en favor del interés público en el ámbito de la salud) sean las responsables del tratamiento (Apartado 3.1 de la Comunicación de la Comisión Europea 2020/C 124 I/01).

Esto también contribuirá a reforzar la confianza de los ciudadanos y, por ende, la aceptación de las aplicaciones (y de los sistemas subyacentes de información sobre cadenas de transmisión de infecciones), además de garantizar que estas cumplan el fin perseguido de protección de la salud pública.

Así, el legislador español se ha dotado de las medidas legales necesarias oportunas para enfrentarse a situaciones de riesgo sanitario, como la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública (modificada mediante

Real Decreto-ley 6/2020, de 10 de marzo, por el que se adoptan determinadas medidas urgentes en el ámbito económico y para la protección de la salud pública, publicado en el Boletín Oficial del Estado de 11 de marzo de 2020) o la Ley 33/2011, de 4 de octubre, General de Salud Pública.

El artículo 3 de la Ley Orgánica 3/1986, señala que:

> *"Con el fin de controlar las enfermedades transmisibles, la autoridad sanitaria, además de realizar las acciones preventivas generales, podrá adoptar las medidas oportunas para el control de los enfermos, de las personas que estén o hayan estado en contacto con los mismos y del medio ambiente inmediato, así como las que se consideren necesarias en caso de riesgo de carácter transmisible."*

Del mismo modo, los artículos 5 y 84 de la Ley 33/2011, de 4 de octubre, General de Salud Pública se refieren a la anterior Ley orgánica 3/1986, y a la posibilidad de adoptar medidas adicionales en caso de riesgo de transmisión de enfermedades. Por lo tanto, en materia de riesgo de transmisión de enfermedades, epidemia, crisis sanitarias etc., la normativa aplicable ha otorgado "a las autoridades sanitarias de las distintas Administraciones públicas" (artículo 1 Ley Orgánica 3/1986, de 14 de abril) las competencias para adoptar las medidas necesarias previstas en dichas leyes cuando así lo exijan razones sanitarias de urgencia o necesidad. En consecuencia, desde un punto de vista de tratamiento de datos personales, la salvaguardia de intereses esenciales en el ámbito de la salud pública corresponde a las distintas autoridades sanitarias de las diferentes administraciones públicas, quienes podrán adoptar las medidas necesarias para salvaguardar dichos intereses esenciales públicos en situaciones de emergencia sanitaria de salud pública (Informe del Gabinete Jurídico AEPD N/REF: 0017/2020).

Aún existiendo alguna duda respecto a las competencias atribuidas al MSND, mediante Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19, en el artículo 4.2.d) se designa al Ministro de Sanidad como autoridad competente delegada en su área de responsabilidad.

Al mismo tiempo, conforme establece el artículo 17.1 del Real Decreto 2/2020, de 12 de enero, por el que se reestructuran los departamentos ministeriales, corresponde al Ministerio de Sanidad "*la propuesta y ejecución de la política del Gobierno en materia de salud, de planificación y asistencia sanitaria, así como el ejercicio de las competencias de la Administración General del Estado para asegurar a los ciudadanos el derecho a la protección de la salud*."

A lo anterior, debemos añadir lo previsto en el Real Decreto 454/2020, de 10 de marzo, por el que se desarrolla la estructura orgánica básica del Ministerio de Sanidad, y se modifica el Real Decreto 139/2020, de 28 de enero, por el que se establece la estructura orgánica básica de los departamentos ministeriales, vigente desde el 12 de marzo de 2020 hasta el 6 de agosto de 2020. Por consiguiente, era la norma vigente en el momento en que se iniciaron las actuaciones del tratamiento.

En su artículo 1 se dispone que *"1. Corresponde al Ministerio de Sanidad, la propuesta y ejecución de la política del Gobierno en materia de salud, de planificación y asistencia sanitaria, así como el ejercicio de las competencias de la Administración General del Estado para asegurar a los ciudadanos el derecho a la protección de la salud*", indi-

cándose a continuación que "*2. Las competencias atribuidas en este real decreto se entenderán en coordinación y sin perjuicio de aquellas que corresponden a otros departamentos ministeriales".*

Planteadas así las cosas, el MSND desarrolla sus funciones a través de diversos órganos directivos, entre los que se encontraba la Dirección General de Salud Pública, Calidad e Innovación (en el momento temporal en que se iniciaron las actuaciones del tratamiento). En el artículo 3 del Real Decreto citado se contienen sus funciones, incluyéndose las relativas a la vigilancia en salud pública o las acciones contempladas en la Ley 33/2011, de 4 de octubre, General de Salud Pública, sean competencia de la administración sanitaria estatal, entre otras.

Por otro lado, el Real Decreto 403/2020, de 25 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Asuntos Económicos y Transformación Digital, dispone en su artículo 1 que el METD se encarga de *"la política de telecomunicaciones y para la transformación digital, en particular impulsando la digitalización de las Administraciones Públicas".*

Dentro de este marco, la SEDIA tiene, conforme al artículo 8, atribuidas las funciones de *"el impulso de la digitalización del sector público y la coordinación y cooperación interministerial y con otras Administraciones Públicas respecto a dichas materias, sin perjuicio de las competencias atribuidas a otros departamentos ministeriales".*

Aplicando lo anterior al caso que nos ocupa y como resultado de las actuaciones desarrolladas por el METD a través de la SEDIA y la SGAD, el papel que le correspondía a la SEDIA conforme al RGPD era el de encargado del tratamiento, ya que la competencia para el tratamiento de datos personales objeto de la aplicación desarrollada la tenía atribuida la actual Dirección General de Salud Pública (Real Decreto 735/2020, de 4 de agosto), antes, Dirección General de Salud Pública, Calidad e Innovación.

Sin embargo, de los hechos probados, se concluye que la SEDIA detentó la condición de responsable del tratamiento desde que se inició el proyecto en el mes de mayo de 2020, hasta el Acuerdo de uso de la aplicación "Radar COVID", en fase de pruebas, por parte de las Comunidades Autónomas y Ciudades Autónomas" de 19 de agosto de 2020 el Consejo Interterritorial del Sistema Nacional de Salud, antes citado, donde ya se reconoce a la SEDIA la condición de encargada del tratamiento.

Dicho lo anterior, y partiendo del hecho de que durante el proyecto piloto el responsable del tratamiento por ser titular de la competencia era la Dirección General de Salud Pública, Calidad e Innovación del Ministerio de Sanidad -admitido por la SEDIA en las alegaciones aducidas en el curso del procedimiento, indicando incluso que era encargada del tratamiento- lo cierto es que, considerando todas las circunstancias de hecho pertinentes y que han sido probadas, la SEDIA detentó la condición de responsable del tratamiento. Esta circunstancia ha quedado probada y deriva de la documentación que consta en el expediente administrativo y de las alegaciones formuladas durante el procedimiento sancionador.

Así, el rol de responsable del tratamiento que detentó la SEDIA, se pone de manifiesto a través de sus propias actuaciones tanto ad intra como ad extra.

Ad intra, respecto del resto de actores implicados en el proyecto piloto pertenecientes a la Administración Pública. La SEDIA determinó gran parte de los fines del tratamien-

to y decidió sobre los medios esenciales para llevarlo a término.

Hemos de partir de la carta de 9 de junio de 2020 de la Dirección General de Salud Pública, Calidad e Innovación. En dicha carta el responsable del tratamiento da el visto bueno al desarrollo del proyecto piloto Radar COVID mediante una aplicación móvil y también determina genéricamente la finalidad del tratamiento de datos personales en el citado proyecto piloto, esto es, la trazabilidad de contactos del COVID-19.

Aclaremos respecto a la alegación formulada por la SEDIA de que queda como encargada del tratamiento de los datos y resultados, que, la carta con relación a los roles se limita al siguiente tenor: "*En su autorización la DGSP establece el 9 de junio de 2020 que: el responsable del tratamiento de los datos de este piloto será la autoridad sanitaria de la Comunidad en que se va a llevar a cabo".*

Esta es una conclusión a la que parece, la SEDIA llega, a la vista de la investigación y posterior apertura del procedimiento sancionador: primero, porque la carta referenciada no hace mención al rol que ha de ocupar la SEDIA, sino que se limita a dar el visto bueno respecto del desarrollo del proyecto piloto; segundo, porque, si como entonces entendía la Dirección General de Salud Pública, Calidad e Innovación, el responsable del tratamiento era la autoridad sanitaria de la Comunidad Autónoma en la que se iba a llevar a cabo el tratamiento, a ella le hubiera correspondido designar al encargado del tratamiento a través de los instrumentos legalmente establecidos y no a la Dirección General de Salud Pública, Calidad e Innovación.

Sin perjuicio de que la Dirección General de Salud Pública, Calidad e Innovación, diera el visto bueno al proyecto piloto Radar COVID mediante la carta de 9 de junio de 2020, lo cierto es que no se determinó formalmente a la SEDIA como encargado del tratamiento durante el proyecto piloto.

Tampoco sirve a tales efectos la mención contenida respecto al "rol" de la SEDIA en el "Pliego de condiciones para el diseño, desarrollo, piloto y evaluación de un sistema que permita el rastreo de contactos en relación con la pandemia ocasionada por la COVID-19" de fecha 10 y 12 de junio de 2020, en la que se limitan a señalar que:

> "*La Orden SND/297/2020, de 27 de marzo, del Ministro de Sanidad encargó a la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA), del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19.*
>
> *En particular, dicha Orden establece en su resolución primera, el Desarrollo de soluciones tecnológicas y aplicaciones móviles para la recopilación de datos con el fin de mejorar la eficiencia operativa de los servicios sanitarios, así como la mejor atención y accesibilidad por parte de los ciudadanos.*
>
> *Adicionalmente, la Dirección General de Salud Pública, Calidad e Innovación, de la Secretaría General de Sanidad (Ministerio de Sanidad) ha dado el Visto Bueno a una prueba piloto de rastreo de contactos en relación a la COVID-19, encargando a la SEDIA el desarrollo de una aplicación móvil para tal fin."*

Interesa hacer un par de puntualizaciones respecto de la Orden Ministerial SND/

297/2020 de 27 de marzo, por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de nuevas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19 (en lo sucesivo, OM).

En concreto el apartado Primero dispone:

> *"Primero. Desarrollo de soluciones tecnológicas y aplicaciones móviles para la recopilación de datos con el fin de mejorar la eficiencia operativa de los servicios sanitarios, así como la mejor atención y accesibilidad por parte de los ciudadanos.*
>
> *1. Encomendar a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo urgente y operación de una aplicación informática para el apoyo en la gestión de la crisis sanitaria ocasionada por el COVID-19. Dicha aplicación permitirá, al menos, realizar al usuario la autoevaluación en base a los síntomas médicos que comunique, acerca de la probabilidad de que esté infectado por el COVID-19, ofrecer información al usuario sobre el COVID-19 y proporcionar al usuario consejos prácticos y recomendaciones de acciones a seguir según la evaluación.*
>
> *La aplicación permitirá la geolocalización del usuario a los solos efectos de verificar que se encuentra en la comunidad autónoma en que declara estar. La aplicación puede incluir dentro de sus contenidos enlaces con portales gestionados por terceros con el objeto de facilitar el acceso a información y servicios disponibles a través de Internet.*
>
> *La aplicación no constituirá, en ningún caso, un servicio de diagnóstico médico, de atención de urgencias o de prescripción de tratamientos farmacológicos. La utilización de la aplicación no sustituirá en ningún caso la consulta con un profesional médico debidamente cualificado.*
>
> *El responsable del tratamiento será el Ministerio de Sanidad y el encargado del tratamiento y titular de la aplicación será la Secretaría General de Administración Digital. El Ministerio de Sanidad, como responsable del tratamiento, autoriza a la Secretaría General de Administración Digital a recurrir a otros encargados en la ejecución de lo previsto en este apartado.*
>
> *2. Encomendar a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de un asistente conversacional/chatbot para ser utilizado vía whatsapp y otras aplicaciones de mensajería instantánea. Proporcionará información oficial ante las preguntas de la ciudadanía. El diseño estará basado en información oficial del Ministerio de Sanidad.*
>
> *El responsable del tratamiento será el Ministerio de Sanidad y el encargado del tratamiento y titular del chatbot será la Secretaría de Estado de Digitalización e Inteligencia Artificial a través de la Subdirección General de Inteligencia Artificial y Tecnologías Habilitadoras Digitales.*

3. Encomendar a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de una web informativa con los recursos tecnológicos disponibles."

Por una parte, el objetivo de la orden no es otorgar base jurídica alguna para el tratamiento de los datos, cuestión que remite a las previsiones del RGPD.

Por otra, esta norma, se cita como legislación aplicable en la Política de Privacidad de manera clara y de forma más soslayada en el Pliego de condiciones, por parte de la SEDIA, como título habilitante para el desarrollo de la aplicación Radar COVID. No obstante, la OM no daba cobertura a esta aplicación, sino solo a los estudios de movilidad realizados durante el estado de alarma, así como a otras de autodiagnóstico que pusieron en funcionamiento el Gobierno y algunas comunidades autónomas al inicio de la pandemia (véase el Convenio entre la SEDIA 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, publicado por Resolución de 30 de abril de 2020). Este tipo de aplicaciones, pretendieron generalizar la geolocalización de usuarios, por lo que encajan mal con el rastreo de contactos. Recordemos que la Comunicación de la Comisión Europea 2020/C 124 I/01, desecha la necesidad de geolocalización a efectos de medir la proximidad y los contactos estrechos (la comunicación entre dispositivos por Bluetooth de baja energía parece ser más precisa y, por tanto, más apropiada que la utilización de los datos de geolocalización (GNSS/GPS o datos de localización de dispositivos móviles)).

El desarrollo del proyecto piloto y su implementación ni tan siquiera estaba incluido en la Orden SND/297/2020, de 27 de marzo, por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19. La App Radar COVID, y por ende su proyecto piloto, no estaba incluida dentro de las soluciones tecnológicas y aplicaciones móviles para la recopilación de datos con el fin de mejorar la eficiencia operativa de los servicios sanitarios.

Si el MSND hubiese querido encomendar a la SEDIA el desarrollo de la aplicación Radar COVID, hubiera mostrado su voluntad inequívocamente. Y lo hubiera realizado de igual forma que el resto de las encomiendas. Sin embargo, la encomienda formal no se produjo.

La SEDIA señala en sus alegaciones que la página 159 de la propuesta de resolución señala lo siguiente: *"La AEPD no entra ni a examinar ni a calificar cuál debe ser el instrumento jurídico a través del cual se encomienda formalmente a la SEDIA el encargo del tratamiento referido al proyecto piloto RADAR COVID. Obviamente, excede de nuestras competencias. Ahora bien, precisamente destacamos la delegación de competencias y la encomienda de gestión de entre los instrumentos previstos en el artículo 8.1 de la LRJSP por ser los idóneos para realizar un encargo de tratamiento entre órganos administrativos."*

Y alude a que el instrumento utilizado, diferente a la encomienda, fue la carta habilitante de Sanidad.

A este respecto, señalar que la voluntad del órgano administrativo competente se manifiesta a través de actos administrativos o normativos, de tal forma que, estos son requeridos para formalizar la encomienda de ser encargado del tratamiento; lo cual se complementa con la obligación prescrita en el artículo 28.3 del RGPD que precisa que "*El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable".*

Así, por ejemplo, se ha puesto de manifiesto tanto en la Orden Ministerial SND/ 297/2020 de 27 de marzo, como en el Acuerdo de 13 de octubre de 2020.

Respecto a quién ha determinado en la práctica los fines y los medios del tratamiento, hemos de significar que, se ha probado que la SEDIA fue nombrada encargada del tratamiento en la reunión del grupo de trabajo interterritorial de fecha 17 de junio de 2020 a la que asistieron representantes de diversas Comunidades Autónomas, así como miembros de la SEDIA, sin presencia alguna de miembros del MSND, donde se expuso que:

> *"…tres principales objetivos de la aplicación: preservar la salud pública, ir un paso por delante de la COVID-19 y minimizar su impacto económico facilitando el movimiento de las personas. Para ello, hay tres momentos clave a tener en cuenta: la activación del Bluetooth (que permite preservar la anonimidad de los usuarios), el reporte de diagnósticos positivos y la notificación a usuarios en riesgo de contagios".*

Además, la aplicación serviría a la finalidad de realizar encuestas on line *"para obtener masa crítica".*

A lo anterior debemos añadir el documento denominado "COVID Radar. Secretaría General de Administración Digital. Funcionamiento general. Madrid, Junio 2020" donde la SEDIA informaba sobre los objetivos de la app:

> "*• Preservar la salud pública sin renunciar a la privacidad de los ciudadanos*
>
> *• Ir un paso por delante del Covid-19: alertar a personas en riesgo es contener el virus de forma proactiva*
>
> *• Minimizar el impacto económico del Covid-19, al controlar la pandemia sin medidas drásticas y facilitando el movimiento de personas".*

Así, la SEDIA al explicitar los objetivos de la aplicación, no estaba sino delimitando los fines del tratamiento, amplificando el fijado por la Dirección General de Salud Pública, Calidad e Innovación (la trazabilidad de contactos); esta participación en la determinación de las finalidades lleva implícita la condición de responsable del tratamiento.

Pero es que, además, determinó parte de los medios esenciales del tratamiento, decidiendo cuestiones tales como que, respecto de la interoperabilidad transfronteriza, se optase por el Protocolo DP3T descentralizado, que incorpora la API de Apple y Google

o la propuesta de cinco modelos para la integración de la aplicación posterior en los servicios de salud autonómicos.

Igualmente, a través del "Pliego de condiciones para el diseño, desarrollo, piloto y evaluación de un sistema que permita el rastreo de contactos en relación con la pandemia ocasionada por la covid-19", aceptado por INDRA, se desarrollaron los medios del tratamiento previamente fijados. La "celebración" del contrato de emergencia con INDRA, como encargada de tratamiento, sin la consiguiente autorización del responsable real del tratamiento requerida por el artículo 28.2 del RGPD, pone de manifiesto que la SEDIA actuaba como responsable del tratamiento decidiendo sobre los medios del tratamiento.

También hay que citar el documento denominado "Diseño Piloto Covid-19 App. Presentación CCAA 17 junio 2020, elaborado por la SEDIA en el que se definen los parámetros clave del Piloto y los canales de acceso por los participantes.

Hay que añadir que, de toda la documentación obrante en el expediente administrativo no constan instrucciones documentadas del responsable real del tratamiento que justifiquen esta actuación "excesiva" de la SEDIA respecto de su rol de encargado del tratamiento.

Siguiendo con nuestra argumentación resulta muy significativa la versión inicial de la "Política de Privacidad de la Aplicación Radar COVID" publicada el día 7 de agosto de 2020 junto con la versión 1.0 de la app Radar COVID (versión piloto), donde consta la siguiente información:

> "*A tal efecto, utilizamos tus datos para prestarte el servicio de "Radar COVID" y para que puedas hacer uso de sus funcionalidades de acuerdo con sus condiciones de uso. De conformidad con el Reglamento General de Protección de Datos (RGPD) así como cualquier legislación nacional que resulte aplicable,* ***la Secretaría General de Administración Digital tratará todos los datos generados durante el uso de la App para las siguientes finalidades****:*
>
> *Ofrecerte información sobre contactos considerados de riesgo de exposición a la COVID-19.*
>
> *Proporcionarte consejos prácticos y recomendaciones de acciones a seguir según se produzcan situaciones de riesgo de cara a la cuarentena o auto-cuarentena.*
>
> *Este tratamiento se llevará a cabo a través de la funcionalidad de alerta de contagios que permite identificar situaciones de riesgo por haber estado en contacto estrecho con personas usuarias de la aplicación que se encuentran infectadas por la COVID-19. De esta manera se te informará de las medidas que conviene adoptar después".*

En esta información se asume con claridad el rol de responsable del tratamiento por la SGAD.

Asimismo, ad extra, a través de las notas de prensa publicadas por el METD, se pone de manifiesto que la SEDIA, desde un principio, actuó como responsable del trata-

miento.

La primera nota de prensa se publica con fecha 6 de mayo de 2020 (hecho probado sexto) donde se informa que "España trabaja a nivel nacional y europeo para la interoperabilidad de las aplicaciones de prevención de contagios frente al COVID-19", destacando el papel del METD junto a los secretarios de estado (SEDIA, incluida).

Es significativo que esta nota de prensa, de 6 de mayo de 2020, es anterior a la carta de la Dirección General de Salud Pública, Calidad e Innovación de 9 de junio de 2020.

Asimismo, con fecha 23 de junio de 2020, en la Referencia del Consejo de Ministros, se da publicidad al Acuerdo adoptado respecto a la declaración de emergencia para la contratación de los servicios de diseño, desarrollo, piloto y evaluación de un sistema que permita el rastreo de contactos, conforme se recoge en el hecho probado décimo cuarto.

Ese mismo día, el METD publica una nota de prensa que informa la aprobación por parte del Gobierno del desarrollo del piloto para una aplicación móvil de notificación de contactos de riesgo por COVID-19, conforme se recoge en el hecho probado décimo tercero.

Posteriormente, en fecha 3 de agosto de 2020, el METD publica otra nota de prensa informando sobre la superación de la fase de pruebas cumpliendo todos los objetivos marcados. (…) Es lo que ha explicado la secretaria de Estado de Digitalización e Inteligencia Artificial, Carmen Artigas, (…), conforme recoge el hecho probado vigésimo segundo.

También, en fecha 9 de septiembre de 2020, el METD publica otra nota de prensa donde informa que se completa la implantación en trece comunidades autónomas, que abarcan el 70% de la población, y libera su código, conforme recoge el hecho probado trigésimo cuarto.

Por último, en fecha 22 de octubre de 2020, el METD publica una nota de prensa informando sobre el compromiso de las principales operadoras de telefonía de no repercutir el consumo de datos de la app Radar COVID a sus usuarios. (…) Y se refiere a la titular de la SEDIA, que es quien mantiene un encuentro con representantes de las principales operadoras de telefonía con el objetivo de establecer vías de colaboración para la difusión de la aplicación móvil de traceo de contactos Radar COVID (hecho probado cuadragésimo).

Y aunque la SEDIA en las alegaciones a la propuesta de resolución discrepa del valor probatorio que les atribuye la AEPD, cuestión ya analizada en el FD IV, lo cierto es que son un elemento más que ha contribuido aclarar el papel de la SEDIA en el desarrollo de la aplicación.

Asimismo, la SEDIA confirmó a esta Agencia -en respuesta al primer requerimiento-, que: *"(…) es oportuno indicar que la app que permitirá el traceo y notificación de contactos con objeto de impulsar la detección precoz de posibles contagiados por la COVID-19 se encuentra todavía en fase de diseño. En este momento, existen todavía muchas indeterminaciones y decisiones pendientes, que se podrán ir dilucidando a*

medida que progrese el proyecto piloto anunciado por la Vicepresidenta Tercera y que se realizará en la Comunidad Autónoma de las Islas Canarias, de lo que se informará oportunamente a la AEPD."

Destaquemos también el documento "FAQs RADAR COVID", remitido por la SEDIA, en fecha 21 de julio de 2020, que incluye en el punto "A.4" la siguiente cuestión:

> *¿Es el Gobierno quien se encarga de gestionar Radar COVID? Sí. Radar COVID es la aplicación del Gobierno de España y ha sido desarrollada por la Secretaría de Estado de Digitalización e Inteligencia Artificial dependiente de la Vicepresidencia Tercera del Gobierno junto al Ministerio de Sanidad.*

Como apuntábamos antes también se pronuncia respecto a los fines de la App que quedan vinculados a los fines del tratamiento en el siguiente sentido:

> *"La finalidad concreta del aplicativo de rastreo es cumplir con lo siguientes objetivos:*
>
> - *Preservar la salud pública sin renunciar a la privacidad de los ciudadanos.*
> - *Ir un paso por delante de la COVID-19, alertando de forma proactiva a personas en riesgo de estar incubando el virus.*
> - *Minimizar el impacto económico de la COVID-19, al controlar la pandemia sin medidas drásticas y facilitando el movimiento de personas."*

Y que duda cabe, con relación a la determinación de los medios, que es la SEDIA a través de la SGAD, la que ha desarrollado la aplicación de rastreo. Así se pone de manifiesto en la Resolución de 13 de octubre de 2020, de la Subsecretaría, que en su apartado Sexto dice:

> "*Que en aplicación de dichos principios, desde el mes de mayo de 2020, la SGAD ha venido desarrollando, con el conocimiento y la conformidad del Ministerio de Sanidad, una aplicación para la trazabilidad de contactos en relación a la pandemia ocasionada por la COVID-19 denominada «Radar COVID.*
>
> *Durante el mes de julio de 2020, con la conformidad de la Dirección General de Salud Pública, Calidad e Innovación del Ministerio de Sanidad, la SGAD llevó a cabo con éxito el proyecto piloto de la misma, cuyo éxito garantiza la viabilidad de la solución propuesta para el rastreo de contactos estrechos"*

Asimismo, tanto en la Política de Privacidad -en su versión inicial-, como en las Condiciones de Uso -en su versión inicial y final-, la SGAD, se identifica como titular de la aplicación Radar COVID respectivamente.

Es decir, de cara a la ciudadanía existía una verdadera apariencia de que era la responsable del tratamiento, a pesar de que, la SEDIA, en las alegaciones a la propuesta de resolución, insiste en negar esta apariencia, remitiéndose a que fue el Gobierno quién impulsó la creación de la aplicación e instó a su uso.

Por último, descartamos la corresponsabilidad de la Dirección General de Salud Pública, Calidad e Innovación y la SEDIA.

El RGPD define en el artículo 26.1 lo que entiende por "Corresponsables del tratamiento":

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

No parece en este caso, que la Dirección General de Salud Pública, Calidad e Innovación y la SEDIA, hayan determinado conjuntamente los objetivos, los medios del tratamiento o sus responsabilidades respectivas, por lo que quedaría descartada la condición de corresponsables del tratamiento.

Hay que destacar el considerando 79 del RGPD que dice:

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

El "Acuerdo de uso de la aplicación "Radar COVID", en fase de pruebas, por parte de las Comunidades Autónomas y Ciudades Autónomas" de 19 de agosto de 2020 el Consejo Interterritorial del Sistema Nacional de Salud en el punto 5 dice:

"5. En relación con el tratamiento de datos de carácter personal, y en aplicación del régimen previsto 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, durante la vigencia de este Acuerdo, el responsable del tratamiento será el Ministerio de Sanidad y, en su respectivo territorio, cada una de las comunidades y ciudades autónomas que se vayan incorporando durante la fase de pruebas al uso de la aplicación, ostentando plenamente sus competencias en materia sanitaria. El encargado del tratamiento será, en ambos casos, la Secretaría de Estado de Digitalización e Inteligencia Artificial".

Señalar, además, que la Secretaría General de Salud Digital, e Innovación del Sistema Nacional de Salud, en respuesta a un requerimiento de fecha 4 de diciembre de 2020, informa a esta Agencia lo siguiente:

> *"2. El Ministerio de Sanidad ejerce el rol de responsable del tratamiento a través de la Secretaría General de Salud Digital, Innovación e Información del SNS (SGSDII), y la Secretaría General de Administración Digital (en adelante, SGAD),*

dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial (en adelante, SEDIA), del Ministerio de Asuntos Económicos y Transformación Digital, ejerce el rol de encargado del tratamiento.

3. Así es desde la firma del Acuerdo suscrito entre ambos ministerios entre el Ministerio de Asuntos Económicos y Transformación Digital y el Ministerio de Sanidad acerca de la aplicación "RADAR COVID", publicado en el BOE de 15/10/2020, (…):

Sin entrar a analizar la condición de responsable del tratamiento de la Dirección General de Salud Pública, Calidad e Innovación, que resulta evidente, hasta que se produce la firma del Acuerdo, ha quedado probado que la SEDIA detentó la condición de responsable del tratamiento, sin disponer de cobertura legal para ejercer esta condición. En consecuencia, no era el órgano competente para tratar los datos de carácter personal en relación con las finalidades pretendidas, con lo que la falta de competencia ha determinado una ausencia de legitimación para el tratamiento de los datos de carácter personal. Como expresábamos anteriormente, la legitimación para llevar a cabo un tratamiento, en el ámbito de las Administraciones Públicas, está indisolublemente unida a la competencia del órgano administrativo que la ostenta, pues sólo aquel que es el competente puede decidir sobre los medios y fines del tratamiento.

A mayor abundamiento, tampoco se produjo con anterioridad a la Resolución de 13 de octubre de 2020, delegación de competencia alguna o encomienda de gestión que le permitiera el ejercicio de la competencia.

En suma, como conclusión de cuanto antecede, cabe afirmar que la SEDIA adscrita al METD, de la que depende la SGAD, con rango de Subsecretaría, ha ejercido como responsable de los tratamientos de datos referidos en los antecedentes de hecho, toda vez que conforme a la definición del artículo 4.7 del RGPD ha determinado los fines y medios de los tratamientos realizados (amén de la apariencia ante los ciudadanos como responsable del tratamiento).

El ordenamiento jurídico ha previsto la contingencia de que quien sea encargado del tratamiento se comporte como responsable del tratamiento. El artículo 28.10 del RGPD dispone que "*Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento".* La consecuencia se determina igualmente en el artículo 33.2 de la LOPDGDD cuando se indica que se consideran responsables y no encargados los que *"en su propio nombre y sin que consten que actúen por cuenta de otro establezca relaciones con los afectados"*.

Los hechos descritos son constitutivos de la infracción prevista en el artículo 83.4.a) y 83.5.a) del RGPD.

VIII

Es oportuno -en este momento-, traer a colación el régimen jurídico relativo a los encargados del tratamiento:

En primer lugar, nos remitimos al artículo 4.8 del RGPD ya indicado.

En segundo lugar, el considerando 81 dice:

> *"Para garantizar el cumplimiento de las disposiciones del presente Reglamento respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este, al encomendar actividades de tratamiento a un encargado, debe recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento. La adhesión del encargado a un código de conducta aprobado o a un mecanismo de certificación aprobado puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable. El tratamiento por un encargado debe regirse por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros que vincule al encargado con el responsable, que fije el objeto y la duración del tratamiento, la naturaleza y fines del tratamiento, el tipo de datos personales y las categorías de interesados, habida cuenta de las funciones y responsabilidades específicas del encargado en el contexto del tratamiento que ha de llevarse a cabo y del riesgo para los derechos y libertades del interesado. El responsable y el encargado pueden optar por basarse en un contrato individual o en cláusulas contractuales tipo que adopte directamente la Comisión o que primero adopte una autoridad de control de conformidad con el mecanismo de coherencia y posteriormente la Comisión. Una vez finalizado el tratamiento por cuenta del responsable, el encargado debe, a elección de aquel, devolver o suprimir los datos personales, salvo que el Derecho de la Unión o de los Estados miembros aplicable al encargado del tratamiento obligue a conservar los datos."*

En tercer lugar, el artículo 28 del RGPD bajo el epígrafe "Encargado del tratamiento" dispone:

> *"1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.*
>
> *2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.*
>
> *3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:*
>
> *a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a*

un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;

b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza legal;

c) tomará todas las medidas necesarias de conformidad con el artículo 32;

d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;

e) asistirá al responsable, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;

f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;

h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

4. Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obliga-

ciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

5. La adhesión del encargado del tratamiento a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a que se refieren los apartados 1 y 4 del presente artículo.

6. Sin perjuicio de que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato u otro acto jurídico a que se refieren los apartados 3 y 4 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales tipo a que se refieren los apartados 7 y 8 del presente artículo, inclusive cuando formen parte de una certificación concedida al responsable o encargado de conformidad con los artículos 42 y 43.

7. La Comisión podrá fijar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.

8. Una autoridad de control podrá adoptar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el mecanismo de coherencia a que se refiere el artículo 63.

9. El contrato u otro acto jurídico a que se refieren los apartados 3 y 4 constará por escrito, inclusive en formato electrónico.

10. Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento."

En cuarto lugar, el artículo 29 del RGPD bajo la rúbrica "Tratamiento bajo la autoridad del responsable o del encargado del tratamiento" establece:

"El encargado del tratamiento y cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo podrán tratar dichos datos siguiendo instrucciones del responsable, a no ser que estén obligados a ello en virtud del Derecho de la Unión o de los Estados miembros."

Por su parte, el artículo 33 de la LOPDGDD bajo el epígrafe "Encargado del tratamiento" dispone:

"1. El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos siempre que se cumpla lo establecido en el Reglamento (UE) 2016/679, en la presente ley orgánica y en sus normas de desarrollo.

2. Tendrá la consideración de responsable del tratamiento y no la de encargado

quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del Reglamento (UE) 2016/679. Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público. Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades.

3. El responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos personales deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado. No procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al responsable, que garantizará su conservación mientras tal obligación persista.

4. El encargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

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

De este modo, teniendo en cuenta las definiciones de responsable y encargado del tratamiento contenidas tanto en el RGPD, como en la LOPDGDD, reiteramos debe considerarse que el criterio definidor de la condición de responsable del tratamiento viene dado por la potestad de determinar los fines y los medios del tratamiento, en tanto que el encargado debe limitar su actuación a seguir las instrucciones del responsable, reputándosele responsable en caso de que determine fines y medios, esto es, si utiliza para fines propios los datos personales que el responsable le haya comunicado para que lleve a cabo el tratamiento objeto de encargo, sin perjuicio de que pueda incurrir en una infracción del RGPD con dicha actuación.

En consecuencia, la existencia de un encargado del tratamiento vendrá delimitada por la concurrencia de dos características derivadas de la normativa citada. De una parte, la imposibilidad de decisión sobre la finalidad, contenido y uso del tratamiento y, de otra parte, la inexistencia de una relación directa entre los usuarios y el encargado, que deberá en todo caso obrar en nombre y por cuenta del responsable como si la relación fuese entre éste y aquellos.

La esencia de la función de encargado del tratamiento es que los datos personales sean tratados en nombre y por cuenta del responsable del tratamiento.

El encargado del tratamiento solo puede realizar tratamientos sobre las instrucciones documentadas del responsable, a menos que esté obligado a hacerlo por el Derecho de la Unión o de un Estado miembro.

Recordemos que según el real decreto Real Decreto 463/2020, de 14 de marzo, el MSND actúa como autoridad competente delegada en su respectiva área de responsabilidad. En consecuencia, dado que el objetivo o finalidad del tratamiento es la prevención de la pandemia del coronavirus, correspondía y corresponde al Ministerio de Sanidad determinar los fines y los medios que se han de utilizar.

Por el contrario, la SEDIA -desde un principio-, debería haber actuado con la condición de encargada del tratamiento, que es la figura en la que claramente se encuadraba conforme a las previsiones del RGPD, cuestión esta que debería haberse instrumentado conforme a las exigencias del artículo 28.3 del RGPD; sin embargo, siendo encargada del tratamiento ha actuado como responsable del tratamiento, tal y como se infiere de los hechos probados.

Pues bien, centrado el tema y conforme a lo antedicho, otro de los actores que intervienen en el proyecto es la sociedad mercantil INDRA SOLUCIONES TECNOLOGÍAS DE LA INFORMACIÓN, S.L.U (en lo sucesivo, INDRA).

Es la SGAD la que, en fecha 15 de junio de 2020, acuerda la contratación de los servicios para el desarrollo de una aplicación para la trazabilidad de contactos en relación a la pandemia ocasionada por la COVID-19, a INDRA, por un importe de 330.537,52 euros (IVA incluido).

El contrato suscrito al efecto se realiza a través de la tramitación de emergencia, en los términos del artículo 120 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014 (en adelante, LCSP).

Se establece así un régimen excepcional "*cuando la Administración tenga que actuar de manera inmediata a causa de acontecimientos catastróficos, de situaciones que supongan grave peligro o de necesidades que afecten a la defensa nacional*". La finalidad última es ejecutar todo lo necesario "para remediar el acontecimiento producido o satisfacer la necesidad sobrevenida", artículo 120 de la LCSP.

Las graves circunstancias concurrentes en estos supuestos exceptúan la necesidad de tramitar expediente de contratación en los términos del artículo 116 y siguientes de la LCSP, excluyendo incluso la existencia de crédito adecuado y suficiente.

Es por ello, por lo que no contamos con los Pliegos de Cláusulas Administrativas Particulares del citado contrato. La Resolución del Tribunal Administrativo Central de Recursos Contractuales núm. 906/2018, de 5 de octubre, en su fundamento de derecho séptimo, indica que los Pliegos de Cláusulas Administrativas Particulares son el instrumento jurídico que delimitan las condiciones y circunstancias de desenvolvimiento desde su inicio de la contratación administrativa y que constituyen la ley del contrato. Se encuentran regulados en el artículo 120 de la LCSP.

En los mismos se determinan, entre otras cuestiones "*los criterios de solvencia y adjudicación del contrato; las consideraciones sociales, laborales y ambientales que como criterios de solvencia, de adjudicación o como condiciones especiales de ejecución se*

establezcan; los pactos y condiciones definidores de los derechos y obligaciones de las partes del contrato; la previsión de cesión del contrato salvo en los casos en que la misma no sea posible de acuerdo con lo establecido en el segundo párrafo del artículo 214.1; la obligación del adjudicatario de cumplir las condiciones salariales de los trabajadores conforme al Convenio Colectivo sectorial de aplicación; y las demás menciones requeridas por esta Ley y sus normas de desarrollo. En el caso de contratos mixtos, se detallará el régimen jurídico aplicable a sus efectos, cumplimiento y extinción, atendiendo a las normas aplicables a las diferentes prestaciones fusionadas en ellos".

Los Pliegos de Cláusulas Administrativas Particulares contendrán también las prescripciones en materia de protección de datos, pues lo relativo al desenvolvimiento del contrato en relación con el tratamiento de los datos personales que se encomienda al encargado del tratamiento también forma parte del contrato suscrito. Siendo las cláusulas de estos pliegos de carácter jurídico, deberán complementarse con las de carácter técnico del Pliego de prescripciones técnicas particulares (artículo 124 de la LCSP), que fijarán desde un punto de vista técnico, cómo se debe ejecutar materialmente el contrato administrativo.

Fijadas así las cosas, si bien la tramitación de emergencia excluye las formalidades previstas en la LCSP respecto de la tramitación del correspondiente expediente de contratación administrativa, no exceptúa el cumplimiento de la normativa de protección de datos. Donde la ley no distingue no podemos hacerlo nosotros, máxime si de lo que se trata es de la defensa de un Derecho Fundamental. La responsabilidad proactiva no se difumina en estos supuestos, sino que sigue plenamente vigente, de tal forma que el responsable del tratamiento deberá cumplir con las obligaciones impuestas por el RGPD y la LOPDGDD.

En la fecha en que se adopta el acuerdo, junio de 2020, la SEDIA actuaba como responsable del tratamiento, debiendo, por lo tanto, cumplir con las exigencias del principio de responsabilidad proactiva y con el artículo 28.3 RGPD.

Y ello, porque el responsable del tratamiento es quien tiene la obligación de garantizar la aplicación de la normativa de protección de datos y la protección de los derechos de los interesados, así como ser capaz de demostrarlo (artículos 5.2, 24, 28 y 32 del RGPD). El control del cumplimiento de la legalidad se extiende durante todo el tratamiento, desde el principio hasta el final. El responsable del tratamiento debe actuar, en cualquier caso, de forma diligente, consciente, comprometida y activa.

Actuando como responsable debió recoger en el contrato administrativo suscrito, la información exigida en el artículo 28.3 del RGPD (objeto, duración, naturaleza, finalidad del tratamiento, tipo de datos personales y categorías de interesados, obligaciones y derechos del responsable…), lo que no se ha producido en el caso analizado.

Y si hubiera actuado en la condición de encargado del tratamiento -que es la que conforme al RGPD le correspondía pero que no ostentaba-, debería haber requerido al responsable del tratamiento la autorización previa que exige el RGPD por escrito, antes de recurrir a otro encargado (INDRA) para desarrollar el servicio encomendado (artículo 28.2 del RGPD).

A mayor abundamiento, ni en el Acuerdo de contratación ni en el Pliego de condicio-

nes, para el diseño, desarrollo, piloto y evaluación del sistema, se recoge cláusula alguna que atribuya a INDRA la condición de encargada del tratamiento. Tan solo recoge -en general-, una Cláusula de Confidencialidad, otra de Protección de Datos Personales, y otra de Seguridad, todas ellas muy abstractas a las que ya nos hemos referido en el informe de actuaciones previas.

Tampoco incluye una sola referencia al responsable del tratamiento.

Los hechos descritos son constitutivos de la infracción prevista en el artículo 83.4.a) del RGPD.

IX

Remitámonos ahora, a la postura unívoca que hemos mantenido en los Informes del Gabinete Jurídico de la AEPD 17/2020 y 32/2020.

Para la AEPD *"todo tratamiento de datos personales que deba realizarse como consecuencia de la pandemia y de la declaración del Estado de alarma deberá respetar el derecho fundamental a la protección de datos personales, ajustándose a las previsiones del RGPD, el cual permite… establecer reglas específicas respecto del ejercicio de dicho derecho, ajustado al propio RGPD, así como a la doctrina elaborada por el Tribunal Constitucional al interpretar el artículo 18.4 de nuestra Constitución, singularmente en lo relativo al principio de proporcionalidad…"* .

Por tanto, de partida, no existe imposibilidad para armonizar los derechos e intereses de los usuarios, cuya protección exige escasa justificación ante la situación epidemiológica que aconteció.

Es momento ahora, de retrotraernos al FD VI donde hacíamos referencia al artículo 5.1 del RGPD.

El responsable del tratamiento debe notificar a los interesados y al público en general que tratará los datos de manera lícita, leal y transparente y debe ser capaz de demostrar que las operaciones de tratamiento cumplen las disposiciones del RGPD. Continua alegando en la propuesta de resolución que en ningún caso se manejaron datos de salud de los participantes en el piloto. Esta afirmación ha sido objeto de aclaración en el FD V.

Aduce, además, que el equipo de Radar COVID, ha ido revisando y actualizando los documentos con el ánimo de mejorar su contenido y facilitar su lectura y comprensión.

El apartado 1 de las Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679 adoptadas el 29 de noviembre de 2017, indica:

> *1. La transparencia es una obligación global del RGPD que se aplica a tres ámbitos fundamentales:*
>
> *1) el suministro de información a los interesados en relación con el tratamiento equitativo;*

2) cómo los responsables del tratamiento se comunican con los interesados en lo que respecta a sus derechos en virtud del RGPD; y

3) cómo los responsables del tratamiento facilitan que los interesados ejerzan sus derechos.

La transparencia es una obligación del responsable, pero también un derecho de los interesados. La transparencia garantiza que el tratamiento de datos no permanezca oculto para estos y se encuentra intrínsecamente ligada a la lealtad y al nuevo principio de responsabilidad proactiva que exige que las operaciones de tratamiento sean transparentes para que los responsables del tratamiento puedan demostrar el cumplimiento de sus obligaciones.

El considerando 39 del RGPD dice:

"El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento."

De los hechos probados, resulta acreditado que la primera versión de la aplicación prevista para el programa piloto (julio 2020), recogía en dos documentos distintos la información relativa a la privacidad:

Condiciones de uso:
https://radarcovid.covid19.gob.es/terms-of-service/use-conditions.html

Política de privacidad:
https://radarcovid.covid19.gob.es/terms-of-service/privacy-policy.html

Sin embargo, ninguno de ellos definía quién era el responsable o encargado del tratamiento.

En las "Condiciones de uso", únicamente constaba una clausula relativa a la titularidad de la aplicación:

"5. Titular de la aplicación La Secretaría General de Administración Digital (SGAD), dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, es la TITULAR de la aplicación Radar COVID. (…)"

La información puesta a disposición de la ciudadanía no se facilitó de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.

También se solicitó a la SEDIA en la práctica de prueba la copia del registro de las actividades de tratamiento de datos personales efectuadas en el proyecto piloto, a los

efectos de constatar el cumplimiento de llevar el RAT y señaló que:

> *"Como Responsable del Tratamiento, el Ministerio de Sanidad incorporó a su Registro de Actividades de Tratamiento, el siguiente tratamiento, disponible en https://www.mscbs.gob.es/servCiudadanos/proteccionDatos/docs/RAT_MSCBS.-pdf"*

En tal registro de actividades del tratamiento consta como responsable del tratamiento la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud.

En cuanto a la accesibilidad de la aplicación Radar COVID-19, aduce la SEDIA, que las condiciones de uso y política de privacidad han estado siempre accesibles para los interesados, tanto desde la aplicación móvil, como desde la web http://radarcovid.gob.es, sin embargo, en el mes de septiembre, se abrió una actuación por el Defensor del Pueblo contra la SEDIA por la falta de adaptación de la aplicación de rastreo de contagios, que no resultaba accesible, especialmente para personas con problemas visuales. La Secretaria de Estado de Digitalización e Inteligencia Artificial reconoció esta circunstancia por el canal de Twitter.

En este sentido las Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679 adoptadas el 29 de noviembre de 2017 indican en el apartado 16:

> *16. De igual manera, si un responsable del tratamiento es consciente de que sus bienes o servicios son utilizados por otros miembros vulnerables de la sociedad, incluidas las personas con discapacidad o las personas con problemas para acceder a la información, o están dirigidos a ellos, el responsable debe tener en cuenta las vulnerabilidades de tales interesados en su evaluación sobre cómo garantizar que cumple sus obligaciones de transparencia en relación con dichos interesados. Esto guarda relación con la necesidad de que un responsable del tratamiento evalúe el nivel probable de comprensión de su audiencia, tal como se indica en el apartado 9. «Por escrito o por otros medios.»*

Por otra parte, respecto a las diversas revisiones en las "Condiciones de uso" y "Política de privacidad" no olvidemos, que el responsable debe observar los mismos principios cuando comunica tanto las declaraciones de privacidad iniciales como en cualquier cambio sustancial o importante que introduzca posteriormente. Aduce en las alegaciones a la propuesta de resolución que, siguiendo el principio de responsabilidad proactiva, ha ido revisando y actualizando los documentos con el animo de mejorar su contenido y comprensión, lo que no se pone en duda.

Las modificaciones incorporadas son considerables y afectan a diversos aspectos.

En fecha 28 de julio de 2020, la SEDIA aporta un documento revisado de "Condiciones de uso", donde se observa que han eliminado el punto 5, relativo al "Titular de la aplicación", sustituyéndolo por "Propiedad intelectual e industrial".

Continúa sin informar sobre la identidad del responsable del tratamiento ni tampoco sobre los datos del DPD, que ni siquiera se mencionan en la Política de Privacidad.

Remitámonos a las Directrices del CEPD 04/2020, que en su apartado 25 dicen:

> *"Para garantizar la rendición de cuentas, debe definirse con claridad quiénes son los responsables del tratamiento de datos en este tipo de aplicaciones. En opinión del CEPD, podrían serlo las autoridades sanitarias nacionales, aunque cabe prever también otras fórmulas. En todo caso, si el despliegue de aplicaciones de rastreo de contactos implica a diferentes agentes, es importante que sus funciones y responsabilidades estén claramente delimitadas desde el principio y que se expliquen a los usuarios."*

La Política de Privacidad en su versión definitiva informa:

> *"Esta aplicación tiene como responsables de tratamiento tanto al MSND, como a las CCAA. Así mismo, la SGAD ejerce como encargada del tratamiento."*

Con relación a las categorías de datos, la versión inicial recoge una información:

> *"− Las claves de exposición temporal (…)*
>
> *− Un código de confirmación de un solo uso de 12 dígitos (…)*
>
> *− Cuestionario voluntario para la recogida de información sobre la experiencia de uso de la aplicación, comprensión de la misma o percepción sobre la privacidad entre otros."*

Y la versión definitiva:

> *"− Las claves de exposición temporal (…)*
>
> *− Un código de confirmación de un solo uso de 12 dígitos (…)*
>
> *− El consentimiento del usuario, si aplica, para la remisión de claves de exposición temporal al nodo europeo de interoperabilidad de aplicaciones de rastreo de contactos.*
>
> *− El aviso de notificación de exposición, a efectos de recoger una estadística anónima y agregada del volumen de notificaciones que produce el sistema a través del rastreo de contactos. Estos datos permiten estimar cuántos usuarios han sido alertados por la Aplicación, de un riesgo potencial de infección, sin poder rastrear su identidad."*

Las Políticas de Privacidad deben ser concretas y específicas sobre el tratamiento de datos personales que se lleva a cabo.

Lo mismo ocurre con las bases de licitud: no se especifican de forma suficientemente clara en la versión inicial ni en la definitiva:

Versión inicial.

> *"10. ¿Cuál es la legitimación para el tratamiento de tus datos? Los datos generados se tratarán legítimamente con las siguientes bases legales:*
>
> *− El consentimiento del usuario libre, específico, informado e inequívoco del USUARIO, poniendo a su disposición la presente política de privacidad, que debe-*

rá aceptar mediante el marcado de la casilla dispuesta al efecto.

− Razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud (artículo 9.2 i) del RGPD), para el tratamiento de los datos de salud (por ejemplo, el estado de una persona contagiada o información sobre síntomas, etc.).

− Cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1 e) RGPD).

− Fines de archivo de interés público, fines de investigación científica o histórica o fines estadísticos (artículo 9.2 j) RGPD).”

En la versión definitiva elimina la cuestión número 10 y se refiere a las bases de forma genérica. También elimina la base relativa al artículo 9.2.j) e introduce la 9.2.h).

“Toda la información se recogerá con fines estrictamente de interés público en el ámbito de la salud pública, y ante la situación de emergencia sanitaria decretada, a fin de proteger y salvaguardar un interés esencial para la vida de las personas, en los términos descritos en esta política de privacidad, y atendiendo a los artículos 6.1.a), 9.2.a), 6.1.c), 6.1.d), 6.1.e), 9.2.c), 9.2.h) y 9.2.i).

La legislación aplicable se enumera a continuación:

Reglamento (UE) 2016/679, 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).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública.

Ley 33/2011, de 4 de octubre, General de Salud Pública.

Ley 14/1986, de 25 de abril, General de Sanidad.

Real Decreto ley 21/2020, de 9 de junio, de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por el COVID-19.

Acuerdo de 9 de octubre de 2020, entre el METD (SEDIA) y el MSND acerca de la aplicación “Radar COVID”.”

En cuanto a los fines del tratamiento la versión inicial informa:

− Ofrecerte información sobre contactos considerados de riesgo de exposición a la COVID-19.

− Proporcionarte consejos prácticos y recomendaciones de acciones a seguir según se produzcan situaciones de riesgo de cara a la cuarentena o auto cuarentena.

Y la versión definitiva, añade:

− Se utilizarán los datos siempre y sólo de forma anonimizada para fines estadísti-

cos y epidemiológicos.

Recordemos que eliminó la base del artículo 9.2.j) del RGPD.

De hecho, en las alegaciones al acuerdo de inicio manifestó que: *"Finalmente se indica que la aplicación no realiza un registro de usuarios, ni obtiene información del dispositivo móvil. No obstante todo lo anterior, no se descarta que en el futuro se puedan realizar, por los Organismos competentes, análisis de datos agregados sobre volumen de descargas de la aplicación, volumen de usuarios contagiados, u otros indicadores anónimos y agregados, para proyectos de investigación científica, cumpliendo siempre la normativa de protección de datos."*

Por último, respecto a la información relativa a *¿Quién tiene acceso a tus datos?*, la versión inicial informa:

> *"El Titular de la Aplicación podrá dar acceso o transmitir los datos a terceros proveedores de servicios, con los que haya suscrito acuerdos de encargo de tratamiento de datos, y que únicamente accedan a dicha información para prestar un servicio en favor y por cuenta del Responsable."*

Y la versión definitiva, añade:

> *"Los datos gestionados por la aplicación móvil (claves diarias de exposición temporal e identificadores efímeros Bluetooth) se almacenan únicamente en el dispositivo del usuario a los efectos de poder hacer cálculos y avisar al USUARIO sobre su riesgo de exposición a la COVID-19.*
>
> *Solo en el caso de reportar un diagnóstico positivo por COVID-19, las claves de exposición temporal de los últimos 14 días generadas en el dispositivo, y bajo el consentimiento explícito e inequívoco del USUARIO, son subidas al servidor para su difusión al conjunto de USUARIOS de este sistema.*
>
> *Estas claves no guardan relación alguna con la identidad de los dispositivos móviles ni con datos personales de los USUARIOS de la Aplicación.*
>
> *Los avisos de notificación de exposición comunicados solo se utilizan para la generación de datos estadísticos agregados y anónimos."*

En suma, la Política de Privacidad se ha visto modificada en numerosos aspectos hasta tal punto que supone un incremento de casi 700 palabras respecto a la versión inicial que la SEDIA justifica en las nuevas funcionalidades que ofrece (como la conexión de Radar COVID al nodo europeo de interoperabilidad) y que ha conllevado la actualización de las condiciones de uso y política de privacidad, a fin de aportar transparencia e información a las personas usuarias de la aplicación.

El artículo 5.1.a) del RGPD, debe conectarse con las previsiones del artículo 12.1 y 2 del RGPD que define el régimen aplicable a la "Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado":

> *"1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y*

sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.

2. El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22. (…)"

La versión inicial de la Política de Privacidad negaba el ejercicio de los derechos 15 a 22 del RGPD:

"8. ¿Cuáles son tus derechos y cómo puedes controlar tus datos? Dado que la aplicación Radar COVID no almacena datos personales, no son de aplicación los derechos de acceso, rectificación, supresión, limitación, oposición y portabilidad, así como a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos. En todo caso, tenemos obligación de indicarte que te asiste en todo momento el derecho para presentar una reclamación ante Agencia Española de Protección de Datos (www.aepd.es)."

La política de privacidad definitiva reconoce los derechos mencionados, excepto el de portabilidad.

En suma, la SEDIA, actuando como responsable del tratamiento, no tomó las medidas oportunas para facilitar al interesado toda la información en los términos que establecen los artículos 12 y 13 del RGPD.

Esta información, debió proporcionarse de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, y, además, en su caso, visualizable.

Ello es especialmente pertinente en situaciones como la que acontece, en la que la proliferación de agentes y la complejidad tecnológica de la aplicación hacen que sea difícil para la ciudadanía saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como sucede en el caso analizado.

Aún en una coyuntura como la acontecida, se ha de actuar conforme a la normativa de protección datos. El ordenamiento jurídico ya contiene previsiones aplicables al control de epidemias y su propagación, sobre todo en caso de catástrofes naturales o de origen humano (considerando 46, artículos 6.1.e), 6.1.d), 9.2.g) e i) del RGPD).

De hecho, el estado alarma ha puesto de manifiesto el protagonismo y la relevancia del derecho a la protección de datos que alcanza un significado sustancial, máxime cuando están en juego el tratamiento de categorías especiales de datos.

Añadir, además, una referencia al artículo 13 del RGPD que, con relación a la "Información que deberá facilitarse cuando los datos personales se obtengan del interesado" dispone:

"1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento; (…);

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al lugar en que se hayan puesto a disposición.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;

b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

d) el derecho a presentar una reclamación ante una autoridad de control;

(…)

f) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información."

Por su parte, el artículo 11 de la LOPDGDD, bajo la rúbrica "Transparencia e información al afectado" señala:

"1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

2. La información básica a la que se refiere el apartado anterior deberá contener, al menos:
a) La identidad del responsable del tratamiento y de su representante, en su caso.

b) La finalidad del tratamiento.
c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679.

3. Cuando los datos personales no hubieran sido obtenidos del afectado, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE) 2016/679 facilitando a aquel la información básica señalada en el apartado anterior, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información. En estos supuestos, la información básica incluirá también: a) Las categorías de datos objeto de tratamiento. b) Las fuentes de las que procedieran los datos."

Así, el deber informativo vinculado a las garantías propias del derecho a la protección de datos en los términos del artículo 13 del RGPD y 11 de la LOPDGDD, forma parte de las garantías vinculadas al derecho fundamental a la protección de datos de carácter personal, que necesariamente deben respetarse.

Incidir en que inicialmente no se incluyó información respecto al responsable, destinatarios o los derechos de los artículos 15 a 22. Tampoco en la versión definitiva se ha incluido la información relativa al DPD al contrario de lo que afirma la SEDIA, que apunta a la existencia de un enlace al MSND para contactar con el DPD, enlace que no existe.

Los hechos descritos son constitutivos de la infracción prevista en el artículo 83.5 del RGPD, apartados a) y b).

X

Engarcemos este último aspecto con otro de carácter relevante que recoge el RGPD.

Nos referimos al régimen jurídico aplicable a la "Evaluación de impacto relativa a la protección de datos" (en lo sucesivo, EIPD) que es el siguiente:

El considerando 89 del RGPD señala:

> *"(…) Por tanto, estas obligaciones generales de notificación indiscriminada deben eliminarse y sustituirse por procedimientos y mecanismos eficaces que se centren, en su lugar, en los tipos de operaciones de tratamiento que, por su naturaleza, alcance, contexto y fines, entrañen probablemente un alto riesgo para los derechos y libertades de las personas físicas. Estos tipos de operaciones de tratamiento pueden ser, en particular, las que implican el uso de nuevas tecnologías, o son de una nueva clase y el responsable del tratamiento no ha realizado previamente una evaluación de impacto relativa a la protección de datos, o si resultan necesarias visto el tiempo transcurrido desde el tratamiento inicial."*

También el considerando 90 del RGPD dice:

> *"En tales casos, el responsable debe llevar a cabo, antes del tratamiento, una evaluación de impacto relativa a la protección de datos con el fin de valorar la particular gravedad y probabilidad del alto riesgo, teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento y los orígenes del riesgo. Dicha evaluación de impacto debe incluir, en particular, las medidas, garantías y mecanismos previstos para mitigar el riesgo, garantizar la protección de los datos personales y demostrar la conformidad con el presente Reglamento."*

Asimismo, el considerando 91 del RGPD dice:

> *"Lo anterior debe aplicarse, en particular, a las operaciones de tratamiento a gran escala que persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional y que podrían afectar a un gran número de interesados y entrañen probablemente un alto riesgo, por ejemplo, debido a su sensibilidad, cuando, en función del nivel de conocimientos técnicos alcanzado, se haya utilizado una nueva tecnología a gran escala y a otras operaciones de tratamiento que entrañan un alto riesgo para los derechos y libertades de los interesados, en particular cuando estas operaciones hace más difícil para los interesados el ejercicio de sus derechos. (…)"*

El artículo 35 del RGPD señala:

> *"1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.*

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

c) observación sistemática a gran escala de una zona de acceso público.

4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.

5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.

6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

7. La evaluación deberá incluir como mínimo: a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento; b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad; c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento

realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.

11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento."

Asimismo, el apartado 39 de las Directrices 04/2020, del CEPD dice:

"Por último, el CEPD considera que ha de llevarse a cabo una evaluación de impacto relativa a la protección de datos (EIPD) antes de empezar a utilizar una aplicación de este tipo por cuanto se considera que el tratamiento puede entrañar un alto riesgo (datos sanitarios, adopción previa a gran escala, seguimiento sistemático, utilización de una nueva solución tecnológica). El CEPD recomienda encarecidamente la publicación de las EIPD."

La AEPD en cumplimiento del mandato previsto en el artículo 35.4 del RGPD publicó una lista orientativa y no exhaustiva de tipos de tratamiento que requieren una evaluación de impacto relativa a la protección de datos. Se basa en los criterios establecidas por el Grupo de Trabajo del Artículo 29 en la guía WP248 "Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del RGPD", complementando lo dispuesto en las Directrices.

Entre los tratamientos en los que es preciso una EIPD se disponen:

"3. Tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc.

4. Tratamientos que impliquen el uso de categorías especiales de datos a las

que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos.

(…)

7. Tratamientos que impliquen el uso de datos a gran escala. Para determinar si un tratamiento se puede considerar a gran escala se considerarán los criterios establecidos en la guía WP243 "Directrices sobre los delegados de protección de datos (DPD)" del Grupo de Trabajo del Artículo 29.

(…)

10. Tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas. (…)"

El CEPD desarrolla la definición de EIPD en las Directrices WP248 como: "… un proceso concebido para describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos personales evaluándolos y determinando las medidas para abordarlos."

La EIPD se encuentra indisolublemente unida al principio de responsabilidad proactiva, al principio de protección de datos desde el diseño y protección de datos por defecto.

La protección de datos desde el diseño y por defecto se reglamenta en el artículo 25 del RGPD ya mencionado en el FD VI.

El principio de privacidad desde el diseño es una muestra del paso de la reactividad a la proactividad y al enfoque de riesgos que impone el RGPD. Por ello, desde los estadios más iniciales de planificación de un tratamiento debe de ser considerado este principio que implica que el responsable del tratamiento desde el momento en que se diseña un eventual tratamiento de datos personales deberá proteger los datos personales y los derechos de los interesados y no sólo cuando efectivamente se produce el tratamiento. Así se expresa en las Directrices 4/2019 del CEPD relativas al artículo 25 Protección de datos desde el diseño y por defecto.

El principio de privacidad desde el diseño engarza con la EIPD al ser ésta una herramienta para determinar y valorar los riesgos del tratamiento, de tal forma que puedan instrumentalizarse las medidas técnicas y organizativas adecuadas para evitar la materialización de los riesgos detectados. Tal y como establece el Grupo de Trabajo del Artículo 29 en sus Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del RGPD, "*La EIPD debe percibirse como un instrumento de ayuda en la toma de decisiones relativas al tratamiento*".

En cuanto a lo que ahora nos interesa indicaremos que la EIPD es responsabilidad del responsable del tratamiento, aunque se la encargue a un tercero. Temporalmente "*debe iniciarse tan pronto como sea viable en el diseño de la operación de tratamiento incluso aunque algunas de las operaciones de tratamiento no se conozcan aún".* Así se determina en las Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del RGPD.

Además, exige la participación del DPD, pues debe ser requerido por el responsable del tratamiento para la elaboración de la EIPD y controlar su realización, conforme previene el artículo 35.2 y el artículo 39.1.c) del RGPD.

En este sentido, las Directrices sobre los delegados de protección de datos del Grupo de Trabajo del artículo 29, adoptadas el 13 de diciembre de 2016 y revisadas por última vez y adoptadas el 5 de abril de 2017, confieren a esta figura un papel relevante y fundamental al indicar que *"siguiendo el principio de la protección de datos desde el diseño, al artículo 35, apartado 2, establece específicamente que el responsable del tratamiento «recabará el asesoramiento» del DPD cuando realice una evaluación de impacto relativa a la protección de datos. A su vez, el artículo 39, apartado 1, letra c), impone al DPD la obligación de «ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35»".* Es importante destacar la recomendación contenida en las citadas Directrices en relación con las funciones específicas del DPD en relación con la EIPD pues este deberá comprobar "*si la evaluación de impacto relativa a la protección de datos se ha llevado a cabo correctamente o no y si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardias aplicar) son conformes con el RGPD".*

En todo caso, y respecto de la EIPD el Grupo de Trabajo del artículo 29 recomienda que el responsable del tratamiento busque el asesoramiento del DPD en las siguientes cuestiones:

> *" . si debe llevarse a cabo o no una evaluación de impacto relativa a la protección de datos;*
> *. qué metodología debe seguirse al llevar a cabo una evaluación de impacto;*
> *. si debe realizarse la evaluación de impacto en la propia organización o subcontratarse;*
> *. qué salvaguardias (incluidas medidas técnicas y organizativas) deben aplicarse para mitigar cualquier riesgo para los derechos e intereses de los interesados*
> *. si la evaluación de impacto relativa a la protección de datos se ha llevado a cabo correctamente o no y si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardias aplicar) son conformes con el RGPD".*

La falta de EIPD, así como su realización defectuosa, incompleta, tardía o sin la participación del DPD supone una conculcación del principio de responsabilidad proactiva y de la privacidad desde el diseño, así como de las previsiones del RGPD sobre la EIPD.

En el primer requerimiento practicado a la SEDIA se requirió: *Copia del análisis de riesgos sobre los derechos y libertades de los usuarios de la app realizado sobre el*

posible tratamiento de datos y la evaluación de impacto relativa a protección de datos a realizar sobre esta iniciativa.

En contestación a este requerimiento, en fecha 18 de junio de 2020, informa: "*El documento de análisis de riesgos se encuentra en elaboración a medida que avanza el diseño de la solución, no estando todavía disponible".*

La Agencia vuelve a solicitar la evaluación en un segundo requerimiento y no será hasta el 22 de septiembre de 2020, cuando aporta lo que en ese momento nos comunicó que era una primera versión de la evaluación de impacto. La segunda de las versiones se aporta en fecha 30 de octubre de 2020. Y ello porque con ocasión del trámite de prueba se ha aportado por la SEDIA por primera vez, una versión de una EIPD anterior a las citadas, fechada en agosto de 2020.

Destaquemos que el lanzamiento del proyecto piloto en La Gomera se produce desde el 29 de junio de 2020 hasta el 29 de julio de 2020 y a nivel nacional, la puesta en servicio de la App se produce el 19 de agosto de 2020.

Por lo tanto, el tratamiento de los datos se materializó antes de elaborar la EIPD, incumpliendo lo dispuesto en el artículo 35 RGPD.

La SEDIA, que actuaba como responsable del tratamiento, debió haber elaborado una EIPD desde el inicio del desarrollo e implantación de la aplicación Radar COVID y, en todo caso, antes de que se produjera el tratamiento de los datos personales. Sin embargo, tal y como consta en los hechos probados la primera EIPD es de agosto de 2020 y fue elaborada a los efectos de lanzar la aplicación a nivel nacional. Idénticos datos, tratamientos y riesgos están presentes en la fase del proyecto piloto que con posterioridad sin que ningún cambio o evento se produjera salvo la amplificación territorial de la aplicación.

La existencia de una primera EIPD en agosto de 2020 denota también una falta flagrante de privacidad desde el diseño, pues el responsable del tratamiento debe planificar el tratamiento y evaluar los riesgos, antes de que el tratamiento mismo se produzca. Sin embargo, se ha producido un tratamiento de datos personales sin un mínimo y somero análisis que indicara si se estaban tratando datos personales y cuáles eran, en su caso, los eventuales riesgos que afectaban a los derechos y libertades de los ciudadanos, así como la necesidad o no de realizar una EIPD.

A todo esto, tenemos que añadir que, en un inicio la SEDIA manifestó a la AEPD que no se estaban tratando datos personales. Llama poderosamente la atención esta primera alegación ante la AEPD cuando la primera vez que verifica que se trataban datos personales es en la EIPD de agosto de 2020 tal y como consta en los hechos probados.

Es más, preguntada la SEDIA en el trámite de prueba sobre la EIPD del proyecto piloto Radar COVID indica que "*Para el proyecto piloto, dadas sus características de simulación de pandemia, no se generó ningún documento de evaluación de impacto de protección de datos, más allá de ir progresando los sucesivos borradores de lo que a la postre sería la versión 1.0 del documento, disponible el 12 de agosto de 2020".*

Lo cierto es que esta imprevisión inicial, pone de manifiesto que no había EIPD, no obstante se estaba llevando a cabo efectivamente un tratamiento de datos de carácter personal durante el proyecto piloto Radar COVID. A tales efectos hemos de mencionar que para llegar a la afirmación de que no hay tratamiento de datos personales es prescripción obligatoria realizar al menos una evaluación inicial de tal extremo para descartarlo, cuestión que tampoco ha sido acreditada por la SEDIA incluso tras el trámite de prueba.

También cabe destacar, que no consta en la documentación remitida a la AEPD, documento alguno en el que se consigne el asesoramiento y la participación obligatoria del DPD en la EIPD.

En relación con la realización de la EIPD de la fase del proyecto piloto Radar COVID, la SEDIA aseveró en el trámite de prueba que *"El Delegado de Protección de Datos del Ministerio de Asuntos Económicos y Transformación Digital no fue consultado a los efectos de la generación de la primera versión del documento de evaluación de impacto de protección de datos, al no ser un procedimiento de carácter obligatorio*".

Sin embargo, el artículo 35 del RGPD, como adelantábamos, establece en su apartado segundo que *"2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos*".

En idéntico sentido el artículo 39.1.c) del RGPD dispone que el DPD tiene la función, entre otras, de "*ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35".*

Derivado de lo anterior podemos concluir que el RGPD impone al responsable del tratamiento, como parte de sus obligaciones, recabar el asesoramiento del DPD al realizar la EIPD, debiendo, asimismo, el DPD, supervisar la aplicación de la EIPD.

En idéntico sentido, las Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679, adoptadas el 4 de abril de 2017 y revisadas por última vez y adoptadas el 4 de octubre de 2017 establecen que está obligado a realizar una EIPD "*El responsable, junto con el delegado de protección de datos y los encargados del tratamiento*" documentando las opiniones y recomendaciones del DPD.

Si bien puede ser cierto lo señalado por la SEDIA de que no existía un procedimiento de interacción concreto con el DPD en su organización, ello no obsta para que se le solicitase su asesoramiento, no sólo cuando se estimara conveniente por el responsable del tratamiento en atención a las circunstancias, sino obligatoriamente en relación con la realización de la EIPD. Y ello porque además, tal y como prescribe el artículo 38.1 del RGPD *"El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales".*

A mayor abundamiento, y a los meros efectos ilustrativos, las Directrices sobre los de-

legados de protección de datos del Grupo de Trabajo del artículo 29 antes citadas, establecen sobre la EIPD y el DPD que el responsable del tratamiento debe "*Garantizar que se informa y consulta al DPD desde el principio facilitará el cumplimiento del RGPD, fomentará un enfoque de privacidad desde el diseño y, por lo tanto, debería ser un procedimiento estándar en la gobernanza de la organización".*

Sin perjuicio de lo anterior, la SEDIA afirma que "*En todo caso, con posterioridad a la elaboración de la evaluación de impacto, se recabó telefónicamente el criterio de este Delegado de Protección de Datos, sobre la publicación en abierto de esta evaluación de impacto. El criterio facilitado fue que no existía experiencia al respecto de publicación de estos documentos".*

La solicitud de asesoramiento del DPD fue posterior a la elaboración de la EIPD y circunscrito a la consulta sobre la publicación en abierto de la EIPD, en los términos del artículo 39.1.c) del RGPD, no sobre la realización de la evaluación misma, lo que no evita que se haya producido una vulneración de la normativa de protección de datos.

Por último, indicaremos que la realización posterior de la EIPD no "subsana" la falta de realización de esta en el momento oportuno y con la participación de todos los actores necesarios, especialmente porque la falta de evaluación de los riesgos y de adopción de las medidas técnicas y organizativas oportunas, ya ha producido un daño intangible en los derechos y libertades de los ciudadanos, más reprochable cuando el tratamiento lo efectúa una Administración Pública.

Los hechos descritos son constitutivos de la infracción prevista en el artículo 83.4.a) del RGPD.

XI

A continuación, procede una somera referencia al artículo 25.1 del RGPD, ya referido en el FD VI y X.

En un mundo cada vez más digital, la adhesión a la protección de datos por diseño y por defecto desempeña un papel crucial en la promoción de la privacidad y la protección de datos en la sociedad.

Esta Agencia registró varias reclamaciones en las que se denunciaba una vulnerabilidad en el diseño de la aplicación.

Según afirmó la SEDIA, esta vulnerabilidad ya era conocida por el equipo de desarrollo de Radar COVID, ya que figuraba al menos en un documento técnico publicado en abril de 2020 por el equipo DP3T: Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems.

No obstante, el equipo de desarrollo no consideró necesario resolver este problema en las primeras versiones dado que, para explotar esta vulnerabilidad, se debía presuponer un remoto escenario donde el operador de telecomunicaciones estuviera interesado en obtener esta información clínica de sus clientes estudiando el tráfico de datos generado por la App Radar COVID.

La aplicación se puso en servicio a nivel nacional el 19 de agosto de 2020. La vulnera-

bilidad fue corregida en la subida correspondiente al 8 de octubre de 2020, para las siguientes versiones de la aplicación: Android, versión 1.0.9, Apple, versión 1.0.8.

El considerando 78 del RGPD dice:

> *"La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos."*

Asimismo, el considerando 83 del RGPD dice:

> *"A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales."*

La SEDIA tras aseverar en la práctica de prueba que los datos recopilados y generados por la aplicación no permiten, por defecto, la identificación directa del usuario o de su dispositivo, previenen que *"sin embargo, y ateniéndonos al Considerando 30 del Reglamento Europeo de Protección de Datos, los usuarios podrían llegar a ser identificables mediante la asociación a algún identificador en línea facilitado por el dispositivo u otro tipo de herramientas o protocolos"*.

En este momento hemos de recordar el concepto de dato personal previsto en el

RGPD y traer a colación la EIPD elaborada por la SEDIA, en agosto de 2020, realizada en atención a la presencia de datos personales y al tratamiento efectuado sobre los mismos.

Así, tras el reconocimiento de la existencia de datos personales implicados, hace referencia a que *"la aplicación ha sido diseñada respetando, como premisa principal, la normativa de protección de datos vigente y en especial aplicando todas las medidas para reducir los posibles riesgos, aplicando todas las medidas técnicas y organizativas apropiadas concebidas para aplicar de forma efectiva los principios de protección de datos".*

Sin embargo, la primera EIPD que presentan está fechada en agosto de 2020, una vez que ya se había producido el tratamiento de datos personales mediante el proyecto piloto Radar COVID

De hecho, se admite abiertamente en la práctica de prueba que "*Para el proyecto piloto, dadas sus características de simulación de pandemia, no se generó ningún documento de evaluación de impacto de protección de datos, más allá de ir progresando los sucesivos borradores de lo que a la postre sería la versión 1.0 del documento, disponible el 12 de agosto de 2020".*

Sin embargo, hemos de destacar que el único cambio fue la decisión del lanzamiento a nivel nacional de la aplicación, sin que ninguna variación sustancial se produjera entre el proyecto piloto y la implementación de la aplicación definitiva en cuanto al tratamiento de datos personales.

De acuerdo con lo anteriormente expuesto, el diseño de la aplicación no ha tenido presente de forma efectiva los principios aplicables a la protección de datos.

En la aplicación de las medidas de seguridad técnicas y organizativas, el responsable no ha tenido en consideración los riesgos que representaba este tratamiento. Mientras que el tratamiento de la dirección IP era necesario para el funcionamiento de la aplicación, la posibilidad de asociar la IP con la subida de un test positivo no lo era. Este tratamiento de datos contradice lo expuesto en la cuestión 8 de la última versión de la política de privacidad, en la que se recalca que "*estas claves no guardan relación alguna con la identidad de los dispositivos móviles ni con datos personales de los USUARIOS de la Aplicación".*

Y aún siendo conscientes del riesgo, no integraron las garantías necesarias para garantizar la confidencialidad de los datos y resiliencia de los sistemas.

Los hechos descritos son constitutivos de la infracción prevista en el artículo 83.4.a) del RGPD.

XII

La AEPD es consciente de la situación extraordinaria y de emergencia que ha generado la pandemia del COVID conllevando la adopción de múltiples medidas para poner fin a la gravedad de la situación.

Es también evidente, que la privacidad, el derecho a la protección de los datos perso-

nales, no puede ser un obstáculo en los avances tecnológicos para combatir la pandemia. Como recoge el considerando 4 del RGPD: *el tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad.*

No obstante lo anterior, en este contexto, no podemos obviar que la función primordial de la AEPD se refiere a la defensa efectiva del derecho fundamental a la protección de datos de carácter personal de la ciudadanía.

De lo hasta aquí expuesto, debe concluirse que, los hechos probados vulneran lo dispuesto en los artículos: 5.1.a), 5.2, 12, 13, 25, 28.3, 28.10 y 35 del RGPD, con el alcance expresado en los FD anteriores, lo que, supone la comisión de las infracciones tipificadas en el artículo 83 apartados 4.a), 5.a) y 5.b) del RGPD.

Por lo tanto, de acuerdo con la legislación aplicable, la directora de la AEPD
RESUELVE:

PRIMERO: IMPONER a la ***SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL*** la sanción de APERCIBIMIENTO por infracción de los siguientes artículos:

- Artículos 5.1.a) y 5.2 del RGPD, tipificada en el artículo 83.5.a) del RGPD y en el artículo 72.1. a) de la LOPDGDD, a los solos efectos de determinar los plazos de prescripción.

- Artículos 12 y 13 del RGPD, tipificada en el artículo 83.5.b) del RGPD y en el artículo 72.1.h) de la LOPDGDD, a los solos efectos de determinar los plazos de prescripción.

- Artículo 25 del RGPD, tipificada en el artículo 83.4.a) del RGPD y en el artículo 73 de la LOPDGDD en el apartado d), a los solos efectos de determinar los plazos de prescripción.

- Artículo 28.3 del RGPD, tipificada en el artículo 83.4.a) del RGPD y en el artículo 73 de la LOPDGDD en el apartado k), a los solos efectos de determinar los plazos de prescripción.

- Artículo 28.10 del RGPD, tipificada en el artículo 83.4.a) del RGPD y en el artículo 73 de la LOPDGDD en el apartado m), a los solos efectos de determinar los plazos de prescripción.

- Artículo 35 del RGPD, tipificada en el artículo 83.4.a) del RGPD y en el artículo 73 de la LOPDGDD en el apartado t), a los solos efectos de determinar los plazos de prescripción.

SEGUNDO: NOTIFICAR la presente resolución a la ***SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL.***

TERCERO: COMUNICAR la presente resolución al Defensor del Pueblo, de

conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al artículo 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la directora de la AEPD en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el artículo 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la AEPD, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el artículo 16.4 de la LPACAP. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-270122

Mar España Martí
Directora de la AEPD