InDret
4.2022

Antoni Rubí Puig
Universitat Pompeu Fabra

Laura Herrerías Castro
Universitat Pompeu Fabra

«Radar COVID» y protección de datos personales

Un análisis de los procedimientos sancionadores de la Agencia Española de Protección de Datos

Sumario

El trabajo analiza las resoluciones de la Agencia Española de Protección de Datos (AEPD) publicadas el 9 de junio de 2022 por medio de las cuales se sanciona a la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA) y a la Dirección General de Sanidad Pública (DGSP) por diversas infracciones del Reglamento General de Protección de Datos cometidas en el desarrollo, implementación y funcionamiento de la aplicación para el rastreo de posibles contactos positivos de COVID-19 denominada «Radar COVID». Después de describir el proceso de desarrollo de la aplicación y su funcionamiento, el trabajo se centra en los aspectos del régimen jurídico sobre protección de datos personales que, según la AEPD, sus promotores habrían incumplido. En este sentido, se analiza el concepto de dato personal manejado por las resoluciones, la calificación de las posiciones de responsable y encargado de los tratamientos de datos entre los sujetos investigados, y los diferentes deberes vinculados al principio de responsabilidad activa. Por último, el trabajo presenta una serie de valoraciones críticas sobre el desarrollo de herramientas informáticas para afrontar situaciones de emergencia sanitaria.

Abstract

This article analyzes the resolutions published on June 9, 2022 by which the Spanish Data Protection Agency (AEPD) imposes an administrative penalty to the Secretary of State for Digitization and Artificial Intelligence (SEDIA) and the General Directorate of Public Health (DGSP) for various infringements of the General Data Protection Regulation that were committed during the development, implementation and operation of «Radar COVID», a COVID-19 contact tracing application. After describing how the app was developed and how it works, the article focuses on the various aspects from the legal regime on the protection of personal data that, according to the AEPD, the app promoters would have violated. In this regard, the concept of personal data used in the resolutions, the allocation of the roles of data controller and data processor between the various investigated subjects, and the different duties linked to the principle of accountability are analyzed. Finally, the article includes a series of criticisms against the development of digital tools to deal with health emergency situations

Title: *«Radar COVID» and personal data protection. An analysis of the Spanish Data Protection Agency's sanction procedures*

Palabras clave: aplicaciones de rastreo, Radar COVID, datos personales, RGPD, AEPD
Keywords**:** *tracing apps, Radar COVID, personal data, GDPR, Spanish Data Protection Agency*

InDret

4.2022

Índice

-

-

1. Introducción*

El pasado 9 de junio de 2022, la Agencia Española de Protección de Datos (AEPD) publicó dos resoluciones mediante las cuales sanciona a la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA) y a la Dirección General de Sanidad Pública (DGSP) por diversas infracciones de la normativa sobre protección de datos personales cometidas en el desarrollo, implementación y funcionamiento de la aplicación para el rastreo de posibles contactos positivos de COVID-19 denominada «Radar COVID»[1].

Las casi 400 páginas que suman ambas resoluciones sirven para ilustrar diversos problemas que puede comportar el desarrollo de herramientas tecnológicas para reaccionar rápidamente frente a eventos disruptivos como una pandemia global. La mayoría de los problemas detectados en la implementación de esta tecnología no son exclusivos del ejemplo español y pueden encontrarse también en las experiencias de desarrollo de aplicaciones de rastreo de positivos de COVID-19 en otros países[2].

Las resoluciones de la AEPD revelan, al menos, tres factores que condicionan el desarrollo de este tipo de herramientas tecnológicas y que ponen en cuestión la conveniencia de impulsarlas. En primer lugar, las aplicaciones de rastreo y otras herramientas similares se han de adoptar en una situación de emergencia permeada de un alto nivel de incertidumbre: los decisores carecen, de entrada, de conocimientos suficientes acerca de la eficacia de la tecnología, de algunas de sus implicaciones éticas y jurídicas[3], así como de la disponibilidad de alternativas mejores. En segundo lugar, se han de adoptar de forma inmediata o, al menos con rapidez y, con frecuencia, con mucha improvisación: los decisores han de valorar si la emergencia y la urgencia permiten una mayor injerencia en los derechos a la intimidad y a la protección de datos personales o si el marco normativo actual -sobre todo, el Reglamento General de Protección de Datos[4]- ya ofrece una ponderación cerrada que les impide ejercer algún margen de discreción. En tercer lugar, se han de adoptar en un entorno institucional y de decisión complejo: los decisores habrán de

*Este trabajo se ha realizado en el marco del proyecto «Coronavirus i dret privat» (2020PANDE00092), financiado por la Agència de Gestió d'Ajuts Universitaris i de Recerca (AGAUR) de la Generalitat de Catalunya.

[1]Se trata de la Resolución de la Agencia Española de Protección de Datos en el expediente N.º PS/00222/2021 (en adelante, «Resolución AEPD SEDIA») [disponible en: https://www.aepd.es/es/documento/ps-00222-2021.pdf (fecha de consulta: 15.10.2022)], y de la Resolución de la Agencia Española de Protección de Datos en el expediente N.º PS/00233/2021 (en adelante, «Resolución AEPD DGSP») [disponible en: https://www.aepd.es/es/documento/ps-00233-2021.pdf (fecha de consulta: 15.10.2022)].

[2] Para un examen general de la litigación en materia de protección de datos personales y COVID-19, véase ANGIOLINI, Chiara, «Case Law Survey On Data Protection – COVID-19 Litigation Project», *Legal Policy & Pandemics. The Journal of the Global Pandemic Network – LPPJ*, vol. 1, núm. 1-2-3, 2021, pp. 197-224. Véase también, YOO, Christopher S./VIDYARTHI, Apratim, «Privacy in the Age of Contact Tracing: An Analysis of Contact Tracing Apps in Different Statutory and Disease Frameworks», *University of Pennsylvania Journal of Law and Innovation*, vol. 5, 2021, pp. 103-158; GREENLEAF, Graham/KEMP, Katharine, «Australia's "COVIDSafe App": An Experiment in Surveillance, Trust and Law», *University of New South Wales Law Research Series*, vol. 7, 2021, pp. 1-17.

[3] Véase Organización Mundial de la Salud, «Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing» (WHO/2019-nCoV/Ethics_Contact_tracing_apps/2020.1).

[4] 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 (OJ L 119/1, 4.5.2016, p. 1-88) (en adelante, «RGPD»).

distribuir entre ellos los roles y las diferentes obligaciones de garantía de los derechos sobre los datos personales.

El presente trabajo describe el desarrollo y funcionamiento de la aplicación «Radar COVID», explica las diferentes infracciones detectadas y las sanciones impuestas a la SEDIA y a la DGSP en sendas resoluciones dictadas por la AEPD, y ofrece, finalmente, algunas valoraciones críticas.

2. Desarrollo e implementación de la aplicación de rastreo «Radar COVID»

Poco después de la declaración del estado de alarma[5], el gobierno de España dio los primeros pasos para poner en marcha diversas herramientas tecnológicas con el fin de intentar actuar contra la propagación del coronavirus SARS-CoV-2. La iniciativa -también seguida en muchos otros países- se emprende en un momento en el cual la información sobre las características del coronavirus, sus formas de contagio y las estrategias de prevención eran más bien limitadas. Así, el 27 de marzo de 2020 el entonces Ministro de Sanidad, Salvador Illa, dictó una Orden por la cual encargaba a la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA), dependiente 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[6]. Mediante el resuelvo primero de esta Orden se encomendaba a la SEDIA: (i) el desarrollo urgente y la operación de una aplicación informática para el apoyo en la gestión de la crisis sanitaria ocasionada por el COVID-19; (ii) el desarrollo de un asistente de conversación o *chatbot* para ser utilizado vía WhatsApp y otras aplicaciones de mensajería instantánea; y (iii) el desarrollo de una web informativa.

A lo que aquí interesa, la Orden describía la referida aplicación informática como una herramienta para permitir a sus usuarios realizar una autoevaluación acerca de la probabilidad de estar infectados con el coronavirus a partir de la información sobre síntomas médicos que le suministraran; y para recibir información, consejos y recomendaciones[7]. En ningún caso, establecía la Orden, la aplicación debería configurarse como un servicio de diagnóstico médico, de atención de urgencias o de prescripción de fármacos. Por otra parte, la aplicación debería permitir la geolocalización del usuario a los solos efectos de verificar que se encontraba en la comunidad autónoma en la que declarara estar. La Orden señalaba, finalmente, que el responsable del tratamiento de los datos personales sería el Ministerio de Sanidad y que el encargado y titular de la aplicación sería la SEDIA.

[5] 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 (BOE núm. 67, de 14.3.2020).

[6] 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 (BOE núm. 86, de 28.3.2020).

[7] La SEDIA puso en marcha una aplicación de autodiagnóstico e información conocida como «Asistencia COVID-19». Paralelamente, algunas CCAA desarrollaron sus propias aplicaciones de autoevaluación del COVID-19, por ejemplo, Cataluña («StopCovid19 CAT»), la Comunidad de Madrid («CoronaMadrid»), y el País Vasco («COVID-19.eus»). Para una descripción detallada de estas 4 aplicaciones véase el informe *COVID-19 Android Apps: Spain App Analysis Report* elaborado por AppCensus [disponible en: https://blog.appcensus.io/wp-content/uploads/2020/04/report.pdf (fecha de consulta: 15.10.2022)]

La descripción del encargo incluida en la Orden no se refiere expresamente a ninguna aplicación informática para el rastreo o trazabilidad de contactos[8]. En otras palabras, el encargo inicial descrito en la Orden no abarcaba el desarrollo de una «aplicación móvil nacional de rastreo de contactos y advertencia», definida por la Comisión Europea como «una aplicación informática aprobada a nivel nacional que funciona en dispositivos inteligentes, en particular teléfonos inteligentes, [que] 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 (*back-end*) a través de internet»[9].

A pesar de no contar con un encargo específico, la SEDIA emprendió durante el mes de abril de 2020 las primeras actuaciones para poder desarrollar una aplicación de rastreo de casos positivos de infección por el coronavirus SARS-CoV-2. Después de una primera reunión interministerial, el 9 de junio de 2020 la entonces Directora General de Salud Pública, Calidad e Innovación (DGSPCI)[10], órgano directivo dependiente del Ministerio de Sanidad, envió una carta al Secretario General de Administración Digital (SGAD), órgano directivo dependiente de la SEDIA, para comunicarle el visto bueno a las pruebas previas necesarias para implementar la aplicación «Radar COVID».

La SGAD acordó el 15 de junio de 2020 la contratación de los servicios para el desarrollo de la aplicación «Radar COVID» con la sociedad mercantil INDRA SOLUCIONES TECNOLOGÍAS DE LA INFORMACIÓN, S.L.U. (en adelante, «INDRA») por un importe de 330.537,52 euros[11]. En este contrato con INDRA, se establecieron tres fases de implantación de la app: fase pre-piloto, fase piloto y fase post-piloto. A los efectos de las resoluciones de la AEPD analizadas en este trabajo, resultan especialmente relevantes la fase piloto y, en menor medida, la fase post-piloto.

La fase piloto se llevó a cabo en la localidad de San Sebastián de La Gomera en las Islas Canarias, con una población censada de unos 7.900 habitantes. Durante esta fase inicial, se perseguía contar con un grupo de población muy limitado para así contrastar la fiabilidad de la aplicación mediante simulaciones y recurriendo a falsos negativos y falsos positivos. El proyecto piloto se llevó a cabo entre el 29 de junio y el 31 de julio de 2020. Durante esta fase, como se verá, la app

[8] Véanse Resolución AEPD SEDIA, p. 76 y Resolución AEPD DGSP, p. 71 y p. 138. La Resolución AEPD SEDIA, p. 80, señala que tampoco había una habilitación para el desarrollo de la aplicación «Radar COVID» en el 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 (BOE núm. 163, de 10.6.2020), cuyos artículos 5, 26 y 27 se referían expresamente a la trazabilidad de contactos.

[9] Art. 1.i de 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 (C/2020/4934) (OJ L 227I, 16.7.2020, p. 1-9).

[10] A partir del 4 de agosto de 2020, el órgano pasa a denominarse Dirección General de Salud Pública (DGSP). Además, parte de sus competencias pasan a otro organismo de nueva creación: la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud (SGSDII). Véase *infra* apartado 4.2.b).

[11] Contrato tramitado de emergencia con arreglo al 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 (BOE núm. 272, de 9.11.2017).

«Radar COVID» estuvo accesible para cualquier ciudadano que quisiera descargarla, y no únicamente para los habitantes de San Sebastián de La Gomera o de otras poblaciones de la isla. Tras considerar que la aplicación había superado esta fase de pruebas y que había permitido resultados notables para la trazabilidad de contactos positivos, el día 19 de agosto sus responsables procedieron a su puesta en funcionamiento en varias CC.AA.

El 15 octubre de 2020 se publica en el BOE el Acuerdo de 9 de octubre entre el Ministerio de Sanidad y el Ministerio de Asuntos Económicos y Transformación Digital acerca de la aplicación «Radar COVID»[12]. Este acuerdo identifica el rol de los diferentes intervinientes en la gestión de la aplicación, así como su papel en la celebración de convenios de colaboración con las autoridades sanitarias de las diferentes CCAA. En particular, el acuerdo especifica que, en estos convenios, el Ministerio de Sanidad y la Consejería competente en materia de sanidad de la Comunidad de que se trate figurarán como responsables de los tratamientos de datos de carácter personal efectuados por la aplicación «Radar COVID» mientras que la SGAD -dependiente de la SEDIA- asumirá la posición de encargado de tratamiento. Se trata del primer documento oficial que procede a una distribución formal de roles relativos a los tratamientos de datos personales entre los principales intervinientes en la gestión de la aplicación, y que no es elaborado hasta varios meses después de la puesta en funcionamiento de la aplicación «Radar COVID».

Antes de describir el funcionamiento de la aplicación «Radar COVID» y la decisión adoptada por la AEPD en sus resoluciones, es oportuno destacar varias vicisitudes ocurridas durante su proceso de desarrollo. En primer lugar, las tareas para la implementación de la aplicación fueron parejas al proceso de investigación de la AEPD. De hecho, el primer requerimiento de información efectuado por la AEPD a la SEDIA se notificó a principios de junio de 2020[13], esto es, antes de iniciar la fase piloto. En efecto, los problemas de la aplicación desde la perspectiva del derecho de la protección de datos personales eran conocidos o podían ser conocidos por los promotores de «Radar COVID» desde los primeros momentos de su desarrollo.

En segundo lugar, diferentes documentos elaborados por los responsables de la aplicación «Radar COVID» -entre ellos, los términos y condiciones de uso y la política de privacidad asociada a la app- se han modificado en diferentes ocasiones. Las diferencias entre las primeras y las últimas versiones son significativas y ponen de relieve no solo la necesidad de una adaptación gradual sino la escasa diligencia desplegada en la redacción de las primeras versiones.

Finalmente, el 9 de septiembre de 2020 se publicó en abierto el código fuente de la aplicación. Pese a la insistencia de varios expertos y activistas para facilitar esta información y poder contrastar el funcionamiento de la app y sus implicaciones técnicas, jurídicas y éticas, no fue hasta esa fecha en la que el código fuente se puso a disposición del público.

3. Funcionamiento y uso de la aplicación «Radar COVID»

«Radar COVID» se describe, en la página web sobre la misma elaborada por el Gobierno de España, como «una aplicación móvil desarrollada para ayudar a controlar la propagación de la

[12] 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» (BOE núm. 273, de 15.10.2020).

[13] Los otros cuatro requerimientos enviados a la SEDIA se formularon en los cinco meses siguientes. El requerimiento a la otra investigada, la SGSDII, se dirigió el 4 de diciembre de 2020.

COVID-19 a través de la identificación de los posibles contactos estrechos de casos confirmados a través de la tecnología Bluetooth»[14].

El funcionamiento de la aplicación es relativamente sencillo pues basta con descargarla desde cualquier dispositivo móvil con sistema operativo Android o iOS, seleccionar el idioma deseado (entre castellano, catalán o valenciano, euskera, gallego, inglés, francés, o rumano), aceptar las condiciones de uso[15] y política de privacidad[16], y, finalmente, activar tanto las notificaciones como el sistema Bluetooth.

A nivel técnico, «Radar COVID» emplea el Sistema de Notificación de Exposiciones (SNE) proporcionado por Apple y Google que, a su vez, fue desarrollado a partir del Protocolo de rastreo de proximidad descentralizado para preservar la privacidad (DP-3T)[17]. Este sistema utiliza la tecnología Bluetooth de baja energía (BLE) para llevar a cabo el rastreo de contactos[18]. En particular, cada teléfono móvil genera una clave aleatoria diaria llamada «clave de exposición temporal»[19] y, a partir de esta clave, se generan unos identificadores anónimos conocidos como «identificadores efímeros Bluetooth». Estos identificadores se intercambian automáticamente entre los teléfonos móviles cercanos que tienen la aplicación y el Bluetooth activado, y quedan almacenados en el registro de contactos del teléfono durante un plazo de 14 días.

Cuando un usuario es diagnosticado de COVID-19 puede solicitar al Servicio Público de Salud de su comunidad autónoma un código de confirmación de un solo uso para introducirlo en la aplicación. Siempre que el usuario lo consienta expresamente, la información del contagio se envía al servidor de la SGAD que se encarga de componer un listado de claves de exposición temporal de personas contagiadas por COVID-19. La aplicación descarga diariamente las claves de exposición temporal del servidor de la SGAD y las compara con los identificadores registrados en los últimos 14 días. Si encuentra una coincidencia, evalúa el riesgo de exposición al virus SARS-CoV-2 en función de la duración (más de 15 minutos) y la distancia (menos de 2 metros) estimada del contacto y envía al usuario una notificación advirtiéndole del día en el que se ha producido el contacto de riesgo. Por el contrario, «Radar COVID» no desvela ni la identidad de la persona contagiada, ni la ubicación donde se ha producido el contacto.

Asimismo, «Radar COVID» es interoperable con aplicaciones similares de rastreo de contactos de modo que los usuarios pueden recibir alertas de contactos de riesgo que se hayan producido

[14] Véase https://radarcovid.gob.es/faq-informacion-general [texto recogido en Resolución AEPD DGSP, p. 68; y Resolución AEPD SEDIA, p. 76 (fecha de consulta: 15.10.2022)].

[15] Disponible en: https://radarcovid.gob.es/condiciones-de-uso (fecha de consulta: 15.10.2022).

[16] Disponible en: https://radarcovid.gob.es/politica-de-privacidad (fecha de consulta: 15.10.2022).

[17] Véanse RAPOSO, Vera Lúcia «"I'm right behind you": Digital contact tracing under European law», *Maastricht Journal of European and Comparative Law*, Agosto 2022; WENDEHORST, Christiane, «COVID-19 Apps and Data Protection», en HONDIUS, Ewoud et al., *Coronavirus and the Law in Europe*, Intersentia, Cambridge, 2021, pp. 163-174.

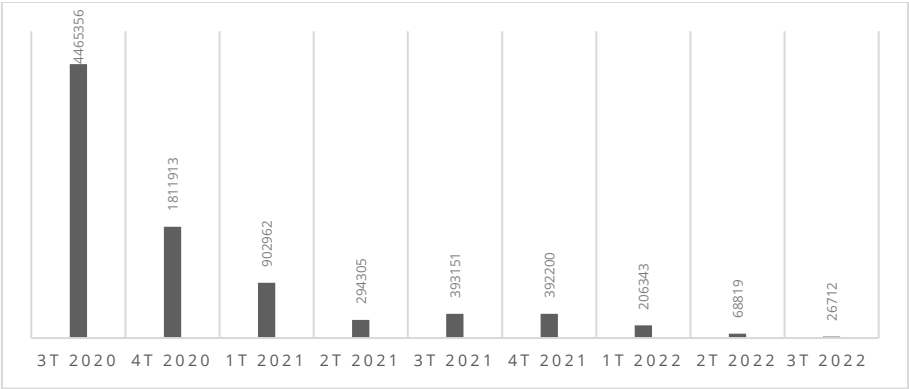
[18] La Recomendación (UE) 2020/518 de la Comisión Europea de 8 de abril de 2020 relativa a un conjunto de instrumentos comunes de la Unión para la utilización de la tecnología y los datos a fin de combatir y superar la crisis de la COVID-19, en particular por lo que respecta a las aplicaciones móviles y a la utilización de datos de movilidad anonimizados (OJ L 114, 14.4.2020, p. 7-15) sugería el uso de la tecnología Bluetooth de baja energía para evitar el tratamiento de datos personales relativos a la localización o los movimientos de personas.

[19] Véase art. 1.k de la Decisión de Ejecución (UE) 2020/1023 de la Comisión de 15 de julio de 2020, según la cual «clave» equivale a: «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».

fuera de España. En concreto, «Radar COVID» es interoperable con Corona Warn App (Alemania), Coronalert (Bélgica), StopCOVID19 (Croacia), Smittestop (Dinamarca), #OstaniZdrav (Eslovenia) COVID Tracker (Irlanda), Immuni (Italia), Apturi COVID (Letonia), Korona STOP (Lituania), CoronaMelder (Países Bajos) y ProteGo Safe (Polonia)[20].

Como advierte la actual política de privacidad de «Radar COVID»: «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».

En cuanto al uso de la aplicación, los datos estadísticos hablan por sí solos: a fecha de 11 de septiembre de 2022, el número de descargas acumuladas era de 8.596.624, lo que representa poco más del 18% de la población española[21]. El mayor número de descargas se concentró durante los meses de agosto (3.368.843 descargas) y septiembre (1.053.819 descargas) de 2020. Desde entonces, el volumen de descargas ha ido disminuyendo de forma significativa[22]. La tabla 1 refleja el total de descargas de la aplicación «Radar COVID» desde el tercer trimestre de 2020 al tercer trimestre de 2022:



Los datos son aún más llamativos con respecto a los códigos de confirmación introducidos por los usuarios en la aplicación. Desde junio de 2020 únicamente se han comunicado 124.473 contagios, lo que representa menos del 1% de los casos positivos de COVID-19 confirmados en

[20] La mayoría de países de la UE han desarrollado aplicaciones de rastreo de contactos a excepción de Bulgaria, Grecia, Luxemburgo, Rumania, Eslovaquia y Suecia. Para una descripción detallada sobre el funcionamiento de las aplicaciones CoronAlert (Bélgica), TousAntiCovid (Francia), Corona Warn App (Alemania), Immuni (Italia), NHS COVID-19 (Reino Unido) y COVIDSafe (Australia), véase POILLOT, Elise et al. «Data protection in the context of COVID-19: A short (hi)story of tracing applications», *Roma TrE-Press*, 2021, pp. 14-93.

[21] El éxito de las apps de seguimiento de contactos se basa en la implicación de un elevado número de usuarios. De acuerdo con la AEPD, el total de usuarios debería representar, como mínimo, el 60% de la población de un determinado territorio, véase AEPD, «El uso de las tecnologías en la lucha contra el COVID19. Un análisis de costes y beneficios», mayo de 2020, pp. 8-9 [disponible en: https://www.aepd.es/sites/default/files/2020-05/analisis-tecnologias-COVID19.pdf) (fecha de consulta: 11.10.2022].

[22] Información disponible en: https://radarcovid.gob.es/estadisticas/descargas-radar (fecha de actualización: 25 de septiembre de 2022 - Semana 38).

España según los datos del Ministerio de Sanidad[23]. De hecho, la última vez que un usuario introdujo un código de confirmación en la aplicación fue el 3 de abril de 2022.

Finalmente, el pasado 9 de octubre de 2022 «Radar COVID» se unió al extenso catálogo de aplicaciones de rastreo de contactos que han dejado de estar operativas[24].

4. Las resoluciones sancionadoras de la AEPD en los procesos PS/00222/2021 y PS/00233/2021

4.1. Procedimiento

La AEPD instruyó el procedimiento sancionador de oficio, a partir del conocimiento de diferentes incidencias relacionadas con la aplicación «Radar COVID» descritas en noticias de prensa, y también en respuesta a diferentes reclamaciones interpuestas por varios particulares, un grupo de profesores e investigadores y por «Rights International Spain», una asociación en defensa de los derechos digitales.

Las actuaciones previas de investigación iniciadas por la AEPD, al menos desde mayo de 2020, se centraron en dos órganos administrativos de la Administración General del Estado: la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA), dependiente del Ministerio de Asuntos Económicos y Transformación Digital; y la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud (SGSDII), dependiente del Ministerio de Sanidad[25]. La primera de ellas fue requerida hasta en cinco ocasiones durante la fase previa de investigación para proporcionar información relativa a la aplicación «Radar COVID» y para acreditar su cumplimiento de la normativa sobre protección de datos. La SGSDII recibió un único requerimiento de información en diciembre de 2020.

El 26 de febrero de 2021 la Subdirección General de Inspección de Datos (SGID) de la AEPD emitió sendos informes de actuaciones previas de investigación contra la SEDIA y la SGSDII en los cuales se describían las incidencias detectadas y se daba respuesta a las alegaciones iniciales formuladas por estas. A partir de dichos informes, la Directora de la AEPD acordó el 21 de mayo de 2021 el inicio de los expedientes sancionadores contra la SEDIA y contra la DGSP. El 11 de junio de 2021 la DGSP presentó un escrito de alegaciones. El 15 de junio hizo lo propio la SEDIA.

Durante los dos procedimientos administrativos se acordó la apertura de sendos plazos de práctica de prueba y se enviaron nuevos requerimientos de información a la SEDIA, la DGSP y la SGSDII.

El 26 de enero de 2022 la instructora del procedimiento formuló dos propuestas de resolución en las que proponía a la Directora de la AEPD que sancionara a la SEDIA y a la DGSP con un

[23]Véase: https://www.sanidad.gob.es/profesionales/saludPublica/ccayes/alertasActual/nCov/situacionActual.htm (fecha de consulta: 15.09.2022).

[24]Información disponible en: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_es (fecha de consulta: 11.10.2022).

[25] La Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud (SGSDII) se creó en agosto de 2020 para reforzar la estructura del Ministerio de Sanidad a raíz de la pandemia ocasionada por el COVID-19. Véase 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 (BOE núm. 211, de 5.8.2020). Véase *infra* apartado 4.2.b).

apercibimiento por la infracción, respectivamente, de los artículos 5.1.a), 5.2, 12, 13, 25, 28.3, 28.10 y 35 RGPD; y de los artículos 5.1.a), 5.2, 12, 13, 25, 28.1, 28.3 y 35 RGPD. La SGAD, por indicación de la SEDIA, formuló nuevas alegaciones.

Finalmente, la Directora de la AEPD dictó dos resoluciones el 18 de febrero de 2022[26] en las que se sanciona a la SEDIA y a la DGSP con un apercibimiento por la comisión de diversas infracciones graves y muy graves de la normativa sobre protección de datos. La SGSDII no es sancionada ya que, al haber sido creada después de los hechos infractores, no pudo participar en ellos. La siguiente tabla describe brevemente las infracciones cometidas:

Norma infringida	Sujeto sancionado	Descripción	Tipificación
5.1.a) RGPD	SEDIA/DGSP	Vulneración del principio de licitud, lealtad y transparencia en el tratamiento de los datos personales.	Muy grave (art. 83.5.a RGPD)
5.2 RGPD	SEDIA/DGSP	Vulneración del deber de responsabilidad proactiva.	Muy grave (art. 83.5.a RGPD)
12 RGPD	SEDIA/DGSP	Falta de suministro de la información en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Muy grave (art. 83.5.b RGPD)
13 RGPD	SEDIA/DGSP	Falta de suministro de información obligatoria sobre el tratamiento de los datos personales.	Muy grave (art. 83.5.b RGPD)
25 RGPD	SEDIA/DGSP	Infracción de las obligaciones derivadas de la protección de datos desde el diseño, por haber omitido la adopción de medidas técnicas y organizativas, no haber realizado las pertinentes evaluaciones de impacto y no haber adoptado garantías necesarias en el tratamiento.	Grave (art. 83.4.a RGPD)
28.1 RGPD	DGSP	Falta de elección de un encargado del tratamiento que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del RGPD y garantice la protección de los derechos de los interesados.	Grave (art. 83.4.a RGPD)
28.3 RGPD	SEDIA/DGSP	Omisión del deber de contar con un contrato o un acto jurídico que regule la relación entre el responsable y el encargado del tratamiento de los datos (entre DGSP y SEDIA y entre DGSP/SEDIA e INDRA).	Grave (art. 83.4.a RGPD)
28.10 RGPD	SEDIA	Extralimitación en el desempeño de las funciones como encargado del tratamiento, que supone la asunción del rol de responsable del tratamiento.	Grave (art. 83.4.a RGPD)
35 RGPD	SEDIA/DGSP	Incumplimiento del deber de elaboración de una evaluación de impacto antes del desarrollo de las operaciones de tratamiento de datos personales.	Grave (art. 83.4.a RGPD)

Las dos resoluciones fueron publicadas finalmente en el sitio web de la AEPD el 9 de junio de 2022.

[26] Ninguna de las dos resoluciones incluye la fecha en la cual fue dictada. La Resolución AEPD SEDIA fue objeto de un recurso de reposición, cuya resolución indica el 18 de febrero como fecha. Véase Resolución del Recurso de reposición Nº RR/00189/2022 en el Procedimiento nº PS/00222/2021, publicada el 10 de junio de 2022 [disponible en https://www.aepd.es/es/documento/reposicion-ps-00222-2021.pdf) (fecha de consulta: 15.10.2022)].

4.2. Principales cuestiones tratadas en las resoluciones de los procedimientos sancionadores

a) *Identificación de los datos personales tratados por «Radar COVID» durante la fase de desarrollo de la aplicación*

Con carácter preliminar, la AEPD ha de valorar si efectivamente la aplicación «Radar COVID» trata datos personales, con qué alcance y desde qué momento. La cuestión es relevante, pues los investigados en el procedimiento sancionador alegaron que durante las primeras fases de desarrollo no se producía ningún tratamiento de datos personales al ser estos ficticios[27], y que, en su caso, los datos personales habían sido anonimizados de modo que habían hecho imposible la identificación de los sujetos usuarios de la aplicación.

La AEPD no comparte las alegaciones formuladas por la SEDIA y la DGSP, ni la información suministrada por la SGSDII, y concluye que la aplicación «Radar COVID» ha tratado diferentes datos personales de usuarios durante diferentes fases de su implementación y, en particular, durante la realización de las pruebas piloto.

Como se ha señalado, se proyectó la realización de las pruebas piloto en la isla de La Gomera para contar con un grupo de población bien delimitado. En particular, las simulaciones y pruebas iniciales se llevaron a cabo en el municipio de San Sebastián de La Gomera, con una población de 7.779 habitantes según los datos del INE, entre los días 29 de junio y 31 de julio de 2020. No obstante, los desarrolladores de la herramienta informática resolvieron no requerir códigos de acceso para su descarga, dada la complejidad de implementar esta solución y el riesgo de menoscabo a la usabilidad de la aplicación[28]. Así las cosas, a la finalización de la prueba piloto, se habían producido 58.652 descargas de la aplicación. Las descargas procedían de otras partes del resto del territorio español, producidas cuando la aplicación no estaba todavía operativa. Para la AEPD, el funcionamiento de la aplicación –ya durante su fase de pruebas- implicaba operaciones de almacenaje y comunicación de diversos datos que han de calificarse como datos personales. En este sentido, la aplicación recopilaba información agregada tanto de los usuarios que la habían descargado como de las personas que asumían el papel ficticio de casos positivos y de los otros usuarios que recibían las alertas de riesgo de contagio.

Para realizar tal valoración, la AEPD parte de un concepto amplio de dato personal, que ha construido la jurisprudencia a partir de la definición que ofrece el artículo 4.1 RGPD[29]: «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».

[27] Resolución AEPD SEDIA, p. 65.

[28] Resolución AEPD SEDIA, p. 161; Resolución AEPD DGSP, p. 129.

[29] Véanse STJUE 20.12.2017, asunto C-434/16, *Peter Nowak c. Data Protection Commissioner*; y STJUE 19.10.2016, asunto C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*. En la jurisprudencia española, la AEPD cita la SAN, Sala Contencioso-Administrativo, 8.3.2002 (ECLI:ES:AN:2002:1485). Véase también STS, Sala Tercera, núm. 1062/2019, de 17.7.2019 (ECLI:ES:TS:2019:2484), relativa a los datos sobre curvas de carga horaria.

En particular, la AEPD concluye que la aplicación trataba ya desde su funcionamiento en la fase de pruebas los siguientes datos personales[30]:

(i) Datos de proximidad o localización de los usuarios de la aplicación. Los datos de geolocalización constituyen datos personales en tanto pueden relacionarse directamente o indirectamente con un individuo identificado o identificable[31].

(ii) Dirección IP del terminal del usuario. Para la AEPD, siguiendo la jurisprudencia del TJUE y la AN, así como su propia práctica[32], no hay dudas acerca del carácter de dato personal de las direcciones IP. Es irrelevante que estos datos se sometieran a procedimientos de encriptación y medidas de salvaguardia y que no permitieran una identificación directa del usuario o del dispositivo, ya que sí permitirían una identificación indirecta[33].

(iii) Datos relativos a la salud, esto es «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» (artículo 4.15 RGPD). Podemos identificar, según la AEPD, tres elementos diferentes que son objeto de tratamiento por parte de la aplicación «Radar COVID»:

- Código de confirmación de un solo uso de 12 dígitos facilitado por las autoridades sanitarias a los usuarios que habían dado positivo en una prueba diagnóstica de COVID-19.
- Dato mediante el cual el usuario es advertido previamente de un contacto de riesgo.
- Día en que el usuario desarrolló síntomas compatibles con COVID-19.

Estos datos personales se consideran especiales (art. 9.1 RGPD), por lo que pesa sobre ellos un principio de prohibición de tratamiento, salvo que concurra alguna de las circunstancias previstas en el artículo 9.2 RGPD. Así las cosas, son objeto de una mayor protección por el ordenamiento jurídico. De nuevo, para la AEPD resulta irrelevante que estos datos no permitieran una identificación directa de un individuo usuario de la aplicación y, en particular, de un usuario contagiado. La propia SEDIA

[30] En sentido similar véase BRADFORD, Laura/ABOY, Mateo/LIDDELL, Kathleen, «COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes», *Journal of Law and the Biosciences*, Mayo 2020, pp. 4-8.

[31] Véanse las Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-19, adoptadas el 21 de abril de 2020 por el Comité Europeo de Protección de Datos (CEPD).

[32] STJUE 19.10.2016, asunto C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*; SAN, Sala Contencioso-Administrativo, 1.9.2011 (ECLI:ES:AN:2011:3907); Véase también el Dictamen 4/2007 sobre el concepto de datos personales elaborado por el Grupo de Trabajo del Artículo 29 (01248/07/ES WP 136); e informes del Gabinete Jurídico de la AEPD 327/2003 o 213/2014.

[33] En este sentido, véase considerando 26 RGPD: «[…] 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. […]».

> admitió en las evaluaciones de impacto sobre los datos personales que realizó con posterioridad (agosto de 2020 y septiembre de 2020) la posibilidad de una identificación indirecta de los usuarios por medio de la relación con otros conjuntos de datos. En consecuencia, se trataría no de datos anonimizados, sino simplemente seudonimizados[34].

En suma, desde el momento en el cual un usuario se descargaba la aplicación «Radar COVID» de las fuentes disponibles, existía tratamiento de datos personales. El tratamiento de datos personales se iniciaba ya en la fase piloto, cuando cualquier sujeto podía descargarse la aplicación, y con independencia de que, en esta fase, se trabajara con datos manipulados para así testar el correcto funcionamiento de la herramienta informática.

b) *Determinación de los sujetos implicados en el tratamiento de datos personales: responsables del tratamiento, encargados del tratamiento y corresponsables*

Una de las dificultades inherentes al desarrollo de una herramienta de rastreo de contactos deriva de la participación de diferentes agentes en las diversas fases de implementación. En el caso español, es necesaria la coordinación de varios órganos de la Administración General del Estado integrados en ministerios diferentes. Además, teniendo en cuenta la descentralización del sistema sanitario español, deben tenerse en cuenta las distintas administraciones autonómicas. Finalmente, el rol de los proveedores privados no puede ignorarse.

Atendiendo a la complejidad del proceso de toma de decisiones administrativas para el desarrollo de la herramienta informática, resulta necesario identificar quién –desde la perspectiva del derecho de protección de datos– asume la condición de responsable del tratamiento, esto es, quién determina en la práctica los fines y los medios del tratamiento de datos personales (art 4.7 RGPD). Es al responsable a quien incumben las principales obligaciones articuladas en el RGPD y, en particular, es quien ha de asumir un rol proactivo (principio de *accountability* o de responsabilidad activa) para cumplir con la normativa y poder acreditar su cumplimiento (arts. 5.2, 24 y 25 RGPD).

La implicación de diferentes sujetos puede comportar dificultades para identificar quién de ellos asume el rol de responsable del tratamiento. A pesar de tener que arrostrar muchas obligaciones y responsabilidades, la posición de encargado del tratamiento (art. 4.8 RGPD) es menos intensiva –y, en general, menos costosa en las inversiones necesarias para desempeñarla– que la de responsable, por lo que puede haber un interés en evitar este último rol. Por ello, en ocasiones, un sujeto con mayor poder de negociación puede imponer contractualmente o formalmente la condición de responsable del tratamiento de datos a otro. Los encargados del tratamiento también pueden tomar decisiones importantes en el desarrollo de una herramienta tecnológica y, por ejemplo, pueden definir aquellos medios no esenciales o aspectos más prácticos de la implementación[35]. En algunos procesos de tomas de decisiones, podrán darse también supuestos de corresponsabilidad en el tratamiento si dos o más sujetos determinan conjuntamente los fines

[34] Véase art. 4.1.5 RGPD.

[35] Para la AEPD, la condición de encargado del tratamiento viene determinada por la concurrencia de dos características: «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 aquéllos» (Resolución AEDE SEDIA, p. 189).

y medios del tratamiento (art. 26 RGPD)[36]. Con todo, la delimitación entre las diferentes figuras previstas en el RGPD, como indica la jurisprudencia y la práctica de la AEPD, es funcional y no se rige por criterios meramente formalistas: debe atenderse caso por caso a las actividades reales desplegadas por cada sujeto y no a la mera designación formal de uno de ellos como responsable del tratamiento[37].

La AEPD destaca «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 personales. [...] La competencia determinará, por tanto, la legitimación para realizar el tratamiento»[38]. En consecuencia, resulta imprescindible identificar las competencias atribuidas a cada órgano administrativo y examinar si se produce o no una actuación extralimitada. En el caso del desarrollo de la aplicación «Radar COVID» debe tenerse en cuenta, además, las modificaciones normativas que alteraron la estructura orgánica de uno de los ministerios afectados y la distribución interna de competencias que complican sobremanera la lectura de las Resoluciones de la AEPD.

> Así, en el caso del Ministerio de Sanidad podemos identificar dos períodos temporales diferentes. El primero de ellos se extiende desde la declaración del estado de alarma hasta la fecha de entrada en vigor de la modificación de la estructura orgánica del Ministerio, esto es, desde el 12 de marzo hasta el 6 de agosto de 2020. Durante este período, el Ministerio de Sanidad, con arreglo a los Reales Decretos 139/2020, de 28 de enero, y 454/2020, de 10 de marzo[39], desarrolló sus funciones por medio de diversos órganos directivos, entre ellos la Dirección General de Salud Pública, Calidad e Innovación (DGSPCI). Este órgano tenía atribuidas funciones de vigilancia en salud pública de carácter estatal, y de elaboración de sistemas de información, gestión de la información, identificación de la población protegida y acceso a la información clínica y terapéutica, entre otros[40].
>
> El segundo período se inicia el 6 de agosto, con la entrada en vigor del Real Decreto 735/2020, de 4 de agosto, y sigue en adelante durante el funcionamiento de la aplicación[41]. Este Real Decreto procedió a una modificación de la estructura orgánica del Ministerio de Sanidad y, en particular, estableció dos cambios relevantes. En primer lugar, la Dirección General de Salud Pública, Calidad e Innovación (DGSPCI) pasó a denominarse Dirección General de Salud Pública (DGSP), y asumió las funciones de vigilancia en salud pública de carácter estatal[42]. Por otra parte, para reforzar la estructura del Ministerio, se creó la Secretaría General de Salud Digital, Información e Innovación

[36] La noción de corresponsabilidad en el tratamiento que ha elaborado el TJUE complica la distribución de roles entre diferentes sujetos implicados en operaciones de tratamiento de datos personales. Véanse STJUE 5.6.2018, asunto C-210/16, *Wirtschaftsakademie Schleswig-Holstein*; STJUE 10.7.2018, asunto C-25/17, *Tietosuojavaltuutettu*; y STJUE de 29.7.2019, asunto C-40/17, *Fashion ID*.

[37] Véanse Directrices 07/2020 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» en el RGPD, adoptadas el 7 de julio de 2021 por el CEPD; e Informes 287/2006 y 64/2020 del Gabinete Jurídico de la AEPD.

[38] Resolución AEPD SEDIA, pp. 171-172; y Resolución AEPD DGSP, p. 135.

[39] Real Decreto 139/2020, de 28 de enero, por el que se establece la estructura orgánica básica de los departamentos ministeriales (BOE núm. 25, de 29.1.2020); 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 (BOE núm. 63, de 12.3.2020).

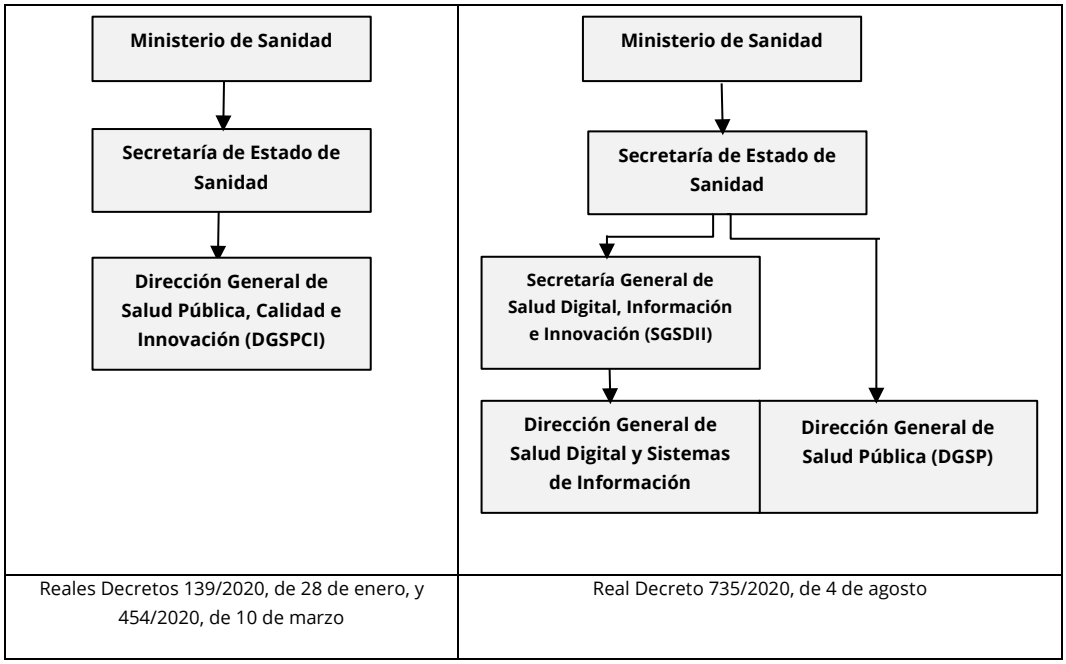
[40] Artículo 3 RD 454/2020.

[41] 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 (BOE núm. 211, de 5.8.2020).

[42] Artículo 4 RD 735/2020, de 4 de agosto.

del Sistema Nacional de Salud (SGSDII), a la cual se atribuyeron algunas competencias de la antigua DGSPCI, en particular, las relativas a la elaboración de sistemas de información, la gestión de la información, la identificación de la población protegida y el acceso a la información clínica y terapéutica[43].

La tabla 1 refleja la estructura orgánica del Ministerio de Sanidad en estos dos períodos en relación con la aplicación «Radar COVID»:



Por otra parte, el Ministerio de Asuntos Económicos y Transformación Digital, con arreglo al art. 1 del Real Decreto 403/2020, de 25 de febrero[44], se encarga, entre otras materias, de «la política de telecomunicaciones y para la transformación digital, en particular impulsando la digitalización de las Administraciones Públicas». La SEDIA forma parte del Ministerio de Asuntos Económicos y Transformación Digital. Las funciones que reglamentariamente tiene atribuidas consisten en «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»[45].

La Secretaría General de Administración Digital (SGAD) es el órgano directivo al que corresponde, bajo la autoridad de la SEDIA, la dirección, coordinación y ejecución de las competencias en materia de transformación digital de la administración, incluyendo su desarrollo técnico[46].

La tabla 2 refleja la estructura orgánica del Ministerio de Asuntos Económicos y Transformación Digital en relación con la aplicación «Radar COVID»:

[43] Artículo 3 RD 735/2020, de 4 de agosto.

[44] 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 (BOE núm. 50, de 27.2. 2020).

[45] Artículo 8 del RD 403/2020, de 25 de febrero.

[46] Artículo 9 del RD 403/2020, de 25 de febrero.

A los efectos de identificar los diferentes responsables y encargados del tratamiento de datos personales en el funcionamiento de la aplicación «Radar COVID», la AEPD distingue dos fases diferentes:

(i) Fase inicial en el despliegue de la aplicación: comprende el período en el cual se concibe el desarrollo de una aplicación para la trazabilidad de contactos, se determinan sus características y se lleva a cabo el proyecto piloto «Radar COVID» para asegurar su correcto funcionamiento. Es en esta fase en la que se cometen las principales infracciones detectadas por la AEPD.

Durante esta primera fase, la AEPD concluye que la DGSPCI ostentaba la condición de responsable del tratamiento y que, además, la SEDIA actuaba *de facto* como responsable del tratamiento sin tener atribuida una competencia para ello.

Para la AEPD la condición de responsable del tratamiento para el desarrollo y funcionamiento de una aplicación de rastreo de contactos como «Radar COVID» debería recaer en una autoridad sanitaria. Cita en este sentido el apartado 3.1 de la Comunicación de la Comisión Europea 2020/C 124 I/01[47], que persigue atribuir a las autoridades sanitarias la función de determinar los fines y medios de los tratamientos de datos personales con el objetivo de reforzar la confianza ciudadana ante estas aplicaciones.

El ordenamiento jurídico español atribuye de entrada a las autoridades sanitarias las competencias para adoptar diferentes medidas para el control de enfermedades y riesgos sanitarios (artículo 3 Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública[48]; artículos 5 y 84 de la Ley 33/2011, de 4 de

[47] De acuerdo con el art. 3.1 de la Comunicación de la Comisión: orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de covid-19 en lo referente a la protección de datos 2020/C 124 I/01 (C/2020/2523; OJ C 124I , 17.4.2020, p. 1-9), «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».

[48] Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública (BOE núm. 102, de 29.4.1986). El art. 3 establece que: «Con el fin de controlar las enfermedades transmisibles, la autoridad sanitaria,

octubre, General de Salud Pública)[49]. En definitiva, para la AEPD, «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»[50].

Como se ha señalado, durante esta fase inicial, el Ministerio de Sanidad, con arreglo a su estructura orgánica, llevaba a cabo sus funciones en relación con los desarrollos tecnológicos para frenar la pandemia, por medio de la Dirección General de Salud Pública, Calidad e Innovación (DGSPCI) –posteriormente, denominada Dirección General de Salud Pública (DGSP)–, la cual *prima facie* debía asumir el rol de responsable del tratamiento de datos personales asociado a la aplicación «Radar COVID». De hecho, la DGSPCI llevó a cabo varias actuaciones que acreditan la adopción de decisiones acerca de las finalidades y los medios del tratamiento de datos personales de la aplicación: participó en varias reuniones para planificar su desarrollo, comunicó el visto bueno a la SGAD para poner en marcha el proyecto piloto, y también validó el informe final del análisis de conclusiones del proyecto[51].

Como pone de relieve la AEPD, la DGSPCI fue «la que decidió el uso de nuevas tecnologías, en forma de aplicación móvil, como medio de apoyo de la estrategia de identificación y seguimiento de contactos, condicionado el tratamiento y los "medios esenciales"»[52]. Hay que recordar que en esta fase todavía no se había creado la SGSDII, por lo que no pudo intervenir en ningún momento en la toma de decisiones acerca de la aplicación.

Por otra parte, la AEPD valora las actuaciones de la SEDIA. Como se ha señalado, conforme al ordenamiento, sus competencias incluyen «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 otros departamentos ministeriales»[53]. De entrada, para la AEPD, su rol por defecto conforme a esta atribución competencial sería el de encargado del tratamiento. Ahora bien, las actuaciones que llevó a cabo durante la fase inicial del proyecto denotan que su implicación correspondió a la propia de un responsable del tratamiento. En este sentido, la AEPD distingue entre un conjunto de actuaciones *ad intra* y otras *ad extra*. Entre las primeras, se ha acreditado que, aunque la DGSPCI dio el visto bueno a la elaboración del proyecto en una carta a la SEDIA de 9 de junio de 2020, fue la SEDIA la que efectivamente determinó los fines del tratamiento y decidió en la práctica sobre los medios esenciales para llevarlo a

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».

[49] Téngase en cuenta también que el artículo 4.2.d) del Real Decreto 463/2020, de 14 de marzo, designaba al Ministro de Sanidad como autoridad competente delegada en su área de responsabilidad.

[50] Resolución AEPD SEDIA, p. 175.

[51] Resolución AEPD DGSP, pp. 138-139.

[52] Resolución AEPD DGSP, p. 139.

[53] Artículo 8 del Real Decreto 403/2020, de 25 de febrero.

cabo. Otro indicio, aunque no determinante, es que durante esta fase no se procedió en ningún momento a una designación formal expresa de la SEDIA como encargada del tratamiento: por ejemplo, no se suscribió un contrato o se dictó un acto jurídico en el sentido del artículo 28.3 RGPD para la designación formal de la SEDIA como encargada del tratamiento. También, en ese momento, la DGSPCI consideraba que, dada la estructura descentralizada del sistema sanitario español, la condición de responsable de los tratamientos realizados por la aplicación «Radar COVID» no debería recaer en el Ministerio de Sanidad o uno de sus órganos directivos, sino que deberían ser las autoridades sanitarias de cada comunidad autónoma las que ostentaran la condición de responsable del tratamiento. En consecuencia, si la DGSPCI consideraba que no era responsable, no podía designar a la SEDIA como encargada del tratamiento[54].

Además, en el momento en el cual se contrata por vía de emergencia los servicios de la empresa INDRA, el responsable del tratamiento debería haber concluido con esta un acuerdo en el sentido del artículo 28.3 RGPD para designarla encargada del tratamiento en relación al desarrollo de la aplicación «Radar COVID» y haber reflejado el contenido mínimo que señala el precepto. Sin embargo, ni la DGSPCI ni la SEDIA procedieron a suscribir este contrato. De hecho, si la SEDIA hubiera ostentado la condición de encargada del tratamiento, no habría podido suscribir el acuerdo ya que debería haber requerido a la DGSPCI, como responsable del tratamiento, para que procediera a autorizarla previamente y, por escrito, como exige el artículo 28.2 RGPD para recurrir a otro encargado[55]. En cualquier caso, ni el acuerdo de contratación, ni el pliego de condiciones designan formalmente a INDRA como encargada o subencargada del tratamiento, ni tampoco reflejan el contenido mínimo que exige el artículo 28.3 RGPD.

A resultas de estas actuaciones, la AEPD concluye 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»[56], pero también fue ella quien determinó «los fines y medios de los tratamientos realizados (amén de la apariencia ante los ciudadanos como responsable del tratamiento)»[57]. La AEPD recuerda que, aún en el caso en el cual la SEDIA hubiera sido formalmente designada como encargada del tratamiento, su actuación en la práctica se habría extralimitado, por lo que podría resultar de aplicación lo previsto en el artículo 28.10 RGPD: «[...] 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».

(ii) Fase de implementación de la aplicación Radar COVID, especialmente a partir de la celebración del Acuerdo de uso de la aplicación de 13 de octubre de 2020 entre el

[54] Resolución AEPD SEDIA, p. 177.

[55] Resolución AEPD SEDIA, p. 191.

[56] Resolución AEPD SEDIA, p. 185.

[57] Resolución AEPD SEDIA, p. 185.

Ministerio de Sanidad y el Ministerio de Asuntos Económicos y Transformación Digital.

En este momento ya se ha creado la SGSDII, concebida para reforzar el Ministerio de Sanidad en sus estrategias digitales y, en particular, a partir del sobreesfuerzo ocasionado por la pandemia. Es la SGSDII la que da continuidad al proyecto sobre la aplicación que había emprendido la DGSPCI, y la que, a su desaparición, la sucede en su condición de responsable del tratamiento. A partir de la creación de la DGSPCI, se dan toda una serie de elementos que contribuyen a una mejor identificación de los roles de los diferentes sujetos implicados en la operativa de la aplicación «Radar COVID». En primer lugar, y sobre todo, el «Acuerdo entre el Ministerio de Asuntos Económicos y Transformación Digital y el Ministerio de Sanidad acerca de la aplicación "Radar COVID"» de 13 de octubre de 2020 establece que la SGSDII asume la condición de responsable del tratamiento de los datos personales y que la SGAD actuará como encargada del tratamiento. En segundo lugar, la política de privacidad de la aplicación en la redacción dada después del acuerdo también identifica a la SGSDII como responsable y a la SGAD como encargada del tratamiento. Finalmente, el Registro de Actividades del Tratamiento (RAT) del Ministerio de Sanidad designa a la SGSDII como responsable de los tratamientos relacionados con la aplicación «Radar COVID». En definitiva, en esta segunda fase, la calificación de las posiciones de los diferentes sujetos implicados en la operativa de la aplicación es más sencilla, pues coinciden las atribuciones competenciales con las funciones efectivamente desempeñadas por cada uno de ellos.

c) *Deberes de información y transparencia*

Al producirse un tratamiento de datos de los usuarios ya durante la fase piloto del proyecto, la AEPD concluye que el responsable del tratamiento debería haber notificado e informado a los interesados sobre los diferentes aspectos previstos en el RGPD para dar cumplimiento así a su obligación de transparencia. En particular, el artículo 12 RGPD establece que el responsable del tratamiento deberá adoptar las medidas oportunas para facilitar a los interesados la información completa relativa a los tratamientos de sus datos personales en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo. El artículo 13 RGPD obliga a informar sobre aspectos, tales como la identidad y los datos de contacto del responsable; los datos de contacto del delegado de protección de datos, en su caso; los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento; los destinatarios o las categorías de destinatarios de los datos personales; las condiciones, en su caso, de las transferencias internacionales de datos; los plazos de conservación de los datos; y los derechos de los interesados y su modo de ejercicio.

Según las resoluciones de la AEPD, en la primera versión del programa piloto de julio de 2020 que se puso a disposición de los usuarios para su descarga, las condiciones de uso y la política de privacidad que la acompañaban no cumplían con las exigencias de información impuestas por los artículos 12 y 13 RGPD. En este sentido, no identificaban quiénes eran los responsables y encargados del tratamiento y la información contenida en ellos no se facilitó de forma «concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo»[58]. Además, en ellos

[58] Resolución AEPD SEDIA, p. 193; Resolución AEPD DGSP, p. 153.

se negaban los derechos de los interesados previstos en los artículos 15-22 RGPD, al considerar que no se producía un tratamiento de datos personales[59].

En definitiva, puesto que los promotores de la aplicación no consideraban que hubiese un tratamiento de datos personales no tuvieron en cuenta las obligaciones establecidas en el RGPD y demás normativa de aplicación, lo que comporta una infracción muy grave con arreglo al art. 83.5.b) RGPD. Además, también comporta un incumplimiento del principio de licitud, lealtad y transparencia en el tratamiento de los datos personales (art. 5.1.a) RGPD) y del deber de responsabilidad proactiva (art. 5.2 RGPD).

La AEPD destaca otros problemas sobre falta de transparencia detectados en momentos posteriores. Por ejemplo, señala que la información no fue accesible para personas con problemas visuales[60]. También explica que, en modificaciones posteriores de la documentación facilitada a los usuarios, tampoco se identificaban correctamente quiénes asumían los roles de responsable y de encargado del tratamiento. Tampoco se facilitaban en dichos documentos datos sobre la identidad del Delegado de Protección de Datos y formas de contacto.

Para la AEPD, la información suministrada tampoco es clara sobre las categorías de datos tratados[61], ni sobre las bases de licitud[62]. La información sobre las finalidades y destinatarios de los datos también resulta genérica y ambigua[63].

Finalmente, las resoluciones destacan que la información no siempre es coherente. De hecho, en enero de 2022, en el apartado de preguntas frecuentes en la página web sobre la aplicación «Radar COVID», se seguía insistiendo que esta no trataba ningún tipo de dato personal[64].

En conclusión, para la AEPD, la SEDIA, actuando *de facto* como responsable, no adoptó las medidas necesarias para facilitar a los interesados toda la información prevista en los artículos 12 y 13 RGPD[65]. Tampoco la DGSP cumplió con su deber que le correspondía como responsable del tratamiento de acuerdo con la atribución competencial[66]. Para la AEPD, cumplir con el deber de transparencia –y su correlato: el derecho de información de los interesados- «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»[67].

[59] Resolución AEPD SEDIA, p. 198; Resolución AEPD DGSP, p. 153.

[60] Resolución AEPD SEDIA, p. 194; Resolución AEPD DGSP, p. 151.

[61] Resolución AEPD SEDIA, p. 195; Resolución AEPD DGSP, pp. 152-153.

[62] Resolución AEPD SEDIA, p. 195-196; Resolución AEPD DGSP, pp. 153-154.

[63] Resolución AEPD SEDIA, p. 197; Resolución AEPD DGSP, pp. 154-155.

[64] Resolución AEPD SEDIA, p. 142; Resolución AEPD DGSP, p. 124.

[65] Véanse también Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679, adoptadas el 29 de noviembre de 2017 por el Grupo de Trabajo del artículo 29 (WP260 rev.01).

[66] Resolución AEPD DGSP, p. 145.

[67] Resolución AEPD SEDIA, p. 198; Resolución AEPD DGSP, p. 156.

d) *Obligación de elaborar las correspondientes evaluaciones de impacto*

Las Resoluciones de la AEPD concluyen que ni la SEDIA ni la DGSPCI elaboraron las pertinentes evaluaciones de impacto relativas a la protección de datos personales (EIPD) antes de iniciar las primeras operaciones de tratamiento, en incumplimiento de lo previsto en el artículo 35 RGPD.

Durante el procedimiento de investigación la SEDIA aportó dos versiones diferentes de una evaluación de impacto, una fechada en 12 de agosto de 2020 –realizada, en principio, antes del lanzamiento de la app «Radar COVID» al público en general– y otra de octubre de 2020. Por ello, al menos durante la fase piloto del proyecto, se habrían tratado datos personales de los usuarios de la app sin haber elaborado antes una evaluación de impacto.

Por otra parte, en la elaboración de las evaluaciones de impacto aportadas por la SEDIA, no se habría contado con la participación del Delegado de protección de datos, lo que comporta una infracción de lo establecido en los artículos 35.2 y 39.1.c) RGPD.

En consecuencia, para la AEPD, «[l]a 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»[68].

En este sentido, la actuación de la SEDIA y la DGSPCI supuso una vulneración del artículo 35 RGPD[69]. En las Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-19, el CEPD señalaba claramente que habría «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)». Además, el CEPD también «recomienda encarecidamente la publicación de las EIPD» (apartado 39).

Además, para la AEPD, las EIPD están vinculadas con el principio de responsabilidad proactiva (artículo 5.2 RGPD) y con el principio de protección de datos desde el diseño y protección de datos por defecto (artículo 25 RGPD). En este sentido, la elaboración de una EIPD permite anticipar los diferentes riesgos asociados a las operaciones de tratamiento que se pretenden poner en marcha e identificar diferentes medidas para evitar o minimizar sus consecuencias. Para la AEPD, los hechos ponen de manifiesto «una falta flagrante de privacidad desde el diseño» ya que se produjo «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»[70].

La AEPD rechaza la argumentación de la SEDIA según la cual al considerar que no se trataba ningún dato personal durante la fase piloto del proyecto no era necesario realizar una EIPD. Para

[68] Resolución AEPD SEDIA, p. 205; Resolución AEPD DGSP, p. 165.

[69] Véanse asimismo considerandos 89, 90 y 91 RGPD y 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 por el GT Artículo 29 (WP 248 rev.01).

[70] Resolución AEPD SEDIA, p. 206.

la AEPD, para discernir efectivamente si la aplicación trataba o no datos personales ya durante la fase piloto, el responsable debería haber elaborado de hecho una EIPD.

e) *Vulnerabilidades en la aplicación*

Desde abril de 2020, se conocía públicamente una vulnerabilidad en el diseño técnico del software que utilizaban las aplicaciones de rastreo basadas en el protocolo abierto «Decentralized Privacy-Preserving Proximity Tracing» (DP3T), que acabó adoptando la aplicación «Radar COVID».

El equipo DP3T había publicado aquel mes su informe técnico «Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems», que relataba que únicamente los usuarios que hubieran recibido un test positivo de COVID-19 subían las claves TEK a los servidores utilizado por la aplicación de rastreo. En consecuencia, cada vez que se observaba una subida de la clave desde un teléfono al servidor, se podía inferir que el propietario del terminal estaba infectado con el coronavirus. Además, aunque se recurriera a encriptar los datos entre la aplicación y los servidores y, en consecuencia, no se pudiera observar el *endpoint* y el contenido de la subida al servidor, a partir de la longitud de los mensajes se revelaba una subida de la clave TEK con resultado positivo al servidor. Esta comunicación de información entre teléfono móvil y servidor podía ser observada por diversos terceros como, por ejemplo, la compañía proveedora de servicios de telecomunicaciones -si la conexión al servidor se realiza mediante GSM-, la proveedora de servicios de acceso a Internet; o de cualquier persona que tuviera acceso a la misma red (WiFi o Ethernet) que el usuario.

Varias reclamaciones ante la AEPD señalaron esta vulnerabilidad, entre ellas, la formulada por diversos profesores expertos en protección de datos personales. Explicaron, además, que, en el caso español, el funcionamiento de la app permitía vincular de modo inequívoco una IP con el hecho de que su titular estaba subiendo un test positivo de COVID. El sistema asociaba la dirección IP a los datos de clave TEK subidos por usuarios que habían dado positivo. Las direcciones IP de los usuarios de «Radar COVID» asociadas a un test positivo de COVID podían ser observadas por la compañía Amazon, que proporcionaba la tecnología del *endpoint* de CloudFront CDN utilizada para la descarga de las claves TEKs. En definitiva, los datos sobre salud quedaban vinculados a una dirección IP, que además de constituir un dato personal, permitiría identificar indirectamente a la persona diagnosticada[71].

El equipo de desarrollo de la aplicación, a pesar de conocer esta vulnerabilidad en el protocolo, consideró que los riesgos eran residuales y prefirió no adoptar ninguna medida de corrección, cuando esta era factible. El problema no fue corregido hasta el 8 de octubre de 2020, esto es, casi dos meses después de su puesta en funcionamiento.

Por ello, concluye la AEPD, «el diseño de la aplicación no ha tenido presente de forma efectiva los principios aplicables a la protección de datos» y «[e]n la aplicación de las medidas de seguridad técnicas y organizativas, el responsable no ha tenido en consideración los riesgos que representaba este tratamiento»[72]. De hecho, para la AEPD, «aun siendo conscientes del riesgo,

[71] Véase *supra* apartado 4.2.a).

[72] Resolución AEPD SEDIA, p. 210.

no integraron las garantías necesarias para garantizar la confidencialidad de los datos y resiliencia de los sistemas»[73].

4.3. Sanción impuesta por la AEPD

A pesar de las múltiples infracciones detectadas durante el procedimiento de investigación y que son prolijamente descritas en las resoluciones, las sanciones impuestas por la AEPD a la SEDIA y a la DGSP se circunscriben a un simple apercibimiento, sin consecuencias económicas.

El artículo 83.7 RGPD establece que «[s]in 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 España, el artículo 77 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)[74] establece que para determinados sujetos –y en particular, en relación con la Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración local–, cuando actuando como responsables o encargados del tratamiento de datos personales, cometan alguna infracción, «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».

Puede discutirse si una sanción de apercibimiento tiene poder disuasorio suficiente para prevenir la comisión de infracciones de la normativa de protección de datos. Anticipar que no seguirán a las infracciones unas consecuencias significativas puede no proporcionar incentivos suficientes a los decisores públicos para evitar su comisión. En cualquier caso, hay otros factores en la normativa sobre protección de datos que pueden reducir este riesgo y proporcionar incentivos a la prevención de infracciones: la posibilidad de iniciar procedimientos disciplinarios contra autoridades y directivos (artículo 77.3 LOPDGDD); la responsabilidad civil derivada de infracciones de la normativa sobre protección de datos (artículo 82 RGPD) o la adopción de medidas de corrección o cese que pueden comportar en la práctica un coste muy elevado o la pérdida de las inversiones previamente realizadas. Las consecuencias reputacionales y, en particular el desgaste político, también pueden incentivar la adopción de decisiones más cuidadosas de los derechos de los datos personales de los ciudadanos.

5. Valoraciones y lecciones para futuras pandemias

5.1. Emergencia y ponderación de derechos

Las dos resoluciones dictadas por la AEPD en relación con el desarrollo e implementación de la aplicación para rastreo de casos positivos «Radar COVID» dan buena cuenta de las múltiples

[73] Resolución AEPD SEDIA, p. 210.

[74] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294, de 6.12.2018).

infracciones de la normativa sobre protección de datos personales que sus promotores habrían cometido. La AEPD relata cómo estos, al menos en los primeros estadios de desarrollo de la aplicación, habrían ignorado los deberes más básicos que prescribe el RGPD y situado sus actuaciones muy por debajo del umbral mínimo de diligencia que impone el principio de responsabilidad activa.

No puede servir de justificación que los responsables en el Ministerio de Sanidad y en el Ministerio de Asuntos Económicos y Transformación Digital, así como los proveedores externos de la tecnología, consideraran que la aplicación en su fase piloto no trataba datos personales sino únicamente datos manipulados y datos anonimizados[75]. Se trate esta de una creencia errónea o de una justificación construida *ex post*, no ha de valer como argumento para dejar sin aplicación el RGPD y demás normativa sobre protección de datos personales.

La situación de urgencia y emergencia tampoco justifica una ignorancia tal del derecho de protección de datos. Como es incontestable, la declaración del estado de alarma que siguió en España a la propagación del coronavirus SARS-CoV-2 ni suspendió la eficacia del RGPD, ni vació de contenido los derechos fundamentales a la intimidad y a los datos personales. En otros términos, una situación de emergencia sanitaria no genera una suerte de *sandbox* jurídico, que permite a los decisores públicos un amplio margen de maniobra para diseñar nuevas herramientas informáticas sin asumir ningún tipo de responsabilidad jurídica.

Ya desde los inicios de la pandemia en España, la AEPD tomó posición sobre la necesidad de una aplicación estricta del RGPD a las diferentes actuaciones que pudieran implicar tratamientos de datos personales. En este sentido, el Gabinete Jurídico de la Agencia Española de Protección de Datos elaboró los informes N/REF 0017/2020 y N/REF 32/2020, en los cuales se destacó que la normativa de protección de datos personales debía aplicarse íntegramente a la situación de emergencia sanitaria provocada por la extensión del virus COVID-19. En particular, el informe N/REF 0017/2020 advierte que «las consideraciones relacionadas con la protección de datos -dentro de los límites previstos por las leyes- no deberían utilizarse para obstaculizar o limitar la efectividad de las medidas que adopten las autoridades, especialmente las sanitarias, en la lucha contra la epidemia, por cuanto ya la normativa de protección de datos personales contiene una regulación para dichos casos que compatibiliza y pondera los intereses y derechos en liza para el bien común» (p. 1).

Esta misma posición se repite en las resoluciones que analizamos en este trabajo. La AEPD se refiere en ellas a la necesaria ponderación de derechos e intereses que ha de realizarse para implementar una aplicación informática de rastreo de contactos positivos. El punto de partida es obvio: el derecho a la protección de los datos personales no es absoluto, sino que debe equilibrarse con otros derechos y modularse con arreglo al principio de proporcionalidad (considerando 4 RGPD). La protección de datos no puede, además, obstaculizar el desarrollo tecnológico[76]. Para la AEPD, las circunstancias extraordinarias y de emergencia generadas por la pandemia obligaban a la adopción de diversas medidas para poner fin a la gravedad de la situación[77]. Hay, pues, una necesidad de actuación para la protección de la salud y la prevención de los contagios, pero para la AEPD, en este escenario, no resulta imposible «armonizar los

[75] Véase *supra* apartado 4.2.a).

[76] Resolución AEPD SEDIA, p. 211; Resolución AEPD DGSP, p. 166.

[77] Resolución AEPD SEDIA, p. 210; Resolución AEPD DGSP, p. 166.

derechos e intereses de los usuarios, cuya protección exige escasa justificación ante la situación epidemiológica que aconteció»[78].

Esta ponderación de derechos e intereses ya está en buena parte realizada por el legislador e incluida en el RGPD. La normativa sobre protección de datos proporciona algunas reglas especiales relacionadas con el control de epidemias y su propagación, catástrofes naturales y de origen humano (considerando 46, artículos 6.1.e), 6.1.d), 9.2.g) e i) RGPD)[79], que establecen salvaguardas a la protección de los datos personales. Las propias reglas del RGPD ofrecen un cierto margen de discreción a los decisores públicos, pero, en cualquier caso, la flexibilidad no puede llegar hasta actuaciones punto menos que perfunctorias en el respeto de los derechos a la protección de datos personales.

5.2. Rapidez e incertidumbre en la adopción de decisiones

Una situación de emergencia sanitaria exige inmediatez y rapidez en la toma de decisiones. Es por eso por lo que estas se han de adoptar con un alto grado de incertidumbre. Así, por ejemplo, en el ámbito de innovaciones tecnológicas para hacer frente a las consecuencias de una crisis sanitaria, los decisores públicos, si actúan, lo han de hacer sin contar con suficientes conocimientos acerca de la eficacia de la tecnología, de algunas de sus implicaciones éticas y jurídicas y de la disponibilidad de alternativas mejores. Buscar el equilibrio entre la necesidad de actuar de un modo rápido y la minimización de riesgos imprevistos o imprevisibles que la actuación puede comportar constituye uno de los retos más importantes a los que aquellos se enfrentan.

Adoptar decisiones en este marco comporta necesariamente cierta dosis de improvisación y flexibilidad, pero ello no puede convertirse en una patente de corso para poner en marcha tratamientos masivos de datos personales sin una mínima previsión. Hay diferencias de nota entre la improvisación y el apaño.

El Gobierno español actuó rápido, pero no tanto como los de otros estados. La aplicación «Radar COVID» estuvo operativa a partir de la segunda quincena de agosto de 2020, cuando en otros países como Israel o Corea del Sur sus aplicaciones de rastreo de positivos se lanzaron ya en abril de 2020, o como Suiza, que activó su aplicación el 26 de mayo de 2020, poco después de que Google y Apple pusieran en marcha su interfaz para notificaciones de contactos, fruto de su acuerdo de colaboración (*«Google Apple Exposure Notification application programming interface»*). En otros términos, las operaciones de desarrollo e implementación de «Radar COVID» fueron posteriores –o parejas en algunos casos- a las que tuvieron lugar en otros países. Era pues relativamente sencillo poder obtener información acerca de las garantías en materia de protección datos que otros Estados miembros de la UE adoptaban durante el desarrollo de sus aplicaciones de rastreo de positivos.

Las tareas de desarrollo e implementación de «Radar COVID» también tuvieron lugar después de que el Comité Europeo de Protección de Datos (CEPD) y la AEPD se hubieran pronunciado sobre las implicaciones jurídicas que podían comportar los tratamientos de datos realizados por aplicaciones de rastreo y otras herramientas informáticas. En este sentido, en las Directrices

[78] Resolución AEPD SEDIA, p. 192.

[79] Resolución AEPD SEDIA, p. 198.

04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-19, se insiste en la necesidad de reducir los datos objeto del tratamiento a los mínimos estrictamente necesarios «de acuerdo con el principio de minimización de datos, además de cumplir otras medidas de la protección de datos desde el diseño y por defecto» a efectos de «limitar el riesgo de identificación y de rastreo físico de personas»[80].

En efecto, los promotores de «Radar COVID» conocían o podían conocer cómo la AEPD afrontaba los retos que la pandemia planteaba para la protección de datos personales. Además, como se ha indicado, las actuaciones de vigilancia y supervisión de la AEPD sobre los promotores de la aplicación «Radar COVID» se produjeron ya desde que estos anunciaran el proyecto.

También muchos juristas especialistas en protección de datos advirtieron desde los primeros meses de la pandemia sobre los riesgos que planteaban las aplicaciones de rastreo de contactos positivos y sobre las garantías exigidas por el RGPD para salvaguardar los derechos de los interesados[81]. La literatura científica en este ámbito es abundante y una parte sustancial se publicó o se puso a disposición del público poco después de que la Organización Mundial de la Salud declarara el 11 de marzo de 2020 la situación de pandemia global.

Las resoluciones de la AEPD muestran cómo los responsables en el Ministerio de Sanidad y en el Ministerio de Asuntos Económicos y Transformación Digital iniciaron y prosiguieron con el desarrollo de la aplicación «Radar COVID» a espaldas del estado de los conocimientos técnicos y jurídicos disponibles en aquellos momentos. Si bien gradualmente fueron corrigiendo las diferentes deficiencias y adaptando sus comportamientos a las exigencias derivadas del RGPD, resulta sorprendente su actuación inicial, especialmente cuando la mayoría de información era fácilmente accesible.

5.3. Complejidad del entorno institucional y de decisión

Otro de los aspectos que sobresale en las resoluciones de la AEPD es la complejidad del entorno institucional en el cual han de adoptarse las diferentes decisiones necesarias para el desarrollo y funcionamiento de una aplicación para el rastreo de contactos positivos de COVID-19.

La existencia de varios nodos de decisión difumina las responsabilidades y dificulta la identificación de las diferentes esferas de control. Esta difusión afecta tanto a las relaciones internas -las que se dan entre los diferentes intervinientes en el proceso de desarrollo y adopción de la herramienta tecnológica- como a las relaciones externas -las que se dan entre los ciudadanos y los operadores de la aplicación-. En la dimensión interna, la falta de una

[80] Directrices 04/2020, pp. 10-11.

[81] Véanse, entre otros, EDWARDS, Lilian et al., «The Coronavirus (Safeguards) Bill 2020. Proposed protections for digital interventions and in relation to immunity certificates», *LawArXiv*, 2020 [disponible en: https://osf.io/preprints/lawarxiv/yc6xu/ (fecha de consulta: 15.10.2022)]. En España, véanse entre otros, PIÑAR MAÑAS, José Luis, «Transparencia y protección de datos en el estado de alarma y en la sociedad digital post COVID-19», en BLANQUER CRIADO, David, *Covid-19 y Derecho Público (durante el estado de alarma y más allá)*, Tirant lo Blanch, Valencia, 2020, pp. 135-184; MARTÍNEZ MARTÍNEZ, Ricard, «Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública», *Diario La Ley*, vol. 38, núm. 1, 2020 [disponible en: https://diariolaley.laleynext.es/dll/2020/03/27/los-tratamientos-de-datos-personales-en-la-crisis-del-covid-19-un-enfoque-desde-la-salud-publica (fecha de consulta: 15.10.2022)]; y MARTÍNEZ MARTÍNEZ, Ricard, «Covid-19 ¿hacia un rediseño de la privacidad?», *La Ley Privacidad*, núm. 5, 2020.

distribución clara de roles y funciones puede inducir a un decisor a creer que son otros quienes asumen la responsabilidad de comprobar que se está cumpliendo con la normativa de protección de datos. Cuando todos o varios de ellos llegan a la creencia de que los deberes los harán otros, la casa queda sin barrer. En la dimensión externa, la difuminación de responsabilidades dificulta el ejercicio de los derechos de los ciudadanos para proteger sus datos personales frente a los operadores de la aplicación: les priva de saber contra quién actuar, por qué razones y de qué modo.

a) *Dimensión interna*

En la dimensión interna, es cierto que el ordenamiento español prevé mecanismos de delegación de competencias o encomiendas de gestión entre diversos órganos administrativos, pero cuyo resultado es siempre que el delegante conserva la competencia y el delegado se ocupa únicamente de su ejercicio[82]. En el ámbito de la protección de datos, ello conlleva que, a pesar de que haya habido una delegación o encomienda, el órgano administrativo en quien se residencia la titularidad de la competencia no pierde su condición de responsable de los tratamientos de datos personales asociados[83]. En otros términos, el principio de atribución competencial permite una correcta identificación *ex ante* de quién se erige como responsable principal del tratamiento de datos personales asociados con una competencia.

Mas, este enfoque formalista puede enredarse: la complejidad deriva de que delegaciones y encomiendas de gestión pueden comportar que el ejercicio de la competencia por otro órgano administrativo suponga una actuación *de facto* como responsable de los tratamientos de datos personales asociados a esa competencia; o bien suponga una actuación como encargado del tratamiento siguiendo las instrucciones y órdenes del delegante; o finalmente, que se trate de un tercero al que de algún modo se le comuniquen los datos personales tratados. Además, la complejidad se incrementa cuando los órganos delegantes y delegados no están sujetos a una relación de subordinación jerárquica, por ejemplo, porque -como en nuestro caso- forman parte de dos ministerios diferentes. Esta última situación puede invitar a los implicados a descartar que la relación entre ambos sea la que media entre un responsable y un encargado del tratamiento de datos personales.

Las resoluciones de la AEPD ponen de manifiesto que cuando se produce una colaboración interministerial para el desarrollo de proyectos que implican tratamientos de datos personales puede fácilmente darse una situación en la cual sujetos sin una atribución competencial explícita acaben comportándose como responsables de los tratamientos y que, en la práctica, acaben determinando por sí mismos o conjuntamente con el titular de la competencia los medios y los fines esenciales. En otros términos, se produce una extralimitación de su propio ámbito de atribución competencial que comporta dejar de actuar en el rol que por defecto asignaría el RGPD -el de encargado del tratamiento- y asumir el rol de responsable. Esta es la conclusión a la que llega la AEPD en relación con el comportamiento de la SEDIA durante el desarrollo de la aplicación «Radar COVID».

[82] Véanse artículos 8-11 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (BOE núm. 236, de 2.10.2015).

[83] Resolución AEPD SEDIA, p. 172.

Por otra parte, la AEPD, tanto con base en el criterio de atribución competencial como en atención a la actuación de hecho, concluye que la DGSPCI -ahora DGSP- también ostenta la condición de responsable del tratamiento. Según la AEPD fue esta «la que decidió el uso de nuevas tecnologías, en forma de aplicación móvil, como medio de apoyo de la estrategia de identificación y seguimiento de contactos, condicionado el tratamiento y los "medios esenciales"»[84]. En las resoluciones dictadas por la AEPD no se entra a valorar si ambas sancionadas actuaron como responsables independientes del tratamiento o como corresponsables del mismo. No era necesario para la valoración de las infracciones imputadas. Con todo, esta idea según la cual la DGSPCI habría «condicionado» el tratamiento de los datos personales y los medios esenciales para ello recuerda bastante a los criterios desarrollados por el TJUE para identificar supuestos de corresponsabilidad en los cuales un sujeto al utilizar una determina herramienta proporcionada por otro puede influir decisivamente en las operaciones de tratamiento que, de no haber sido por dicha influencia, no habrían ocurrido[85].

b) *Dimensión externa*

La multiplicidad de sujetos implicados en el desarrollo y gestión de la aplicación «Radar COVID» dificulta el ejercicio de los derechos de los interesados reconocidos por el RGPD. Para un sujeto interesado en proteger, por ejemplo, su derecho de acceso a los datos personales tratados por el responsable de la aplicación, la complejidad institucional puede disuadir su ejercicio y menoscabar la tutela otorgada por el RGPD. Si bien el artículo 12.3 LOPDYGDD establece que el encargado podrá tramitar, por cuenta del responsable, las solicitudes de ejercicio formuladas por los afectados de sus derechos, se trata de una solución voluntaria: el encargado dará respuesta a los interesados si así se estableciere en el contrato o acto jurídico que le vincule con el responsable del tratamiento.

Los cambios en la estructura administrativa del Ministerio de Sanidad ocurridos durante la pandemia y, en particular, durante la fase de desarrollo de la aplicación para el rastreo de casos positivos no contribuyeron a mejorar la posición de los usuarios y otros interesados cuyos datos personales pudieran verse afectados.

Finalmente, los problemas en la dimensión externa se ven incrementados por los problemas de falta de transparencia, los múltiples cambios en los diferentes documentos que acompañaban a la aplicación y la aparición de varias noticias en prensa sobre la brecha de seguridad detectada y los riesgos para la protección de los datos personales.

5.4. Una tecnología que no ha funcionado bien

Las resoluciones de la AEPD llegan tarde a la opinión pública. Han pasado casi dos años desde que se iniciara la fase de pruebas de la aplicación «Radar COVID» para que los ciudadanos de este país hayan podido contrastar si esta era o no compatible con el régimen jurídico aplicable a los

[84] Resolución AEPD DGSP, p. 139.

[85] STJUE de 29.7.2019, asunto C-40/17, *Fashion ID*, par. 78-79: «78. […] al insertar tal módulo social en su sitio de Internet, Fashion ID influye de manera decisiva en la recogida y transmisión de datos personales de los visitantes de ese sitio a favor del proveedor de dicho módulo —en el caso de autos, Facebook Ireland— que, de no haberse insertado ese módulo, no habrían tenido lugar. 79. En estas circunstancias, […], debe considerarse que Facebook Ireland y Fashion ID determinan conjuntamente los medios que originan las operaciones de recogida y de comunicación por transmisión de datos personales de los visitantes del sitio de Internet de Fashion ID».

tratamientos de sus datos personales. Y, sobre todo, las resoluciones llegan en un momento en el cual la utilidad y efectividad de las aplicaciones de rastreo de casos positivos habían quedado ya en entredicho.

Las aplicaciones de rastreo de positivos de COVID-19 han fallado en todo el mundo[86]. No únicamente en España encontramos problemas relacionados con la escasa utilización de las aplicaciones de rastreo, con la falta de confianza hacia ellas a partir de las percepciones sobre los riesgos para la privacidad que pueden comportar, o con su eficacia más bien escasa o relativa. También es cierto que los sesgos retrospectivos contribuyen a una valoración crítica: a toro pasado es mucho más fácil ver todo lo que ha fallado.

a) *Utilización escasa de aplicaciones de rastreo*

Las aplicaciones de rastreo han sido escasamente utilizadas. Además, el bajo uso de estas aplicaciones se proyecta sobre todas las modalidades de aplicaciones y no habría sido influido por factores tales como el grado de protección de la privacidad adoptado, el propio diseño tecnológico empleado en la aplicación -por ejemplo, basado en tecnología GPS o Bluetooth-, la arquitectura centralizada o descentralizada del sistema, o las características del proceso de implementación[87]. A pesar de estas diferencias, todas las aplicaciones de rastreo han tenido niveles de uso similares, siempre bajos. La mayoría de países no superaron niveles de uso del 10% de la población[88].

A los factores que condicionan la confianza de los ciudadanos, que examinamos en el subapartado siguiente, hay que añadir las dificultades de acceso a la tecnología por parte de los grupos más vulnerables a la enfermedad. Una parte importante de la población con un mayor riesgo de desarrollar complicaciones derivadas de la COVID-19 -las personas mayores de 80 años- carece de *smartphones* o tiene competencias de uso más limitadas que el usuario medio.

b) *Desconfianza hacia las aplicaciones de rastreo*

El escaso uso de las aplicaciones de rastreo responde, en parte, a problemas de confianza con la tecnología. Los promotores de estas aplicaciones no lograron convencer a sus ciudadanos de la conveniencia de instalar la aplicación en sus teléfonos móviles y de utilizarla y, además, tuvieron que arrostrar obstáculos que fueron surgiendo durante los procesos de desarrollo.

Así, las noticias sobre problemas de seguridad y privacidad que aparecieron en prensa y que se centraron en los riesgos de reidentificación de los sujetos que habían dado positivo en COVID-19 no contribuyeron a una mayor adopción de la tecnología. Si bien los problemas de privacidad son solo uno de los problemas identificados en el desarrollo e implementación de aplicaciones de rastreo[89], la preocupación por una posible vulneración de los derechos a la protección de datos

[86] GIL, Elad D., «Digital Contact Tracing Has Failed: Can it be Fixed with Better Legal Design», *Virginia Journal of Law & Technology*, vol 25, núm. 1, 2021, pp. 1-37, p. 7.

[87] GIL, Elad D., *op. cit.*, p. 7.

[88] GIL, Elad D., *op. cit.*, p. 9. Véase también https://www.coe.int/en/web/data-protection/contact-tracing-apps (fecha de consulta: 15.10.2022).

[89] O'CONNELL, James *et al.*, «Best Practice Guidance for Digital Contact Tracing Apps: A Cross-disciplinary Review of the Literature», *JMIR Mhealth Uhealth*, vol. 9, núm. 6, 2021, pp. 1-23.

personales es seguramente uno de los principales factores que alimenta la desconfianza hacia estas nuevas tecnologías.

Además de la desconfianza generalizada hacia el tratamiento de datos personales llevadas a cabo por parte de las administraciones públicas[90], hay que sumar las suspicacias ante la implicación del sector privado en el desarrollo de las aplicaciones de rastreo. En el caso de «Radar COVID», la participación de grandes empresas como Google, Apple o Amazon puede llevar a las personas a ser más reticentes a descargar la aplicación y a instalarla en sus teléfonos móviles. También las experiencias en otras jurisdicciones, donde se han utilizado sistemas de rastreo y trazabilidad muy intensos y en ocasiones forzados u obligatorios, han despertado otros recelos[91].

Las resoluciones dictadas por la AEPD que comentamos en este trabajo confirman que acaso la desconfianza hacia la aplicación de rastreo «Radar COVID» estaba más que justificada.

c) *Inefectividad de las aplicaciones de rastreo*

Las aplicaciones de rastreo se plantearon como una herramienta que podía contribuir rápidamente a la identificación y aislamiento de casos positivos y evitar medidas más gravosas como confinamientos o restricciones de actividades sociales. En una fase posterior a los primeros confinamientos, las aplicaciones de rastreo debían contribuir a la recuperación económica.

Las aplicaciones de rastreo no han sido una tecnología completamente nueva y, por tanto, una disrupción tecnológica absoluta. Como casi todas las tecnologías, se asienta sobre otras herramientas y factores ya desarrollados en el pasado, que combina para dar lugar a utilidades y funcionalidades novedosas. Así, los sistemas de información geográfica para el tratamiento de epidemias se han venido utilizando al menos desde los años 60[92]. Por otra parte, las operaciones de rastreo son habituales en salud pública para contener y prevenir enfermedades infecciosas. Por último, las tecnologías de GPS y Bluetooth están disponibles desde hace décadas para varios propósitos. De hecho, lo que hacen las aplicaciones informáticas es combinar estos factores, mejorar el rastreo manual y permitir escalarlo fácilmente.

Frente a las ventajas que prometían las aplicaciones de rastreo, pueden indicarse varios elementos que les restan efectividad y fiabilidad. En primer lugar, la efectividad está claramente condicionada por efectos de red: cuantos más usuarios, más efectiva será la aplicación para rastrear casos positivos y advertir a sus usuarios de la necesidad de adoptar medidas de prevención o de realizar nuevas pruebas test. Para un uso efectivo, algunos autores plantearon

[90] Por ejemplo, en relación con la aplicación de rastreo en Reino Unido, se ha señalado que la confianza en el gobierno constituyó un factor clave para la adopción de la app, mientras que su uso prolongado venía más condicionado por percepciones de transparencia. En este sentido, HORVATH, Lazlo *et al.*, «Adoption and continued use of mobile contact tracing technology: multilevel explanations from a three-wave panel survey and linked data», *BMJ Open*, vol. 12, núm. 1, 2022, pp. 1-8.

[91] COTINO HUESO, Lorenzo, «Inteligencia artificial, big data y aplicaciones contra la COVID-19: privacidad y protección de datos», *IDP. Revista de Internet, Derecho y Política*, núm. 31, 2020, p. 9.

[92] KAMEL BOULOS, Maged N./GERAGHTY, Estella M., «Geographical tracking and mapping of coronavirus disease COVID-19/severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) epidemic and associated events around the world: how 21st century GIS technologies are supporting the global fight against outbreaks and epidemics», *International Journal of Health Geographics*, vol. 8, núm. 19, 2020, pp. 1-12., *apud* ROIG BATALLA, Antoni, «Garantías frente a las aplicaciones de rastreo de contagios en situaciones de pandemia», *Teoría y Realidad Constitutional*, núm. 48, 2021, pp. 527-542).

modelos que requerían del rastreo de al menos un 56% de la población[93]. En segundo lugar, la efectividad de las aplicaciones de rastreo como estrategia preventiva depende de que transcurra muy poco tiempo entre un contacto de un usuario con una persona contagiada y la recepción del mensaje acerca de tal contacto de riesgo con un positivo. Esto es, el rastreo de contactos para ordenar una cuarentena no es una medida efectiva salvo en los primeros momentos de transmisibilidad, por lo que la aplicación no ha resultado especialmente efectiva para las finalidades pretendidas por sus promotores. Finalmente, la efectividad también depende de los errores cometidos por la tecnología. Si los niveles de falsos positivos y falsos negativos son relevantes, la fiabilidad de las aplicaciones de rastreo se resiente.

6. Bibliografía

BRADFORD, Laura/ABOY, Mateo/LIDDELL, Kathleen, «COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes», *Journal of Law and the Biosciences*, 2020, pp. 1-21.

ANGIOLINI, Chiara, «Case Law Survey On Data Protection – COVID-19 Litigation Project», *Legal Policy & Pandemics. The Journal of the Global Pandemic Network – LPPJ*, vol. 1, núm. 1-2-3, 2021, pp. 197-224.

COTINO HUESO, Lorenzo, «Inteligencia artificial, big data y aplicaciones contra la COVID-19: privacidad y protección de datos», *IDP. Revista de Internet, Derecho y Política*, núm. 31, 2020, pp. 1-17.

EDWARDS, Lilian *et al*., «The Coronavirus (Safeguards) Bill 2020. Proposed protections for digital interventions and in relation to immunity certificates», *LawArXiv*, 2020.

GIL, Elad D., «Digital Contact Tracing Has Failed: Can it be Fixed with Better Legal Design», *Virginia Journal of Law & Technology*, vol. 25, núm. 1, 2021, pp. 1-37.

GREENLEAF, Graham/KEMP, Katharine, «Australia's "COVIDSafe App": An Experiment in Surveillance, Trust and Law», *University of New South Wales Law Research Series*, vol. 7, 2021, pp. 1-17.

HINCH, Robert *et al.*, «Effective configurations of a digital contact tracing app: a report to NHSX», *GitHub,* 2020.

HORVATH, Lazlo *et al.*, «Adoption and continued use of mobile contact tracing technology: multilevel explanations from a three-wave panel survey and linked data», *BMJ Open*, vol. 12, núm. 1, 2022, pp. 1-8.

KAMEL BOULOS, Maged N./GERAGHTY, Estella M., «Geographical tracking and mapping of coronavirus disease COVID-19/severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) epidemic and associated events around the world: how 21st century GIS technologies are supporting the global fight against outbreaks and epidemics», *International Journal of Health Geographics*, vol. 8, núm. 19, 2020, pp. 1-12.

[93] HINCH, Robert *et al.*, «Effective configurations of a digital contact tracing app: a report to NHSX», *GitHub,* 2020 [disponible en: https://github.com/BDI-pathogens/covid-19_instant_tracing/blob/master/Report%20-%20Effective%20Configurations%20of%20a%20Digital%20Contact%20Tracing%20App.pdf (fecha de consulta: 15.10.2022)].

MARTÍNEZ MARTÍNEZ, Ricard, «Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública», *Diario La Ley*, vol. 38, núm. 1, 2020.

MARTÍNEZ MARTÍNEZ, Ricard, «Covid-19 ¿hacia un rediseño de la privacidad?», *La Ley Privacidad*, núm. 5, 2020.

O'CONNELL, James *et al.*, «Best Practice Guidance for Digital Contact Tracing Apps: A Cross-disciplinary Review of the Literature», *JMIR Mhealth Uhealth*, vol. 9, núm. 6, 2021, pp. 1-23.

PIÑAR MAÑAS, José Luis, «Transparencia y protección de datos en el estado de alarma y en la sociedad digital post COVID-19», en BLANQUER CRIADO, David, *Covid-19 y Derecho Público (durante el estado de alarma y más allá)*, Tirant lo Blanch, Valencia, 2020, pp. 135-184.

POILLOT, Elise *et al*. «Data protection in the context of COVID-19: A short (hi)story of tracing applications», *Roma TrE-Press*, 2021, pp. 1-150.

RAPOSO, Vera Lúcia «"I'm right behind you": Digital contact tracing under European law», *Maastricht Journal of European and Comparative Law*, Agosto 2022.

ROIG BATALLA, Antoni, «Garantías frente a las aplicaciones de rastreo de contagios en situaciones de pandemia», *Teoría y Realidad Constitucional*, núm. 48, 2021, pp. 527-542.

WENDEHORST, Christiane, «COVID-19 Apps and Data Protection», en HONDIUS, Ewoud *et al*., *Coronavirus and the Law in Europe*, Intersentia, Cambridge, 2021, pp. 157-179.

YOO, Christopher S./VIDYARTHI, Apratim, «Privacy in the Age of Contact Tracing: An Analysis of Contact Tracing Apps in Different Statutory and Disease Frameworks», *University of Pennsylvania Journal of Law and Innovation*, vol. 5, 2021, pp. 103-158.