PRIVACIDAD, GEOLOCALIZACIÓN Y APLICACIONES DE RASTREO DE CONTACTOS EN LA ESTRATEGIA DE SALUD PÚBLICA GENERADA POR LA COVID-19

PRIVACY, LOCATION DATA AND CONTACT TRACING APPS IN THE COVID-19 PUBLIC HEALTH STRATEGY

Actualidad Jurídica Iberoamericana Nº 12 bis, mayo 2020, ISSN: 2386-4567, pp. 848-859

Mª Belén
ANDREU
MARTÍNEZ

ARTÍCULO RECIBIDO: 9 de mayo de 2020
ARTÍCULO APROBADO: 10 de mayo de 2020

RESUMEN: La COVID-19 ha puesto de nuevo en primer plano el uso de la tecnología y los datos de los ciudadanos como herramienta de ayuda en el control de la pandemia. Ante el impacto que pueden producir en la privacidad de las personas, en el trabajo se hace referencia a algunas de las herramientas que se han propuesto, planteando las bases legales y condiciones para su implantación.

PALABRAS CLAVE: Clave: privacidad; geolocalización; rastreo contactos; COVID-19

ABSTRACT: *COVID-19 has once again brought to the fore the use of technology and citizen data as a tool for the control of the pandemic. In view of the impact on privacy, this document analyses some of the tools that have been proposed, setting out the legal bases and conditions for their implementation.*

KEY WORDS: *Privacy; location data; contact tracing; COVID-19.*

I. La crisis generada por la COVID-19 ha hecho que la cuestión relativa al lícito tratamiento de los datos de salud de la población y la protección de la privacidad de las personas se haya convertido en un tema de enorme relevancia, hasta el punto de que las distintas autoridades nacionales de protección de datos y las europeas se han tenido que pronunciar en diversas ocasiones y en un tiempo record sobre estas cuestiones.

Como punto de partida es preciso señalar que el RGPD aporta no solo un marco jurídico más específico para el tratamiento de datos de salud (con referencias concretas además al ámbito de la salud pública), sino que también se refiere a la legitimación para el tratamiento en situaciones de crisis sanitaria o pandemia (considerando 46). De manera sucinta, la licitud del tratamiento de datos por parte de las autoridades sanitarias en este tipo de situaciones podría fundamentarse en las bases previstas en los artículos 6.1.d (protección de intereses vitales del interesado o de tercero), 6.1.e (misión realizada en interés público o en el ejercicio de poderes público) y, en el caso de los datos de salud, en el artículo 9.2.c (protección del interés vital del interesado o de un tercero), 9.2.g (tratamiento por razones de interés público esencial) o 9.2.i (tratamiento necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves), además de que ciertas actuaciones puedan fundamentarse en el 9.2.h (prestación de asistencia sanitaria o social) o 9.2.j (investigación científica).

En nuestro país existe un conjunto de normas que regulan la acción de los poderes públicos en materia de salud pública y epidemiología y que pueden, a su vez, constituir la base legal que requieren algunos de los supuestos anteriormente mencionados (en particular, para los arts. 6.1.e, 9.2. g-j). Esto es lo que viene a establecer la disposición adicional 17.1 LOPDGDD, considerando que se encuentran amparados en las letras g) a j) del artículo 9.2 RGPD los tratamientos de datos de salud previstos en distintas leyes, entre otras, la Ley 14/1986, de 25 de abril, General de Sanidad (LGS) y la Ley 33/2011, de 4 de octubre, General de Salud Pública (LGSP). Y, además, legitima la investigación con datos de salud realizada por las autoridades sanitarias con competencias en vigilancia de la salud pública sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública (disp. adic. 17.2.b LOPDGDD; analizada en el informe de la Agencia Española de Protección de Datos –AEPD- 121/2018). Respecto de la estrategia en materia de salud pública, a grandes rasgos ésta se contiene

• Mª Belén Andreu Martínez
Profesora Titular de Derecho civil, Universidad de Murcia. Correo electrónico: beland@um.es

principalmente en la LGSP que establece, entre otros, el deber de colaboración y comunicación (arts. 8 y 9) o la cesión de datos entre administraciones sanitarias cuando sea "estrictamente necesario para" para la tutela de la salud de la población (art. 41). Pero, además, en supuestos de extraordinaria gravedad o urgencia, o de riesgo inminente y extraordinario para la salud, tanto la LGSP (art. 54) como la LGS (arts. 26, 28) prevén la adopción de medidas especiales y, en particular, Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública, las regula específicamente para el control de enfermedades transmisibles (art. 3), cuando lo exijan razones sanitarias de urgencia o necesidad (art. 1), con obligación además de participar por parte del ciudadano (art. 5.2 LGSP).

La existencia de este marco jurídico y la posibilidad de tratamiento de datos de los ciudadanos en situaciones de crisis sanitaria ha sido remarcada también desde un primer momento por autoridades de protección de datos. En este sentido, tanto la AEPD (entre otros, informe 17/2020), como el Supervisor Europeo de Protección de Datos (SEPD, "Statement on the processing of personal data in the context of the COVID-19 outbreak", 19-3-2020) han precisado que la normativa de protección de datos no debía suponer un obstáculo para la lucha contra el coronavirus, pero salvaguardando siempre las reglas establecidas en dicha normativa.

Ahora bien, en la práctica está siendo problemática la aplicación de estas reglas en el uso de soluciones tecnológicas para la lucha contra la pandemia, lo que ha llevado a declaraciones restrictivas sobre su uso y a una gran confusión sobre su eficacia y seguridad.

2. A lo largo de la crisis provocada por el COVID-19 hemos visto cómo han proliferado o se han propuesto distintos tipos de soluciones tecnológicas para el apoyo en la lucha contra la pandemia. Ahora bien, es importante diferenciar entre ellas, pues no todas plantean las mismas cuestiones. LA AEPD ha hecho una primera aproximación en su Documento "El uso de las tecnologías en la lucha contra el COVID-19. Un análisis de costes y beneficios" (mayo 2020), refiriéndose a: geolocalización mediante la tecnología recogida por los operadores de telecomunicaciones; apps, webs y chatbots para auto test y cita previa; geolocalización a través de redes sociales; apps de seguimiento de contactos; pasaportes de inmunidad o cámaras infrarrojas.

En el caso de España, a nivel estatal la Orden SND/297/2020, de 27 de marzo (BOE 28-3-2020) dio entrada a las dos primeras:

A) La realización de un estudio sobre movilidad de las personas en los momentos previos y durante el confinamiento (DataCOVID-19). La finalidad declarada de este estudio (según la Exposición de Motivos) era conocer dichos desplazamientos para ver cómo de dimensionadas estaban las capacidades sanitarias de cada provincia (no se mencionaba entre las finalidades el control del cumplimiento del confinamiento). Este estudio se llevó a cabo por el INE, siguiendo el modelo de otro realizado previamente por este organismo (en noviembre de 2019), e implica el cruce de datos de las operadoras de comunicaciones electrónicas móviles, de forma anonimizada y agregada.

La Orden señala que en su ejecución se "velará" por el cumplimiento del RGPD y la LOPDGDD; ahora bien, una vez llevada a cabo la anonimización, sobre la "información anónima" resultante en la que se basa el estudio a priori no sería aplicable la normativa de protección de datos (considerando 26 RGPD). Por otra parte, a pesar de la base legal que la Orden cita para justificar las actividades que en él se proponen, el estudio se hace únicamente con aquellas operadoras con las que se llegue a acuerdo. No se dice nada, en cambio, sobre la posibilidad de los ciudadanos de oponerse a que sus datos puedan ser utilizados para la realización de este estudio (sí se permitió por algunas operadoras en el estudio llevado a cabo en noviembre). Sin entrar ahora en el tema de si el ciudadano debe disponer o no, en general, de esta facultad, lo cierto es que la fundamentación y finalidades del tratamiento en este caso, vinculadas a la gestión de una crisis sanitaria por parte de las autoridades, junto con el deber de participación del ciudadano en estos casos que establece la legislación en salud pública, justificarían esta solución.

B) El desarrollo de un chatbot para proporcionar información oficial ante preguntas de la ciudadanía, una web informativa con los recursos tecnológicos disponibles y una aplicación informática para la gestión de la crisis que incluye la posibilidad de auto diagnóstico e información sobre el COVID-19 (consejos prácticos, recomendaciones de acciones). La aplicación permitiría la geolocalización del individuo a los solos efectos de verificar que se encuentra en la CCAA que declara estar.

Partiendo de las bases legítimas del artículo 6 y 9 del RGPD señaladas en el punto 1, el marco legal que fundamentaría la adopción de estas medidas, conforme a la Exposición de Motivos de la Orden, sería la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública y, en particular, su artículo 3 (que permite 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). Pero también la propia normativa de declaración del estado de alarma (en particular, el art. 4 del Real Decreto 463/2020, de 14 de marzo, por

el que se declara el estado de alarma y que permite a las autoridades competentes delegadas, dictar las órdenes, resoluciones, etc. en su esfera de competencia para la protección de bienes, personas y lugares, mediante la adopción de cualquier de las medidas previstas en el artículo 11 LO 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio).

Teniendo en cuenta el tipo de medidas que se prevén, que no son altamente intrusivas en la privacidad (información oficial al ciudadano, estudio de movilidad basado en información anónima y agregada, aplicación de instalación voluntaria para autodiagnóstico e información), el marco legal señalado permitiría justificar su adopción (se ha defendido que superaría el juicio de ponderación requerido por el TEDH, R. Martínez, "Protección de datos y geolocalización en la Orden SND/297/2020", Hay Derecho. Expansión, 31-3-2020). Podría plantear dudas la geolocalización de las personas (que en este caso se limita a un control de movilidad y/o confinamiento entre Comunidades Autónomas y que podría establecerse como una opción voluntaria en la app). Y también si dichas medidas necesitan para su adopción de la existencia de un estado de alarma o es suficiente el marco legal de medidas especiales en salud pública (Ley Orgánica 3/1986) y el rango normativo que precisa la determinación de la finalidad y garantías adecuadas del tratamiento. Sobre esto volveremos más adelante.

3. En una fase de desconfinamiento de la población, el objetivo se está centrando, no obstante, en la rápida detección de los casos positivos, para que se pueda detener la cadena de transmisión. Y es aquí donde han entrado en juego con gran fuerza las aplicaciones de rastreo de contactos. El seguimiento de contactos es una técnica conocida en epidemiología (a través de entrevistas), pero la imposibilidad de hacer un seguimiento "manual" o "analógico" ante el elevado número de contagiados por el COVID-19 ha planteado el uso de medios tecnológicos. En este sentido, distintos países en Europa han lanzado ya alguna aplicación con esta finalidad o han anunciado que lo harán próximamente. Por lo que la protección de la privacidad de las personas se ha situado en el centro del debate, sobre todo a la vista de los precedentes de aplicación de este tipo de control en China, Corea del Sur o Singapur (puede verse una comparativa de distintas aplicaciones a nivel mundial en el proyecto "Covid Tracing Tracker", MIT Technology Review).

A priori cabrían varias alternativas: acudir a la localización o ubicación de la persona (utilizando GPS o los datos de posición de los abonados mediante la triangulación por las antenas de telefonía que realizan los operadores de telecomunicaciones para la prestación del servicio); o realizar un seguimiento de proximidad a través de tecnología como el Bluetooth (modelo Singapur). Este último no implica uso

de localización, sino que se generan unos códigos o pseudónimos encriptados que se intercambian (a través de Bluetooth) los teléfonos que tienen instalada la aplicación cuando se dan ciertas condiciones de proximidad (por distancia y tiempo de proximidad), conforme a la previa definición que se haya establecido de "contacto" a efectos de contagio de la enfermedad. En caso de positivo, se podría generar una alerta a los "contactos" de los 14 días anteriores. A su vez, dentro de estos se suele hablar de centralizados (ej., Robert) o descentralizados (ej., DP-3T), según el modo en que se genere el "código" y la alerta a los contactos (control por una autoridad central o por el usuario). Por su parte, Google y Apple también están desarrollando una API conjunta, que permita que los teléfonos iOS y Android se comuniquen entre sí a través de Bluetooth, y que podrá ser utilizada por las aplicaciones que creen las autoridades sanitarias.

De entre los múltiples pronunciamientos que se han producido acerca de estas aplicaciones, vamos a destacar dos: la Comunicación de la Comisión europea "Orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de COVID-19 en lo referente a la protección de datos", de 17-4-2020 (2020/C 124 I/01); y las Directrices del SEPD ("Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak"), de 21-4-2020.

La Comisión europea considera a las aplicaciones relacionadas con la COVID-19 un elemento importante en la lucha contra la pandemia (incluso más que otras medidas, como el confinamiento, para interrumpir la cadena de transmisión), sobre todo en la estrategia de salida y como complemento a otras medidas. Conscientes del recelo que provocan, ambas autoridades destacan la necesidad de la aceptación social de estas soluciones, de generar confianza en los ciudadanos y del respeto a sus derechos fundamentales.

Para ello, se plantea en cualquier caso la voluntariedad en la instalación de estas aplicaciones y la "desactivación" una vez la pandemia esté controlada, entre las medidas para garantizar que el ciudadano tenga el control de sus datos. En este sentido, el SEPD señala que un monitoreo sistemático de la localización de una persona y/o de sus contactos constituye una injerencia importante en su privacidad. Por lo que solo se puede legitimar si se basa en su consentimiento a cada una de las finalidades (precisa también la Comisión europea la importancia de no agrupar finalidades y poder consentirlas por separado) y no sufre ningún perjuicio si la rechaza.

Por otra parte, ambas instituciones destacan la importancia de que estas aplicaciones se utilicen como parte de la estrategia de salud pública. En este sentido, se recomienda que el responsable del tratamiento sea la correspondiente

autoridad sanitaria nacional, debiendo estar claro el rol y responsabilidad de otros actores que puedan intervenir.

Constituye éste un elemento fundamental, en la medida en que la información que se proporcione a través de estas aplicaciones debe estar contextualizada en el correspondiente escenario de salud pública nacional y, además, la información que se genere debe utilizarse en beneficio del sistema de salud. En este sentido, se señala que la confirmación del diagnóstico de infectado y su notificación a contactos debe ser resultado de una evaluación realizada por la autoridad pública. Igualmente la determinación, por ejemplo, de qué es un contacto. Por otra parte, dadas las limitaciones de los sistemas tecnológicos de rastreo de contactos (al depender su eficacia del número de descargas, posibles "falsos positivos" de contactos, uso malicioso por el usuario…), es importante que se utilice como apoyo al trabajo que realizan los equipos de "rastreo manual".

Asimismo, no pueden utilizarse este tipo de soluciones tecnológicas para una vigilancia masiva de la población. Señala el SEPD que, conforme al principio de limitación de finalidad, debe estar especificada dicha finalidad, eliminándose otros posibles usos (comerciales, policiales, etc.), que no estén relacionados con la gestión del COVID-19.

Ambas autoridades claramente apuestan por los sistemas de rastreo de contactos por proximidad (Bluetooth) y no por el seguimiento de los movimientos individualizados de las personas (localización de la persona). Apunta, en este sentido, el SEPD los principios de minimización, privacidad por diseño y por defecto; principios que justificarían también que el funcionamiento de estas aplicaciones se realice sin identificación del usuario (y estableciendo medidas para evitar la reidentificación), la información se almacene en el terminal/dispositivo, se recolecte solo cuando fuera necesario (confirmación de contagio), a lo que se podría añadir, como medida de control del usuario, que la persona debe consentir la compartición de los datos que se recabaron en su dispositivo (para generar la alerta). Ambas autoridades aceptan tanto los sistemas centralizados, como los descentralizados. Si bien, se inclinan más bien por estos últimos, al considerarlos más adaptadas a los principios de protección de datos (entre ellos, minimización).

Una cuestión relevante es la relativa a la base legal para el tratamiento de los datos. Aunque la instalación de la aplicación sea voluntaria y se base, por tanto, en el consentimiento, el tratamiento de los datos que se recaben con ella no tienen por qué tener dicha base. De hecho, ambas instituciones señalan otras bases de legitimación más adecuadas en el caso de datos tratados por las autoridades sanitarias: las previstas en los artículos, 6.1.c y e RGPD; y, tratándose de datos de salud, el art. 9.1.i RGPD (aunque también apunta el SEPD la posibilidad de acudir según el caso a las bases establecidas en el art. 9.1.a y h RGPD, esto es,

consentimiento explícito y prestación de asistencia sanitaria). En cualquier caso, lo relevante es que, salvo que la base para el tratamiento sea el consentimiento (en cuyo caso, éste debe cumplir los requisitos para su validez, arts. 4.11 y 7 RGPD), en los restantes supuestos, como ya hemos señalado anteriormente, la base legítima debe estar establecida en el derecho de la UE o del Estado miembro y, además, incorporar medidas adecuadas y específicas para proteger los derechos y libertades del interesado (art. 9.2.i, cuando implique tratamiento de datos de salud), y, en el caso de los arts. 6.1.c y e, cumplir con los requisitos del artículo 6.3 RGPD.

La Comisión europea señala que tanto la legislación previa al COVID-19, como la que se está promulgando para luchar contra la pandemia podría usarse como base jurídica para el tratamiento, siempre que en ella se prevean medidas que autoricen el seguimiento de epidemias y se cumplan los demás requisitos del artículo 6.3 RGPD. El SEPD indica incluso que, entre las salvaguardas significativas, se incluiría una referencia a la naturaleza voluntaria de la aplicación; además, una clara especificación de la finalidad y limitaciones explícitas con respecto al uso posterior de los datos personales, así como una identificación clara de los responsables involucrados; categorías de datos, así como las entidades (y los propósitos para los cuales se pueden divulgar los datos personales). También recomienda incluir, tan pronto como sea posible, los criterios para determinar cuándo se desmantelará la solicitud y qué entidad será responsable de tomar esa determinación. Se requiere, por tanto, una concreta previsión normativa que recoja estas especificaciones acerca de la aplicación.

Como hemos señalado anteriormente, en nuestro país contamos con una primera base de legitimación en la LO 3/1986, que prevé la posibilidad de adoptar medidas para el control de enfermedades transmisibles, así como la finalidad y necesidad de estas medidas para el ejercicio de la potestad pública, en este caso, la protección de la salud pública, ante el riesgo para la salud de la población, y el control de enfermedades transmisibles, en situaciones de urgencia o necesidad (arts. 1-3). Ciertamente la LO está pensando en medidas dirigidas a personas o grupos de personas concretas y no a la población en general, pero, en cualquier caso, la instalación de una aplicación de rastreo de contactos sería voluntaria (a diferencia del carácter compulsivo de las medidas que prevé esta norma). Lo que no se prevé en ella es un detalle de las disposiciones específicas (art. 6.3 RGPD) o salvaguardas significativas señaladas por el SEPD. Para ello se puede acudir a la propia normativa de prórroga del estado de alarma (aunque esto supone vincular esta medida al propio estado de alarma y su subsistencia).

En cualquier caso, las indicaciones de la Comisión europea y del SEPD acerca de las aplicaciones de rastreo de contactos pueden servir de guía a la

hora de abordar una estrategia de incorporación de las mismas por parte de las autoridades sanitarias, que debe estar basada necesariamente en los principios de privacidad por diseño y por defecto (art. 25 RGPD, minimización de datos, limitación de finalidad, del plazo de conservación…). Esto requiere, no obstante, clarificar previamente aspectos como su eficacia o seguridad. No está claro que los sistemas descentralizados por los que parecen decantarse las instituciones europeas sean más seguros o garanticen la no identificación del usuario (V. Botti, "Rastreen mi móvil… y háganlo bien, Innovadores. La Razón, 6-5-2020). Tampoco la utilidad, al ser voluntaria su instalación (experiencias en otros países como Singapur o Noruega reflejan que solo entre un 10% y 15% de la población proceden a instalarla).

4. Frente a los sistemas de proximidad, el uso de la localización de la persona plantea cuestiones adicionales, al contar con un régimen específico bastante estricto, recogido en la Directiva 2002/58/CE sobre privacidad y comunicaciones electrónicas. En concreto, el artículo 6 se refiere a los datos de tráfico (que incluye la etiqueta de localización o identificador de celda desde la que se activó el servicio), que deben eliminarse o anonimizarse cuando ya no sean necesarios para llevar a cabo la transmisión, pudiendo ser tratados únicamente los necesarios para la facturación y cobro del servicio. Y el artículo 9, referido a datos de localización, distintos de los de tráfico, que solo pueden tratarse previa anonimización o con el consentimiento de la persona para la prestación de servicios de valor añadido. El artículo 15 de la Directiva permite, no obstante, limitar los derechos y obligaciones previstos, entre otros, en los artículos 6 y 9, cuando dicha limitación constituya una medida necesaria proporcionada y apropiada por lo motivos establecidos en dicho precepto (seguridad nacional, seguridad pública, prevención de delitos…; con base en esta excepción se dictó de hecho la polémica Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas).

A la vista de lo anterior, para el SEPD la posibilidad de acceso a estos datos por parte de las autoridades sanitarias, a día de hoy, pasa por la anonimización de estos datos (o, en el caso de datos de localización, distintos de los de tráfico, por el previo consentimiento de la persona). En este sentido, ha enfatizado la preferencia por el uso de datos anonimizados, en lugar de datos personales, en el caso de que se opte por acudir a datos de localización a efectos del control de la epidemia (aunque el propio SEPD pone de relieve la dificultad de la anonimización en estos casos).

Por su parte, la AEPD (en su Comunicado sobre apps y webs de autoevaluación del Coronavirus, de 26-3-2020) dio entrada a la posibilidad de geolocalizar a través del teléfono móvil a personas que han dado positivo en COVID-19, con base en

"las amplias competencias que en situaciones excepcionales, como sin duda lo es la presente epidemia, tienen las autoridades sanitarias, teniendo en cuenta, además, que una de las medidas excepcionales para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 es la de limitar la libertad de circulación de las personas". Por tanto, aunque sin citarla expresamente, se basaba en la normativa especial en materia de salud pública (en particular, LO 3/1986), pero aludía también a la vinculada al estado de alarma, en cuanto limita la libertad de circulación. Y ello porque para la AEPD nos encontraríamos ante una obligación impuesta por las autoridades sanitarias para evitar la propagación del virus y que requiere el "control de las personas contagiadas y que han sido obligadas a permanecer en su domicilio en cuarentena". Ciertamente las limitaciones de circulación asociadas al estado de alarma ayudan a justificar una medida como la geolocalización para el control de dicha cuarentena, pero la LO 3/1986 permite adoptar medidas de "control de enfermos" referidas a sujeto concretos o grupos de personas.

Posteriormente, en la Nota técnica para el uso de las tecnologías en la lucha contra el COVID-19 (mayo 2020), la AEPD ha precisado que la información de ubicación de la que disponen los operadores de telecomunicaciones puede ser demandada, sin anonimizar, por las fuerzas y cuerpos de seguridad del estado, previa orden judicial, y anonimizada para hacer estudios de movilidad. Apunta, no obstante, como derivada la posibilidad de que se usen "datos anonimizados de geolocalización para observar movimientos globales, pero con la posibilidad de que la policía pidiera la reidentificación en determinados casos conforme a los criterios establecidos por las autoridades sanitarias para garantizar el control de la epidemia". Parece que se deja abierta la puerta a un posible uso de datos de localización (no anonimizados), pero no se detalla en qué supuestos y se echa mano de la policía, cuando su habilitación, conforme a la Ley 25/2007, es para la persecución de delitos graves (arts. 1 y 6).

Como vemos, la posición de las autoridades de control es bastante restrictiva en cuanto al uso de los datos de localización. Se ha defendido la posibilidad de acudir a la excepción prevista en el art. 15 Directiva 2002/58/CE, junto con la normativa nacional que habilita para la adopción de medidas especiales en materia de salud pública para el control de enfermedades transmisibles, con la única finalidad de localización de los posibles sujetos contagiados y, en último extremo, la ubicación del paciente (R. Martínez, "Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública", Diario La Ley, nº 9604, 30-3-2020). Si bien, una cuestión fundamental que habrá que resolver es la relativa a la determinación de las garantías adecuadas para la protección del derecho fundamental a la protección de datos de los ciudadanos y la norma o normas en las que estas garantías se establecen, en conexión con la reserva de

ley (art. 53.1 CE) y la doctrina relativamente exigente del TC al respecto (SSTC 292/2000; 76/2019, aunque ésta última referida a datos especialmente protegidos).