

PROTECCIÓN DE DATOS PERSONALES EN EL CONTEXTO DE LA COVID-19: LEGITIMACIÓN EN EL TRATAMIENTO DE DATOS DE SALUD POR LAS ADMINISTRACIONES PÚBLICAS

Juan Francisco Rodríguez Ayuso*

Resumen

El presente estudio ofrece una investigación sistemática, exhaustiva y actualizada de la declaración del estado de alarma y el tratamiento de datos personales relativos a la salud de los ciudadanos afectados y/o potencialmente afectados por la situación excepcional derivada de la COVID-19. En concreto, analiza la distinción del estado de alarma con los estados de excepción y sitio, y la posible afectación del derecho fundamental a la protección de datos personales en situaciones excepcionales de crisis sanitarias y los efectos que dicha declaración puede tener en la normativa aplicable, emanada, a nivel comunitario, por el Reglamento general de protección de datos o RGPD y, a nivel nacional, como complemento y desarrollo del mismo, en la Ley Orgánica de Protección de Datos Personales y de garantía de los derechos digitales o LOPDGDD. Seguidamente, y tomando en consideración toda la normativa, general y sectorial, aplicable en materia de protección de datos y de sanidad, se procede al análisis de las bases legitimadoras procedentes y de las excepciones que, aplicables a situaciones de emergencia sanitaria como la actual, habilitan el tratamiento atendiendo a la naturaleza de quien intervenga como responsable, haciendo especial énfasis en el interés público perseguido por las Administraciones públicas y en el interés vital del propio interesado.

Palabras clave: dato personal; datos de salud; tratamiento de datos; COVID-19; RGPD; Administraciones públicas; autoridades sanitarias; bases de legitimación.

PERSONAL DATA PROTECTION IN THE COVID-19 CONTEXT: LEGITIMATION IN HEALTH DATA PROCESSING BY PUBLIC AUTHORITIES

Abstract

This study offers a thorough, systematic, up-to-date analysis of the declaration of the State of Alert and the processing of personal data concerning the health of people affected and/or potentially affected by the exceptional situation stemming from COVID-19. Specifically, it analyses the distinction between the state of alert and the states of exception and siege, and the possible effect on the fundamental right to personal data protection in the exceptional circumstances of health crises, as well as the effects said declaration could have on applicable legislation stemming, on a European level, from the General Data Protection Regulation (GDPR) and, on a Spanish level, supplementing and developing the GDPR, the Organic Law on Personal Data Protection and Guarantees for Digital Rights (LOPDGDD). Then, taking into account both general and sectoral legislation applicable to health and data protection, the study proceeds to analyse the legitimate bases and exceptions applicable to health emergency situations like the current one which enable data processing – bearing in mind the nature of the controller – placing special emphasis on the public interest pursued by the public administrations and the vital interest of the person concerned.

Key words: personal data; health data; data processing; COVID-19; GDPR; public administrations; health authorities; legitimate bases.

* Juan Francisco Rodríguez Ayuso, profesor ayudante doctor y coordinador académico del Máster universitario en protección de datos. Universidad Internacional de La Rioja (UNIR), av. de la Paz, 137, 26006 Logroño (La Rioja). juanfrancisco.rodriguez@unir.net

Artículo recibido el 09.04.2020.

Citación recomendada: Rodríguez Ayuso, Juan Francisco. (2020). Protección de datos personales en el contexto de la COVID-19: legitimación en el tratamiento de datos de salud por las Administraciones públicas. *Revista Catalana de Dret Públic*, (número especial), 137-152. <https://doi.org/10.2436/rcdp.i0.2020.3449>.

Sumario

- 1 Estado de alarma ante situaciones excepcionales de crisis sanitarias
- 2 Salud y protección de datos personales
 - 2.1 Consentimiento del interesado
 - 2.2 Cumplimiento de una obligación legal aplicable al responsable del tratamiento
 - 2.3 Interés vital del interesado o de otra persona física
 - 2.4 Interés público
- 3 Tratamientos que no requieren la identificación del titular de los datos como manifestación del principio de minimización de datos
- 4 Conclusiones
- 5 Referencias bibliográficas

1 Estado de alarma ante situaciones excepcionales de crisis sanitarias

El presente estudio de investigación podría comenzar con una frase, tantas veces repetida, que adquiere especial intensidad en nuestros días: “ante situaciones excepcionales, medidas excepcionales”.

En efecto, como resultado del potente efecto globalizador propio de la sociedad de la información en la que nos hallamos plenamente inmersos, asistimos en la actualidad a un complejo escenario de emergencia sanitaria, hasta hace unos meses inimaginable, que ha puesto progresivamente en jaque el entramado político, institucional, económico, ético y sanitario de los Estados (Ministerio de Sanidad, 2020) y que está llamado a transformar, casi definitivamente, el comportamiento relacional de los individuos y del entorno en el que se desenvuelven.

La COVID-19, excepcional en sus efectos más adversos, exige la adopción de medidas extraordinarias que permitan acabar o, cuanto menos, minorar el ya más que elevado número de víctimas. En este punto, el ordenamiento jurídico debe articularse del modo más preciso y riguroso posible para permitir, sin resultar mermado, dar acertada respuesta a las aspiraciones propias de todo ser humano en orden a la preservación del más alto valor humano que da razón y sirve de sustento al resto: la vida (Martínez, 2020).

A tal fin, la labor de todo jurista e investigador debe ser la de conseguir, con pretensiones honestas y circunscritas, por ende, a su ámbito de estudio, encontrar, de forma escalonada y suficientemente motivada, el sustento normativo que permita alcanzar tan excelso objetivo. En lo que aquí respecta, este análisis busca ahondar, desde una perspectiva teleológica, en el modo en el que la protección de datos personales (especialmente de categorías especiales, como son los datos de salud), como derecho fundamental pero no absoluto que es, debe articularse para no obstaculizar la plena efectividad de las medidas que adopten las autoridades sanitarias en el ya declarado estado de alarma.¹

El artículo 116.1 de la Constitución española² (en adelante, CE) establece que una ley orgánica regulará los estados de alarma, de excepción y de sitio, así como las competencias y limitaciones correspondientes.³ Al amparo de esta previsión, surge la Ley Orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio⁴ (en adelante, LOEAES), cuyo capítulo II (artículos 4 a 12) regula el estado de alarma, plenamente justificado para situaciones, como la actual, provocada por “[c]risis sanitarias, tales como epidemias y situaciones de contaminación graves” [artículo 4.b) LOEAES]. Entre las medidas que puede llegar a comportar, las indicadas en el artículo 11 LOEAES, además del deber de colaboración, que, siguiendo la previsión del artículo 30.4 CE, se recoge en el artículo 7 bis de la Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil.⁵

El estado de alarma (artículo 116.2 CE):

“[...] será declarado por el Gobierno mediante decreto acordado en Consejo de Ministros por un plazo máximo de quince días, dando cuenta al Congreso de los Diputados, reunido inmediatamente al efecto y sin cuya autorización no podrá ser prorrogado dicho plazo”.

Así ha sido. Constatada la expansión del coronavirus en nuestro país, el Gobierno ha promulgado, con aplicación en todo el territorio nacional, el Real Decreto 463/2020, de 14 de marzo, por el que se declara

1 Sobre el carácter limitado y necesariamente ponderable de los derechos fundamentales, *vid.* Sentencias del Tribunal Constitucional núm. 11/1981, de 08/04/1981, FJ 7.º y 10.º; 2/1982, de 29/01/1982, FJ 5.º; 62/1982, de 15/10/1982, FJ 5.º; 110/1984, de 26/11/1984, FJ 5.º; 13/1985, de 31/01/1985, FJ 2.º; 53/1986, de 05/05/1986, FJ 3.º; 196/1987, de 11/12/1987, FJ 4.º, 5.º y 6.º; 197/1987, de 11/12/1987, FJ 11.º; 37/1989, de 15/02/1989, FJ 7.º; y 120/1990, de 27/06/1990, FJ 5.º.

2 *Boletín Oficial del Estado* (en adelante, BOE) núm. 311, de 29/12/1978.

3 Recuérdese que, de acuerdo con el artículo 81.1 CE, corresponde a las leyes orgánicas el desarrollo de los derechos fundamentales y de las libertades públicas, las que aprueben los estatutos de autonomía y el régimen electoral general y las demás previstas en la Constitución.

4 BOE núm. 134, de 05/06/1981.

5 BOE núm. 164, de 10/07/2015.

el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19^{6 y 7} (en adelante, RDDEA), que se ha visto acompañado con la aprobación de numerosas disposiciones en todos los niveles territoriales (Minero, 2020)⁸ encaminadas a hacer frente al impacto ocasionado por la pandemia. La duración inicial del estado de alarma es de quince días (que se extiende desde la entrada en vigor del Real Decreto en el BOE —14 de marzo— y hasta quince días después —28 de marzo—, tal y como establecen el artículo 3 y la disposición final tercera), si bien ha sido objeto de sucesivas prórrogas merced, primero, al Real Decreto 476/2020, de 27 de marzo, por el que se prorroga el estado de alarma declarado por el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19,⁹ después, al Real Decreto 487/2020, de 10 de abril, por el que se prorroga el estado de alarma declarado por el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19,¹⁰ y al Real Decreto 492/2020, de 24 de abril, por el que se prorroga el estado de alarma declarado por el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19.¹¹ En cuanto a las medidas previstas, estas quedan recogidas en los artículos 7 a 19 RDDEA.

La declaración del estado de alarma no supone, en ningún caso, ni expresa ni tácitamente, la suspensión del derecho fundamental a la protección de datos; es más, tan solo supone la adopción de determinadas medidas que traen consigo la limitación, que no suspensión, en el ejercicio de determinados derechos y libertades (Piñar, 2020). Cosa distinta sucede con el estado de excepción o de sitio, que, a tenor del artículo 55.1 CE, sí que comportaría la suspensión de los derechos reconocidos en los artículos 17; 18.2 y 3; 19; 20.1, *a*) y *d*), y 5; 21; 28.2, y 37.2 CE. El derecho fundamental a la protección de datos personales emana del artículo 18.1 CE,¹² precepto que no se encuentra recogido en el elenco anterior y que nos permite concluir de forma taxativa que ni en el estado de alarma, ni en el estado de excepción ni en el estado de sitio podrán adoptarse medidas que supongan una suspensión, ni siquiera mínima, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE¹³ (en adelante, Reglamento general de protección de datos o RGPD), de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales¹⁴ (en adelante, LOPDGDD) ni de cualquier otra normativa conexas, que seguirán siendo aplicables en toda su integridad.¹⁵

6 BOE núm. 67, de 14/03/2020.

7 En España, el único precedente lo encontramos en el Real Decreto 1673/2010, de 4 de diciembre, por el que se declara el estado de alarma para la normalización del servicio público esencial del transporte aéreo (BOE núm. 295, de 04/12/2010), promulgado con objeto de garantizar el derecho de todos los españoles a la libre circulación por todo el territorio nacional, tras las circunstancias extraordinarias acaecidas tras el cierre del espacio aéreo español como consecuencia de la situación desencadenada por el abandono de sus obligaciones por parte de los controladores civiles de tránsito aéreo.

8 Se puede consultar, de forma actualizada, el conjunto de disposiciones aplicables en relación con la crisis sanitaria de la COVID-19 en el siguiente enlace: https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=355_Crisis_Sanitaria_COVID-19&tipo=C&modo=2.

9 BOE núm. 86, de 28 de marzo de 2020.

10 BOE núm. 101, de 11 abril de 2020, precedido de la Resolución de 9 de abril de 2020, del Congreso de los Diputados, por la que se ordena la publicación del Acuerdo de autorización de la prórroga del estado de alarma declarado por el Real Decreto 463/2020, de 14 de marzo, y que se extiende hasta el 26 de abril de 2020.

11 BOE núm. 115, de 25 de abril de 2020.

12 Así lo declaró la Sentencia del Tribunal Constitucional (Pleno) núm. 292/2000, de 30/11/2000.

13 *Diario Oficial de la Unión Europea* L 119/1, de 05/05/2016.

14 BOE núm. 294, de 06/12/2018.

15 Debe tenerse en cuenta que, merced a la disposición derogatoria única de la LOPDGDD, se deroga la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD —BOE núm. 298, de 14/12/1999—), el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos (BOE núm. 183, de 30/07/2018), y cuantas disposiciones de igual o inferior rango contradigan, se opongan o resulten incompatibles con lo dispuesto en el RGPD. De este modo, y así lo ha ratificado, entre otros, la Autoridad

Cuestión distinta es que sea necesario amoldar este derecho fundamental para, en palabras de la Agencia Española de Protección de Datos (en adelante, AEPD), “[...] permitir legítimamente los tratamientos de datos personales en situaciones, como la presente, en que existe una emergencia sanitaria de alcance general” (AEPD, 2020). Así lo ha reiterado, a nivel comunitario y de forma prácticamente simultánea, el Comité Europeo de Protección de Datos, quien subraya que, en absoluto, el respeto a la privacidad de los interesados ni al derecho que la sustenta puede suponer un escollo en la toma de decisiones que impliquen el uso de datos personales para atajar la pandemia actual, incluso cuando estemos hablando de datos sensibles, como son los datos relativos a la salud de las personas (EDPB, 2020).

2 Salud y protección de datos personales

Llegados a este punto, y a la vista de la (relevante) conclusión anterior respecto del encuadre y enfoque constitucional del derecho fundamental a la protección de datos, el siguiente paso reside en articular el posible tratamiento, por parte de las Administraciones públicas (a nivel público) y de las empresas (a nivel privado), de información personal de los ciudadanos como medida de control, prevención y solución de esta situación de emergencia sanitaria de alcance general.

Un primer aspecto, no exento de debate, reside precisamente en determinar quién puede intervenir en este contexto como responsable del tratamiento, entendido este como “[...] la persona física o jurídica, autoridad pública, servicio u otro organismo que, sólo o junto con otros, determine los fines y medios del tratamiento”. Para poder responder a esta cuestión, necesitamos saber cuáles son las finalidades para las cuales se van a tratar los datos y quién determina estas finalidades, y los medios para poder alcanzarlas.

En relación con la primera cuestión, parece evidente que todas las finalidades deberán estar relacionadas directamente con el control del virus y, por ende, con la salvaguarda de la vida de las personas físicas, ya sean identificadas o identificables, que, en cuanto titulares de los datos, tendrán la consideración de interesados [artículo 4.1) RGPD].

Por tanto, la clave está en determinar quién debe alcanzar la consecución de estas finalidades e implementar, en su correspondiente ámbito de actuación, los instrumentos necesarios para su obtención. A mi juicio, y pese a la opinión contraria de organismos tan procedentes y relevantes como las autoridades de control italiana (GPDP, 2020) y francesa (CNIL, 2020), considero que el RGPD habilita plenamente en estos casos tanto a las Administraciones públicas (personificadas en el Ministerio de Sanidad o el Instituto Nacional de Estadística) como a las empresas privadas a tratar, en su condición de responsables del tratamiento, datos personales de personas infectadas o susceptibles de llegar a estarlo con el fin de evitar la propagación del coronavirus y procurar la defensa de sus vidas (Marzo, 2020). Ninguna interpretación distinta de la anterior consideraría coherente con el espíritu de la norma, cual es, repito, atender a una medida excepcional como la actual, con recursos limitados, donde todos tenemos la obligación de colaborar y donde es preciso defender la privacidad de los ciudadanos, sí, pero sin que ello suponga, de manera alguna, una merma de su integridad física, ya que, huelga decirlo, difícilmente podremos garantizar la privacidad de quien no vive para disfrutarla.

Un segundo elemento vendrá determinado por la naturaleza de los datos personales a tratar con ocasión de esta crisis sanitaria, que, en su mayor parte, se encuadrarán dentro de lo que se conoce como *categorías especiales de datos personales* (artículo 9 RGPD).¹⁶ En concreto, y en lo que aquí interesa, serán datos relativos a la salud

Catalana de Protección de Datos (<https://apdcat.gencat.cat/es/documentacio/preguntes-frequents/Entrada-en-vigor-del-Reglament-general-de-proteccio-de-dades-i-LOPDGDD>), sigue en vigor el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante, RDLOPD —BOE núm. 17, de 19/01/2008—), en todo aquello que no se oponga o resulte incompatible con el RGPD y la LOPDGDD.

¹⁶ Dentro de este artículo quedarían incluidos todos aquellos datos personales que, de un modo más palpable o con efectos más evidentes, inciden en la esfera privada de los interesados, como son aquellos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical o el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida u orientación sexual del

“[...] aquellos 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].

Un primer estadio en el análisis de la licitud del tratamiento de datos personales relativos a la salud de sus titulares nos lleva a las bases jurídicas del artículo 6.1 RGPD. Y es que, contrariamente a lo que pudiera pensarse, será preciso, primero, establecer si concurre alguna justificación de las previstas en la normativa para determinar si el tratamiento es lícito como condición *sine qua non* para, solo después, determinar si, además, existe alguna circunstancia excepcional del artículo 9.2 RGPD que permita superar la regla general que prohíbe tratar datos especialmente protegidos;¹⁷ algo que, *a priori*, parece contrario con el fin último de tratamientos de esta naturaleza, alineados con el valor constitucional fundamental de garantizar la vida, la salud y la dignidad humanas, y muy alejado, por ende, de todo fin discriminatorio inspirador de la prohibición del artículo 9.1 RGPD.

No obstante, para un mejor entendimiento de cuanto se expone, parece más didáctico o clarificador exponerlas conjuntamente, estableciendo la concordancia de cada una de las bases jurídicas habilitantes con su correspondiente excepción.

2.1 Consentimiento del interesado

La noción de consentimiento encierra una de las más relevantes novedades que trae consigo el nuevo marco regulador sobre protección de datos. Así, mientras que la normativa anterior entendía por *consentimiento* toda manifestación de voluntad libre, específica e informada, mediante la que el interesado consentía el tratamiento de sus datos personales [artículo 2.h) Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos],¹⁸ el RGPD se refiere al consentimiento como toda manifestación de voluntad, libre, específica, informada e inequívoca, por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de sus datos personales [artículo 4.11) RGPD]; de este modo, incorpora el adjetivo *inequívoco* y, aún más relevante, introduce la obligación de que el consentimiento se exteriorice mediante una declaración o una clara acción afirmativa.

Siguiendo el orden que marca la normativa (que no predispone prelación alguna, pues todas cumplen el mismo fin y lo hacen en la misma medida), hemos de acudir al consentimiento del interesado como base jurídica para el tratamiento de sus datos personales [artículos 6.1.a) RGPD y 6 LOPDGDD], consentimiento que deberá ser explícito para poder superar la prohibición general del tratamiento de datos de salud [artículo 9.2.a) RGPD].

Con fecha de 27 de marzo, el Ministerio de Sanidad ha promulgado la Orden SND/297/2020, de 27 de marzo, por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de diversas actuaciones para la gestión de la

interesado. Al respecto y por lo que respecta al tratamiento de datos de salud en este contexto, *vid.* Comité de Bioética de España, *Informe del Comité de Bioética de España sobre los requisitos ético-legales en la investigación con datos de salud y muestras biológicas en el marco de la pandemia de COVID-19*, 2020; European Data Protection Board, *Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak*, 2020.

17 En este punto, discrepo con Minero Alejandro, G., cuando sostiene que “[...] cuando hablamos de datos de la salud, al tratarse de una categoría especial de datos, el precepto aplicable para identificar las bases jurídicas del tratamiento de estos datos no es el artículo 6 del RGPD, sino una norma de protección reforzada, el artículo 9 del RGPD, que prevé una serie de circunstancias que permiten no aplicar la regla general del tratamiento basado en el consentimiento del interesado”. En primer lugar, y así lo ha establecido la AEPD (2016), *Guía para el cumplimiento del deber de informar*, porque el consentimiento no es la regla general que permite el tratamiento, sino una regla más de todas las existentes o, tanto más, la causa residual, aplicable únicamente “[...] cuando la legitimación para la finalidad principal no encuentre acomodo en ninguna de las bases jurídicas anteriores”. En segundo lugar, porque, tal y como reitera la propia AEPD en su Informe 0017/2020, las bases jurídicas del artículo 6 RGPD deberán concurrir siempre, ya que son las que permiten cumplir el principio de licitud del tratamiento [artículo 5.1.a) RGPD]; si, además, concurren datos sensibles, tendremos que buscar salvar la prohibición general del tratamiento que establece el artículo 9 RGPD, que actuará como una especie de segundo requisito o exigencia adicional pero que, en ningún caso, podrá sustituir o reemplazar la concurrencia de una base legal.

18 *Diario Oficial de las Comunidades Europeas* L 281/31, de 23/11/1995.

crisis sanitaria ocasionada por el COVID-19,¹⁹ desarrollando diversas actuaciones que persiguen contribuir a mejorar la gestión de la crisis.²⁰ Entre estas actuaciones, esta orden prevé el desarrollo de soluciones tecnológicas y aplicaciones móviles para la recopilación de datos con el fin de mejorar la eficiencia operativa de los servicios sanitarios, así como conseguir la mejor atención y accesibilidad por parte de los ciudadanos.

En concreto, establece la necesidad de implementar una aplicación informática que permitirá realizar al usuario la autoevaluación, con base en los síntomas médicos que comunique, de la probabilidad de que esté infectado por la COVID-19, ofrecerle información al respecto y proporcionarle consejos prácticos y recomendaciones a seguir según la evaluación, además de posibilitarle la geolocalización para verificar que se encuentra donde declara estar (Martínez, 2020). Estas funcionalidades serán voluntarias, de modo que todo interesado que quiera someterse a ellas habrá de prestar su consentimiento explícito. El responsable del tratamiento será el Ministerio de Sanidad, y el encargado del tratamiento, la Secretaría General de Administración Digital (artículos 28 RGPD y 33 LOPDGDD).

También prevé el desarrollo de un asistente conversacional o *chatbot* para ser utilizado mediante aplicaciones de mensajería instantánea y que proporcionará información oficial, siendo necesario, igualmente, el consentimiento de quien plantee las dudas o consultas relacionadas con la crisis sanitaria. El responsable del tratamiento será el Ministerio de Sanidad, y el encargado del tratamiento será la Secretaría de Estado de Digitalización e Inteligencia Artificial mediante la Subdirección General de Inteligencia Artificial y Tecnologías Habilitadoras Digitales.

Ya en el ámbito privado, también se están produciendo iniciativas tecnológicas que tienen por finalidad el seguimiento de contactos para identificar y alertar a las personas que han estado en contacto con alguien infectado por coronavirus, y que se harán depender del consentimiento de los interesados. Es el caso, entre otras, de la solución conjunta llevada a cabo por Apple y Google.²¹

También podrán verse amparadas en el consentimiento del interesado las investigaciones científicas que, sobre datos personales de salud de los interesados, pueden implementarse para luchar contra la pandemia. Así lo establece, al amparo del artículo 9.2.j) RGPD, la disposición adicional decimoséptima, apartado 2.a), LOPDGDD. Este precepto comunitario permite el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89.1 RGPD, sobre la base del derecho nacional o comunitario, que deberá ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

19 BOE núm. 86, de 28/03/2020.

20 Esta orden acoge el mandato emanado de la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública (en adelante, LMESP —BOE núm. 102, de 29/04/1986—), modificada mediante Real Decreto-ley 6/2020, de 10 de marzo, por el que se adoptan determinadas medidas urgentes en el ámbito económico y para la protección de la salud pública (BOE núm. 62, de 11/03/2020); del RDDEA, y de la Orden SND/234/2020, de 15 de marzo, sobre adopción de disposiciones y medidas de contención y remisión de información al Ministerio de Sanidad ante la situación de crisis sanitaria ocasionada por el COVID-19 (BOE núm. 68, de 15/03/2020), modificada por la Orden SND/267/2020, de 20 de marzo, por la que se modifica la Orden SND/234/2020, de 15 de marzo, sobre adopción de disposiciones y medidas de contención y remisión de información al Ministerio de Sanidad ante la situación de crisis sanitaria ocasionada por el COVID-19 (BOE núm. 78, de 21/03/2020).

21 No obstante, hay autores como Cotino Hueso —“Inteligencia Artificial y vigilancia digital contra el COVID-19 y contra la privacidad. El diablo está en los detalles”, en *Instituto Español de Estudios Estratégicos*, núm. 36, 2020— que sostienen que, en estos casos, puede no proceder el consentimiento como base jurídica. En concreto, el referido autor establece lo siguiente: “[o]tro detalle no poco importante es la voluntariedad de estas aplicaciones. De momento, en España y la UE (y el sistema PEPP-PT), así como Google y Apple, hablan de voluntariedad. Pero lo cierto es que jurídicamente el consentimiento, por lo general, no vale cuando se trata de los poderes públicos teniendo en cuenta el artículo 7.4.º RPDG (Informe 185/2018 AEPD). Y, en ningún caso, sería un consentimiento válido si el uso de la app es condición para el acceso a zonas de la ciudad, transporte, servicios sociales, sanitarios, etc. Y siendo realistas, si estas aplicaciones son voluntarias y no se utilizan por casi toda la población, podrían llegar a ser inútiles para sus finalidades. De ahí la necesidad de legitimar legalmente su uso”.

2.2 Cumplimiento de una obligación legal aplicable al responsable del tratamiento

Una segunda base jurídica que concurre en los datos de salud en el contexto de la COVID-19 es la necesidad del tratamiento para el cumplimiento de obligaciones del responsable del tratamiento (el empleador) o el ejercicio de derechos específicos del interesado en el ámbito del derecho laboral y de la seguridad y protección social [artículos 6.1.c) y 9.2.b) y h) y 9.3, ambos del RGPD, y 8 LOPDGDD].²²

De acuerdo con el artículo 6.1.c) RGPD, será legítimo el tratamiento de datos con el fin de cumplir una obligación legal aplicable al responsable del tratamiento. Esta previsión encuentra continuidad, en el caso analizado, en el artículo 9.2, letras b) (que alude al tratamiento para el cumplimiento de obligaciones y el ejercicio de derechos específicos en el ámbito del derecho laboral y de la seguridad y protección social) y h) (que, en el ámbito específico sanitario, regula el tratamiento para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del derecho nacional o comunitario o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el artículo 9.3 RGPD),²³ este último apartado dispone que los datos de salud podrán ser tratados cuando el tratamiento (por ejemplo, controles de temperatura, test PCR, test de anticuerpos, etc.) sea realizado por un profesional sujeto a la obligación de secreto profesional (artículo 5 LOPDGDD) o bajo su responsabilidad o por cualquier otra persona sujeta también a la obligación de secreto, habilitando, pues, la realización, por empresas de seguridad privada (en virtud del artículo 31.10 de la Orden INT/318/2011, de 1 de febrero, sobre personal de seguridad privada),²⁴ de pruebas a los trabajadores de la empresa en el marco de la prevención del riesgo de contagio del virus.

En este caso, el empresario tiene un deber de protección de los trabajadores frente a los riesgos laborales, motivo por el que deberá garantizar la seguridad y salud de todos los que estén a su servicio en los aspectos relacionados con el trabajo. Así lo imponen el artículo 20 del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores²⁵ (en adelante, ET), y los artículos 2.1 y 14 y siguientes de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales (en adelante, LPRL). Centrados en el tratamiento específico de datos de salud, y merced a la habilitación prevista en la disposición adicional decimoséptima LOPDGDD,²⁶ también resultará aplicable el artículo 33 de la Ley 33/2011, de 4 de octubre, General de Salud Pública (en adelante, LGSP),²⁷ que regula la actuación sanitaria de forma coordinada con los empresarios y los representantes de los trabajadores.

Por su parte, el artículo 21.c), al igual que el artículo 29 LPRL (que transpone el artículo 13 de la Directiva del Consejo, de 12 de junio de 1989, relativa a la aplicación de medidas para promover la mejora de la seguridad y de la salud de los trabajadores en el trabajo),²⁸ hace recaer en el empleado una serie de obligaciones en materia de prevención de riesgos laborales. Más concretamente, le obliga a:

“[...] informar de inmediato a su superior jerárquico directo, y a los trabajadores designados para realizar actividades de protección y de prevención o, en su caso, al servicio de prevención, acerca de cualquier situación que, a su juicio, entrañe, por motivos razonables, un riesgo para la seguridad y la salud de los trabajadores; contribuir al cumplimiento de las obligaciones establecidas por la autoridad competente con el fin de proteger la seguridad y la salud de los trabajadores en el trabajo y cooperar con el empresario para que éste pueda garantizar unas condiciones de trabajo que sean seguras y no entrañen riesgos para la

22 Agencia Española de Protección de Datos, *Informe del Gabinete Jurídico núm. 0017/2020*. En la misma línea, Agencia Española de Protección de Datos, *Comunicado de la AEPD sobre apps y webs de autoevaluación del Coronavirus, 2020*.

23 BOE núm. 42, de 18/02/2011.

24 BOE núm. 42, de 18/02/2011

25 BOE núm. 255, de 24/10/2015.

26 Esta disposición adicional ampara en las letras g), h), i) y j) RGPD los tratamientos de datos relacionados con la salud y de datos genéticos que estén regulados en las leyes y disposiciones de desarrollo en ella contempladas.

27 BOE núm. 240, de 05/10/2011.

28 BOE núm. 240, de 05/10/2011.

seguridad y la salud de los trabajadores. En el ámbito de la situación actual derivada del COVID-19 ello supone que el trabajador deberá informar a su empleador en caso de sospecha de contacto con el virus, a fin de salvaguardar, además de su propia salud, la de los demás trabajadores del centro de trabajo, para que se puedan adoptar las medidas oportunas”.²⁹

2.3 Interés vital del interesado o de otra persona física

De acuerdo con el considerando 46 RGPD:

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

Sobre esta base, surgen los artículos 6.1.d) y 9.2.c), ambos del RGPD, que aluden a la necesidad del tratamiento por parte de las Administraciones públicas cuando sea preciso para proteger intereses vitales del interesado o de otra persona física, si bien el último de ellos exige, además, que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento. En este caso, no tendrá que ampararse en norma alguna de carácter nacional o comunitario [a diferencia de las letras c) y e) del artículo 6.1 RGPD], pues así lo establece el artículo 6.3 RGPD.

Esta extensión del tratamiento a terceros supone, en palabras de la propia AEPD, que “[...] dicha base jurídica del tratamiento (el interés vital) puede ser suficiente para los tratamientos de datos personales dirigidos a proteger a todas aquellas personas susceptibles de ser contagiadas en la propagación de una epidemia, lo que justificaría, desde el punto de vista de tratamiento de datos personales, en la manera más amplia posible, las medidas adoptadas a dicho fin, incluso aunque se dirijan a proteger personas innominadas o en principio no identificadas o identificables, por cuanto los intereses vitales de dichas personas físicas habrán de ser salvaguardados”.³⁰

2.4 Interés público

Además del considerando anterior, conviene añadir, a este supuesto de legitimación, el considerando 54 RGPD, que establece que:

“El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas. En ese contexto, ‘salud pública’ debe interpretarse en la definición del Reglamento (CE) n.º 1338/2008 del Parlamento Europeo y del Consejo, es decir, todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad. Este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines”.

En consecuencia, deberemos aludir a los artículos 6.1.e) y 9.2.g) e i), todos ellos del RGPD, y 8 LOPDGDD, respaldados, además, por la precitada disposición adicional decimoséptima. El primero alude al cumplimiento

29 Agencia Española de Protección de Datos, *Informe del Gabinete Jurídico* núm. 0017/2020.

30 Agencia Española de Protección de Datos, *Informe del Gabinete Jurídico* núm. 0017/2020.

de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos a las Administraciones públicas en su condición de responsables del tratamiento, mientras que el segundo, en sendas letras y haciéndose eco de esta previsión, alude, respectivamente, al tratamiento por razones de un interés público esencial (propias de la urgencia derivada del coronavirus) y al tratamiento por razones de interés público en el ámbito de la salud pública (característica de la crisis sanitaria actual).

En estos casos, será necesario contar con una base normativa que ampare estos tratamientos y que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado. Pues bien, esta normativa emana:

- En primer lugar, de los artículos 1 a 3 LMESP, que aluden a las actuaciones desarrolladas por los poderes públicos, a fin de controlar las enfermedades transmisibles, sobre los enfermos y quienes estén o hayan estado en contacto con ellos.
- En segundo lugar, del artículo 26 de la Ley 14/1986, de 25 de abril, General de Sanidad,³¹ que atribuye competencias a los servicios sanitarios ante la existencia de un riesgo inminente y extraordinario para la salud.
- En tercer lugar, ligado también con el tratamiento de datos de salud, del artículo 7 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica,³² que establece el derecho de toda persona a que se respete la confidencialidad de sus datos de salud y a que nadie pueda acceder a ellos sin previa autorización legal.
- En cuarto lugar, de los artículos 10.3 y 55.1.j) de la Ley 18/2009, de 22 de octubre, de salud pública,³³ que, de una parte, regulan la obligación de las Administraciones públicas, de los organismos competentes en materia de salud pública y de los centros, servicios y establecimientos y los profesionales sanitarios, de participar en el Sistema de Formación e Investigación en Salud Pública y en el Sistema de Información de Salud Pública, y, de otra, su capacidad para adoptar medidas de reconocimiento médico, tratamiento, hospitalización o control si hay indicios racionales de la existencia de peligro para la salud de las personas.
- En quinto y último lugar, de los artículos 5 y 9 LGSP, que establecen el derecho y el deber de todas las personas de participar de forma efectiva en las actuaciones de salud pública y de comunicar aquello que pudiera constituir un riesgo o peligro grave para la salud, respectivamente. La colaboración con los servicios competentes resulta esencial para el logro de los objetivos del Real Decreto 2210/1995, de 28 de diciembre, por el que se crea la red nacional de vigilancia epidemiológica.³⁴

De este modo, y conjugando esta base de legitimación con la dispuesta en la letra anterior, aludimos al tratamiento de datos de salud de personas físicas cuando “[...] por indicación de las autoridades sanitarias competentes, sea necesario comunicar a otras personas con las que dicha persona física ha estado en contacto la circunstancia del contagio de esta, para salvaguardar tanto a dichas personas físicas de la posibilidad de contagio (intereses vitales de las mismas) cuanto para evitar que dichas personas físicas, por desconocimiento de su contacto con un contagiado, puedan expandir la enfermedad a otros terceros (intereses vitales de terceros e interés público esencial y/o cualificado en el ámbito de la salud pública)”.³⁵

Por último, también podrá ampararse en la base jurídica del artículo 6.1.e) RGPD la realización, por las Administraciones públicas, de investigaciones científicas en materia de salud y en la lucha contra el coronavirus,

31 BOE núm. 102, de 29/04/1986.

32 BOE núm. 274, de 15/11/2002.

33 BOE núm. 276, de 16/11/2009.

34 BOE núm. 21, de 24/01/1996.

35 Agencia Española de Protección de Datos, *Informe del Gabinete Jurídico núm. 0017/2020*.

sobre la base de la excepción situada en el artículo 9.2.j) RGPD y al amparo de lo dispuesto por la letra b) del apartado 2 de la disposición adicional decimoséptima LOPDGD (European Data Protection Board, 2020).³⁶

De conformidad con el considerando 159 RGPD:

“El presente Reglamento también debe aplicarse al tratamiento de datos personales que se realice con fines de investigación científica. El tratamiento de datos personales con fines de investigación científica debe interpretarse, a efectos del presente Reglamento, de manera amplia, que incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado. Además, debe tener en cuenta el objetivo de la Unión establecido en el artículo 179, apartado 1, del TFUE de realizar un espacio europeo de investigación. Entre los fines de investigación científica también se deben incluir los estudios realizados en interés público en el ámbito de la salud pública. Para cumplir las especificidades del tratamiento de datos personales con fines de investigación científica deben aplicarse condiciones específicas, en particular en lo que se refiere a la publicación o la comunicación de otro modo de datos personales en el contexto de fines de investigación científica. Si el resultado de la investigación científica, en particular en el ámbito de la salud, justifica otras medidas en beneficio del interesado, las normas generales del presente Reglamento deben aplicarse teniendo en cuenta tales medidas”.

A su vez, el Grupo de Trabajo del Artículo 29 añadió que el ámbito de investigaciones de esta naturaleza no puede extenderse más allá de su significado común, aunque entiende que el término *investigación científica* en este contexto alude a proyectos de investigación establecidos de conformidad con las normas metodológicas y éticas pertinentes relacionadas con el sector, de conformidad con las buenas prácticas. En este sentido, el artículo 89 RGPD contiene un apartado primero que establece la necesidad de que este tipo de tratamiento se vea acompañado de la adopción de garantías adecuadas en forma de medidas técnicas y organizativas acordes al riesgo elevado que normalmente conlleva el manejo de información sensible de los individuos. Como podemos observar, la normativa no obstaculiza la implementación de medidas adoptadas en la lucha contra la pandemia de COVID-19, siendo un instrumento legislativo amplio que prevé varias disposiciones que permiten manejar el procesamiento de datos personales a efectos de la investigación científica relacionada con la pandemia, en cumplimiento de los derechos fundamentales a la privacidad y a la protección de los datos personales (European Data Protection Board, 2020).

La letra b) de la disposición adicional decimoséptima permite al responsable del tratamiento, cuando este sea un grupo de investigación (no solo de naturaleza pública), realizar estudios científicos sin necesidad (a diferencia del supuesto precedente) de contar con el consentimiento del interesado, siempre que la excepcionalidad, relevancia y gravedad de la situación para la salud pública así lo aconsejen. Es este supuesto el que, precisamente, legitimará la investigación científica que podrá llevarse a cabo para corregir los efectos propios del coronavirus, toda vez que las especiales circunstancias derivadas de esta pandemia así lo justifican.

A este respecto, resultan fundamentales las recientes conclusiones aportadas por el Comité de Bioética de España (2020), que establecen lo siguiente:

“[...] con carácter general, el uso secundario de los datos de salud y muestras biológicas se somete a un régimen muy estricto, al tratarse de datos especialmente protegidos. Por ello, tal uso secundario, distinto de aquél para el que fue recabado el dato o tomada la muestra (véase, asistencia sanitaria) en circunstancias de normalidad, exigiría la autorización expresa de los pacientes y, en su caso, representantes legales.

36 De acuerdo con este organismo, cuando se habla de tratamiento de datos de salud con fines de investigación científica hay dos tipos de usos de los datos: la investigación de datos personales (sobre la salud), que consiste en el uso de datos recogidos directamente con fines de estudios científicos (uso primario), y la investigación sobre datos personales (de salud), que consiste en el tratamiento ulterior de datos inicialmente reunidos para otro fin (uso secundario). Como ejemplo del primer caso, menciona aquel en el que, para la realización de un ensayo clínico con personas sospechosas de estar infectadas por la COVID-19, se reúnen datos sanitarios y se utilizan cuestionarios; del segundo, aquel en el que un sujeto de datos ha consultado a un proveedor de atención de la salud en calidad de paciente en relación con los síntomas del SARS-CoV-2, de modo que, si los datos sanitarios registrados por el proveedor de atención de la salud se utilizan posteriormente con fines de investigación científica, ese uso se clasifica como tratamiento ulterior de los datos sanitarios (uso secundario) que se han reunido con otro propósito inicial. Esta distinción entre la investigación científica basada en el uso primario o secundario de los datos sobre la salud, concluye el Supervisor Europeo de Protección de Datos, será especialmente importante cuando se aluda a la base jurídica del tratamiento, a las obligaciones de información y al principio de limitación de la finalidad.

Sin embargo, tal regla general encuentra excepciones en nuestro ordenamiento jurídico, lo que permite el uso secundario sin necesidad de recabar un nuevo consentimiento *ad hoc* o incluso sin contar con un consentimiento amplio (*broad consent*) en el que se haya autorizado el uso de los datos y muestras para otros fines y en relación con líneas de investigación vinculadas a la enfermedad que provocó la asistencia sanitaria y recabar tales datos y muestras.

[...] Así pues, en situaciones de excepcional relevancia y gravedad para la salud pública, contexto que evidentemente concurre en el momento actual, se autorizan dos tipos de actuaciones. Por un lado, las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo estudios científicos sin el consentimiento de los afectados e incluso manteniéndose los datos de identificación del sujeto fuente (DA 17.^a 2.b)”.

3 Tratamientos que no requieren la identificación del titular de los datos como manifestación del principio de minimización de datos

El RGPD contempla expresamente aquellos supuestos en los que, para la consecución de los fines del tratamiento perseguidos por el responsable o, bajo sus instrucciones, del encargado del tratamiento, no es necesario conocer la identidad del interesado en cuanto titular de los datos personales. En concreto, el considerando 57 de la norma dispone, de un modo literal, cuanto se indica a continuación:

“Si los datos personales tratados por un responsable no le permiten identificar a una persona física, el responsable no debe estar obligado a obtener información adicional para identificar al interesado con la única finalidad de cumplir cualquier disposición del presente Reglamento. No obstante, el responsable del tratamiento no debe negarse a recibir información adicional facilitada por el interesado a fin de respaldarle en el ejercicio de sus derechos. La identificación debe incluir la identificación digital de un interesado, por ejemplo, mediante un mecanismo de autenticación, como las mismas credenciales empleadas por el interesado para abrir una sesión en el servicio en línea ofrecido por el responsable”.

Al amparo de este considerando, surge el artículo 11 RGPD, que, clasificando en dos apartados claramente diferenciados el contenido del párrafo precedente, sostiene de forma clara lo siguiente:

“1. Si los fines para los cuales un responsable trata datos personales no requieren o ya no requieren la identificación de un interesado por el responsable, este no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir el presente Reglamento.

2. Cuando, en los casos a que se refiere el apartado 1 del presente artículo, el responsable sea capaz de demostrar que no está en condiciones de identificar al interesado, le informará en consecuencia, de ser posible. En tales casos no se aplicarán los artículos 15 a 20, excepto cuando el interesado, a efectos del ejercicio de sus derechos en virtud de dichos artículos, facilite información adicional que permita su identificación”.

De una lectura sosegada del precepto anterior podemos extraer tres conclusiones básicas que exponemos a continuación.

En primer lugar, y aunque pueda parecer lo mismo, que no es así, el apartado primero del *supra* citado artículo exonera al responsable del tratamiento de la obligación de asumir cargas adicionales con vistas a cumplir la normativa (entiéndase, en esencia, RGPD y LOPDGDD). En cambio, el apartado segundo impone al interesado un deber de actuación con el fin de poder ejercitar los derechos que legítimamente puedan llegar a corresponderle de los previstos, no solo en los artículos 15 a 22 RGPD y 13 a 18 LOPDGDD (acceso, rectificación, supresión, limitación del tratamiento, portabilidad de los datos y a no ser objeto de decisiones individuales automatizadas, incluida la elaboración de perfiles), sino también en los artículos 77 a 79 RGPD (que regulan, respectivamente, el derecho del titular de los datos a presentar una reclamación ante una autoridad de control,³⁷ el derecho a la tutela judicial efectiva contra una autoridad de control y el derecho a la

37 En nuestro país, la AEPD tendrá la condición de representante común de las autoridades de protección de datos del Reino de España en el CEPD (artículo 44.2 LOPDGDD). Para un estudio más pormenorizado de las autoridades de control, vid. Rodríguez Ayuso, Juan Francisco. (2020). *Control externo de los obligados por el tratamiento de datos personales*. Barcelona: Bosch.

tutela judicial efectiva contra un responsable o encargado del tratamiento); en concreto, le exige renunciar al secreto o confidencialidad de su identidad, ya que, hasta el momento en que lo haga, no dejará de ser una persona física *identificable*, pero no *identificada*.

De acuerdo con el artículo 4.1) RGPD, será dato personal cualquier información sobre una persona física (que tendrá la consideración de *interesado* a los efectos de la normativa comunitaria en materia de protección de datos) identificada o identificable. A su vez, esta misma letra define qué se entiende por *persona física identificable*, aludiendo a aquella cuya identidad pueda determinarse, ya sea de forma directa o indirecta, “[...] 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”, siendo este un elenco *numerus apertus*, no *numerus clausus*.

Ahora bien, aun cuando el responsable del tratamiento no esté obligado a implementar estas medidas, ciertamente voluntarias o proactivas, dirigidas a la identificación del interesado, sí que tendrá la obligación de no oponerse o negarse a actuar cuando sea el titular de los datos personales quien, voluntariamente y con la intención de hacer valer sus derechos, remita la información adicional que, en su caso, resulte necesaria para su identificación ante el responsable del tratamiento. Así lo confirma el apartado segundo del artículo 12 RGPD, precepto que regula el deber de información al que ha de atender el responsable del tratamiento para dar adecuado cumplimiento a la transparencia en su actuación como parte integrante del —más amplio— principio de licitud, lealtad y transparencia regulado en el artículo 5.1.a) RGPD.

En segundo lugar, dentro del artículo 11.1 RGPD podemos, a su vez, establecer una distinción entre dos supuestos: a) aquel en el que los fines perseguidos por el responsable del tratamiento *no requieren* la identificación del interesado, en cuyo caso este no estará obligado a *obtener*³⁸ (pues nunca llegó a disponer de ella) información adicional para identificar al interesado con el fin de que este pueda ejercitar, llegado el caso, los derechos que le corresponden, y b) aquel otro en el que los objetivos que el responsable del tratamiento pretende alcanzar *ya no requieren* conocer la identidad del titular de los datos personales objeto de tratamiento, donde no será preciso *mantener* (pues ya dispone de ella) aquella información personal que permite la identificación de este.

En tercer y último lugar, resulta necesario prestar atención a uno de esos que se conocen como *conceptos jurídicos indeterminados*, entendidos como aquellos elementos que se contienen en una norma jurídica y que solo pueden reconocerse o explicarse de manera abstracta o genérica.³⁹ Nos estamos refiriendo, en lo que aquí interesa, al término *información adicional*, que ostenta un papel fundamental en la plasmación práctica del contenido del artículo 11 RGPD, habida cuenta de que —parece evidente— será preciso que el responsable del tratamiento, aun no teniendo la obligación de obtener o mantener esta información adicional, sí que deberá concretar, con carácter previo, aquella que habrá de proporcionar el interesado para poder identificarse y ejercitar los derechos que, en su caso, le correspondan (Puyol, 2016).

38 En mi opinión, el artículo 11 RGPD incurre en una tautología del término *tratar* que no induce sino confusión en el lector, toda vez que da a entender que la obtención, el mantenimiento y el tratamiento de los datos personales son operaciones distintas, cuando, en realidad, tanto la obtención como el mantenimiento son operaciones que se insertan dentro de una categoría más amplia o general: la del tratamiento propiamente dicho. Así puede deducirse del artículo 4.2) RGPD, que define el *tratamiento* como “[c]ualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción”.

39 Para un análisis más preciso o exhaustivo del significado y alcance de los conceptos jurídicos indeterminados, *vid.* Dei Cas, B., “El concepto jurídico indeterminado como límite de la discrecionalidad”, en *Revista de Derecho*, núm. 14, 2008, p. 71-86, y García de Enterría Martínez-Carande, E., “Una nota sobre el interés general como concepto jurídico indeterminado”, en *Revista española de Derecho Administrativo*, núm. 89, 1996, p. 69-89.

4 Conclusiones

A lo largo del presente estudio hemos podido concluir que la declaración del estado de alarma como consecuencia de la crisis sanitaria actual derivada de la COVID-19 no supone, ni directa ni indirectamente, la suspensión del derecho fundamental a la protección de datos, aun cuando sí que trae consigo la implementación de determinadas actuaciones que pueden llegar a limitarlo. Resulta necesario, por tanto, determinar las bases jurídicas que permiten que los tratamientos de datos implementados, tanto por organismos públicos como por empresas privadas, sean lícitos.

Así, entre las causas de legitimación que, habiendo de ser combinadas con las excepciones propias y precisas para levantar la prohibición general en el tratamiento de datos de salud de los interesados, resultan aplicables, se encuentran fundamentalmente las siguientes:

- En primer lugar, el consentimiento del propio interesado, que, experimentando una renovación ciertamente más exigente con la nueva normativa en materia de protección de datos, permite el tratamiento para: a) el desarrollo de soluciones tecnológicas y aplicaciones móviles que, sobre la base de la autoevaluación del propio titular de los datos, permiten que estos sean recopilados con el fin de mejorar la eficiencia operativa de los servicios sanitarios, así como la mejor atención y accesibilidad por parte de los ciudadanos, ofreciéndoles información y proporcionándoles consejos prácticos y recomendaciones a seguir según la evaluación, además de posibilitarles la geolocalización para verificar que se encuentran donde declaran estar; b) el seguimiento de contactos para identificar y alertar a las personas que han estado en contacto con alguien infectado por coronavirus, y c) la realización de investigaciones científicas que, sobre datos personales de salud de los interesados, pueden implementarse para luchar contra la pandemia.
- En segundo lugar, el cumplimiento de una obligación legal aplicable al responsable del tratamiento, que, derivada de la normativa en materia de prevención de riesgos laborales, habilita a las empresas a realizar controles a los empleados para garantizar la seguridad del entorno de trabajo. Esta obligación, de doble vertiente, impele igualmente a los trabajadores a informar de inmediato a su superior jerárquico directo de cualquier situación que pueda entrañar un riesgo para la seguridad y la salud de los demás compañeros.
- En tercer lugar, el interés vital del afectado por la enfermedad del coronavirus o de un tercero, siempre que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento. Esta extensión del tratamiento a terceros comporta que la legitimación pueda ser suficiente cuando el tratamiento se dirija también a proteger a aquellas personas susceptibles de ser contagiadas en la propagación de la epidemia.
- En cuarto y último lugar, el interés público perseguido por el responsable del tratamiento, donde será necesario disponer de una base normativa (numerosa y enumerada en estas páginas) que ampare estos tratamientos y que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado. En este supuesto se encontraría: de un lado, el tratamiento de datos de salud de interesados cuando sea necesario comunicar a otros individuos con los que dicha persona física ha estado en contacto la circunstancia del contagio, para salvaguardarlas del mismo e impedir que estas, por desconocimiento de su contacto con un contagiado, puedan expandir la enfermedad a otros terceros, y, de otro, la realización de estudios científicos sin necesidad de contar con el consentimiento del titular de los datos, siempre que la excepcionalidad, relevancia y gravedad de la situación para la salud pública así lo aconsejen, como sucederá con aquellas investigaciones científicas que podrán llevarse a cabo para corregir los efectos propios de la COVID-19, toda vez que las especiales circunstancias derivadas de esta pandemia así lo justifican.

Finalmente, hemos analizado, como expresión del principio de minimización de datos, aquellos tratamientos de datos personales que no requerirán la identificación del interesado, a fin de procurar cumplir más satisfactoriamente el principio de responsabilidad proactiva que demanda el RGPD. En estos casos, si los fines para los cuales el responsable trata datos personales no requieren o ya no requieren la identificación del interesado,

este no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir la regulación sobre protección de datos, debiendo de ser este quien decida facilitar esta información a cambio de poder ejercitar los derechos que le corresponden.

5 Referencias bibliográficas

- Agencia Española de Protección de Datos. (2016). *Guía para el cumplimiento del deber de informar*. Madrid: AEPD.
- Agencia Española de Protección de Datos. (2020). *Informe del Gabinete Jurídico núm. 0017/2020*. Madrid: AEPD.
- Comité de Bioética de España. (2020). *Informe del Comité de Bioética de España sobre los requisitos ético-legales en la investigación con datos de salud y muestras biológicas en el marco de la pandemia de COVID-19*.
- Commission Nationale de l'Informatique et des Libertés. (2020). *Coronavirus (COVID-19): les rappels de la CNIL sur la collecte de données personnelles*.
- Congreso de los Diputados. (2018). Enmiendas e índice de enmiendas al articulado. 121/000013, Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal. *Boletín Oficial de las Cortes Generales*, 13, 129-130.
- Dei Cas, Bárbara. (2008). El concepto jurídico indeterminado como límite de la discrecionalidad. *Revista de Derecho*, 14, 71-86.
- European Data Protection Board. (2020). *Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak*. Bruselas: EDPB.
- European Data Protection Board. (2020). *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak*. Bruselas: EDPB.
- Garante per la Protezione dei Dati Personali. (2020). *Coronavirus: No do-it-yourself (DIY) data collection, says the Italian DPA*. Roma: GPDP.
- García de Enterría Martínez-Carande, Eduardo. (1996). Una nota sobre el interés general como concepto jurídico indeterminado. *Revista Española de Derecho Administrativo*, 89, 69-89.
- Grupo de Trabajo del Artículo 29 sobre Protección de Datos. (2017). Dictamen 03/2017 sobre el tratamiento de los datos personales en el contexto de los sistemas de transporte inteligentes (STI) cooperativos, 17/ES WP 252, adoptado el 4 de octubre de 2017.
- Grupo de Trabajo del Artículo 29 sobre Protección de Datos. (2018). *Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679*, 17/ES WP259.
- Ministerio de Sanidad. (2020). *Informe del Ministerio de Sanidad sobre los aspectos éticos en situaciones de pandemia: El SARS-CoV-2*.
- Martínez Martínez, Ricard. (11 de marzo de 2020). A la muerte por protección de datos. *LOPD y Seguridad*.
- Martínez Martínez, Ricard. (19 de marzo de 2020). Los tratamientos de datos personales en la crisis del COVID-19: un enfoque desde la salud pública. *Diario La Ley*, 1(38).
- Martínez Martínez, Ricard. (31 de marzo de 2020). Protección de datos y geolocalización en la Orden SND/297/2020. *Hay Derecho*.
- Marzo Portera, Ana. (18 de marzo de 2020). La inoportuna doctrina de las autoridades europeas de protección de datos frente al Covid-19. *Hay Derecho*.

- Mínero Alejandro, Gemma. (27 de marzo de 2020). COVID-19 y protección de datos personales. Quo vadis? *Blog de la Facultad de Derecho*.
- Piñar Mañas, José Luis. (2020). La protección de datos durante la crisis del coronavirus. *Consejo General de la Abogacía Española*.
- Puyol Montero, Javier. (2016). Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos. En José Luis Piñar Mañas (dir.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad* (p. 149-150). Madrid: Reus.
- Rodríguez Ayuso, Juan Francisco. (2020). *Control externo de los obligados por el tratamiento de datos personales*. Barcelona: Bosch.