EL TRATAMIENTO DE DATOS PERSONALES DURANTE LA PANDEMIA POR COVID-19. ALGUNAS REFLEXIONES Y LECCIONES APRENDIDAS

Gemma Minero Alejandre*

Resumen

En este trabajo se estudian las bases jurídicas legitimadoras del tratamiento de datos personales relacionados con la salud durante la crisis sanitaria provocada por la COVID-19. Se analizan los principios rectores de todo tratamiento regulados en el Reglamento General Europeo de Protección de Datos, que también han de regir en aquellos tratamientos realizados en base al consentimiento expreso del sujeto interesado o, en el caso de las personas fallecidas, de sus representantes legales. Se reflexiona sobre tratamientos específicos realizados y se tienen en cuenta las recomendaciones aprobadas por el Comité Europeo de Protección de Datos y la Agencia Española de Protección de Datos.

Palabras clave

Protección de datos personales, consentimiento del interesado, responsable del tratamiento, salud pública, estado de alarma, crisis sanitaria, geolocalización, aplicaciones móviles de rastreo, derecho sui generis*, inversión.*

Abstract

This paper studies the legal basis of personal data processing. In particular, in relation to processing of data concerning health, during the COVID-19 health crisis. Data-protection principles contained within the General Data Protection Regulation are analyzed. These general data-protection principles are also applied in cases where the data subject has explicitly consented the processing. The paper also analyzes some real specific data processing made during the COVID-19 pandemic. It takes into account the recommendations made by the European Data Protection Committee, and the Spanish Agency for Data Protection.

* Profesora Contratada Doctora del Departamento de Derecho Privado, Social y Económico de la Facultad de Derecho de la Universidad Autónoma de Madrid. gemma.minero@uam.es

Keywords

Data protection, data subject's consent, controller, public health, state of alarm, health crisis, geolocation, contact tracking apps, sui generis *right, investment.*

SUMARIO: I. Introducción al objeto de estudio. II. Advertencias de las autoridades de protección de datos y bases jurídicas del tratamiento distintas del consentimiento. III. Principios rectores del tratamiento de datos personales. IV. En particular, algunas reflexiones sobre las aplicaciones de rastreo. V. Tutela de la base de datos por un derecho de propiedad intelectual muy especial: el derecho *sui generis*. VI. Algunas conclusiones. VII. Bibliografía.

I. **INTRODUCCIÓN AL OBJETO DE ESTUDIO**

Desde la suscripción del Convenio número 108 del Consejo de Europa sobre Protección de datos de carácter personal (2), hasta hoy, han sido muchos los pasos dados y los cambios efectuados en la configuración del régimen de tutela frente al uso de datos personales.

El derecho a la protección de datos personales es actualmente un derecho independiente de otros derechos previstos en el artículo 18 de la Constitución española, como puede ser el derecho a la intimidad o el derecho al honor. Este precepto constitucional, en su apartado cuarto, contempla un reconocimiento muy escueto, limitado a la previsión de que la ley limite «el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Sin embargo, la jurisprudencia, primero, y el legislador europeo, después, se han encargado de perfilar una tutela robusta. (3)

---

(2) Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981 (BOE n.º 274, de 15 de noviembre de 1985), ratificado por España el 27 de enero de 1984 y entrado en vigor el 1 de octubre de 1985. De acuerdo con el artículo 1 de este tratado internacional, el objetivo que se persigue con su aprobación es el de «garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona». Tal y como consta en el preámbulo, el Convenio se adopta «considerando que es deseable ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados». Téngase presente la relación directa entre la tutela de los datos personales y el derecho al respeto de la vida privada, que tanto el preámbulo como el articulado se encargan de señalar.

(3) Así lo indica expresamente el apartado primero del preámbulo de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (BOE n.º 294, de 6 de diciembre de 2018), y así había sido reconocido previamente por la jurisprudencia constitucional. La STC 254/1993, de 20 de julio, supone la primera aproximación al significado del artículo 18.4 de la Constitución. Se identificó, entonces, en esta norma una nueva garantía constitucional,

Goza de regulación en un cuerpo normativo propio –la actual Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, en adelante LOPDGDD, que transpone el Reglamento General Europeo de Protección de Datos, en adelante RGPD–, de cuya aplicación se deduce que se ha convertido en uno de los derechos más importantes para el desarrollo de una sociedad democrática avanzada y para el libre desarrollo de la personalidad y de la dignidad de las personas, sobre todo, más que nunca, en el entorno digital (4).

Es innegable que el éxito del desarrollo tecnológico y de las nuevas formas de consumo pasan por el tratamiento masivo de datos personales, que, en ocasiones, raya la vigilancia constante y la influencia patente en las preferencias y decisiones de los ciudadanos. Influencia que no ha estado exenta de polémica desde que brotó la pandemia provocada por la COVID-19, entre otros contextos, en relación con un conjunto de datos personales tratados por los sistemas de detección y control de la enfermedad y en las aplicaciones de rastreo o seguimiento, que tratan datos de particular relevancia para el individuo, como son los datos de la salud (5). Esta categoría especial de datos, además, tiene un alto valor en el mercado (6).

---

que constituye una dimensión del derecho a la intimidad, en el que se incluye la facultad de los interesados de acceder a los datos que la Administración posee de ellos. Esta línea de ambigüedad se mantuvo en las SSTC 143/1994 y 11/1998, virando en las dos sentencias dictadas por este órgano el 30 de noviembre de 2000 (SSTC n.º 290/2000 y 292/2000). En estas dos últimas resoluciones se configura el derecho a la protección de datos como un verdadero derecho fundamental nuevo, con razón de ser propia y existencia autónoma. En efecto, hasta la jurisprudencia constitucional dictada en 2000, las sentencias destacaron la transcendencia de este derecho, pero también su carácter instrumental, para servir a la protección de otros derechos fundamentales, como «instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos». Véase Lucas Murillo De La Cueva, P., «La Constitución y el derecho a la autodeterminación informativa», *Cuadernos de Derecho Público,* n.º 19-20, 2003, p. 27 y ss.

(4) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (DOUE n.º 119, de 4 de mayo de 2016). El reconocimiento de este derecho también se recoge en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea.

(5) De acuerdo con el Tribunal de Justicia de la Unión Europea, el término «datos relativos a la salud» debe interpretarse en sentido amplio [sentencia de 6 de noviembre de 2003, C-101/01 (Lindqvist), apartado 50]. Han de entenderse englobados en este término los datos contenidos en la historia clínica y resultados de exámenes y tratamientos, contestaciones de los interesados a encuestas de autocomprobación, como es la declaración de síntomas y, finalmente, información que se convierte en datos sanitarios al ser utilizada en el contexto específico de la crisis sanitaria, como puede ser información sobre un viaje reciente un país afectado por una determinada variante de la COVID-19, el lugar de residencia o los datos de localización (ubicación) de una persona en las horas y días previos al diagnóstico positivo del virus, con el objeto de identificar al resto de personas que pudieran haberse expuesto a una situación de riesgo de contagio. Véase, Comité Europeo De Protección De Datos, *Directrices 03/2020 sobre el tratamiento de datos relativos a la salud con fines de investigación científica en el contexto del brote de COVID-19*, adoptadas el 21 de abril de 2020, disponibles en la siguiente URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_es.pdf (último acceso: 6 de mayo de 2021), p. 5.

(6) Sin embargo, el éxito obtenido por este tipo de aplicaciones es más que dudoso. Se ha sostenido que la eficacia de estas para combatir la pandemia exigía el uso por al menos el 60% de la población de un concreto municipio o país. Teniendo en cuenta el carácter voluntario del uso de este tipo de tecnologías –naturaleza no imperativa sobre la que volveremos más adelante–, puede afirmarse que ninguna de las aplicaciones ha conseguido un mínimo nivel de éxito.

En este sentido, ahora más que nunca, se hace necesaria la tarea de concienciación ciudadana para adquirir el conocimiento de la existencia, del contenido de este derecho fundamental y de las vías para su reivindicación. En este trabajo se reflexiona sobre algunas de las implicaciones jurídicas que la normativa vigente exige en los tratamientos de datos personales de los que hemos sido objeto en los últimos meses –o seguimos siéndolo, en algunos casos–.

Quedan fuera de este estudio los tratamientos de datos debidamente anonimizados llevados a cabo durante la crisis sanitaria, pues, tras la anonimización, siempre que esta se haya realizado correctamente, no podremos hablar de datos personales ni aplicar la normativa reguladora de estos (7). Así, por ejemplo, los datos de geolocalización anonimizada de móviles, que fueron requeridos tanto por el Gobierno español como por la Comisión Europea a los teleoperadores de comunicaciones para detectar movimientos de población (8). No se optó, sin embargo, por hacer un tratamiento de datos personales como medida de vigilancia y mitigación de aglomeraciones de ciudadanos, como hubiera sido el hecho de geolocalizar a determinadas personas identificadas o identificables y reconstruir sus movimientos y cambios de localización o enviar mensajes sobre salud pública por teléfono o

(7) La anonimización supone dar un paso más allá de la seudonimización. Esta segunda se define en el artículo 4.5 del RGPD como «el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable». De acuerdo con el Grupo de Trabajo sobre Protección de Datos del artículo 29 (Unión Europea), la seudonimización es una útil medida de seguridad, pero no es un método de anonimización, porque permite singularizar a los interesados y vincularlos entre conjuntos de datos diferentes. Por ello, la probabilidad de que el seudoanonimato admita la identificabilidad es alta y este tipo de tratamiento entra dentro del ámbito de aplicación del régimen jurídico de la protección de datos. Véase Grupo De Trabajo Sobre Protección De Datos Del Artículo 29 (Unión Europea), *Dictamen sobre técnicas de anonimización*, 10 de abril de 2014, p. 3. El Comité de Bioética de España valora positivamente que en el contexto de la base legitimadora de la investigación científica en situaciones de riesgo para la salud pública –sobre la que posteriormente se volverá a lo largo de este trabajo– se pueda hacer uso de la seudonimización frente a la tradicional estricta anonimización porque ello permite tanto «ampliar el conjunto de los datos que se utilizan en la investigación» como «lo que es muy importante en el estado actual de la ciencia del Big Data, contrastar los resultados de la explotación de datos con, por ejemplo, la verdadera evolución de los pacientes (verificación de resultados)». Comité De Bioética De España, *Informe sobre los requisitos ético-legales en la investigación con datos de salud y muestras biológicas en el marco de la pandemia de COVID-19,* p. 19, accesible en la siguiente URL: http://assets.comitedebioetica.es/files/documentacion/Informe%20CBE%20investigacion%20COVID-19.pdf (último acceso: 6 de mayo de 2021).

(8) Véase Orden SND/297/2020, de 27 de marzo, disponible en https://www.boe.es/boe/dias/2020/03/28/pdfs/BOE-A-2020-4162.pdf y, en el ámbito europeo, véase

https://www.politico.com/news/2020/03/24/europe-mobile-data-coronavirus-146074, ambas referenciadas por la AEPD en estudio «El uso de las tecnologías en la lucha contra el COVID19», accesible en https://www.aepd.es/sites/default/files/2020-05/analisis-tecnologias-COVID19.pdf (último acceso: 6 de mayo de 2021). Con ello se sigue la directriz de dar prioridad al uso de datos de localización anonimizados, sobre la que llamaba la atención el Comité Europeo De Protección De Datos, en su resolución «Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID 19», adoptadas el 21 de abril de 2020, p. 6, accesible en https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_es.pdf (último acceso: 6 de mayo de 2021).

SMS a grupos de personas en una zona específica. (9) De ahí lo infundado de buena parte de las críticas vertidas en debates mediáticos y medios de comunicación. (10)

A falta de jurisprudencia del Tribunal Constitucional y del Tribunal Supremo que avale las afirmaciones contenidas en este trabajo –dado lo prematuro de la cuestión–, este artículo plasma algunas ideas doctrinales, basadas en las recomendaciones realizadas por las autoridades nacionales y europeas en materia de protección de datos y en el estudio del funcionamiento e idiosincrasia de algunos ejemplos reales de tratamiento de datos referidos a la salud de los ciudadanos. (11)

II. ADVERTENCIAS DE LAS AUTORIDADES DE PROTECCIÓN DE DATOS Y BASES JURÍDICAS DEL TRATAMIENTO DISTINTAS DEL CONSENTIMIENTO

El Comité Europeo de Protección de Datos, en su declaración de 19 de marzo de 2020 *–Declaración sobre el tratamiento de datos personales en el contexto del brote de COVID-19–*, advertía del hecho de que el RGPD sigue vigente en tiempos de pandemia. En principio, la crisis sanitaria no suspende ni restringe la posibilidad de que los interesados ejerzan sus derechos de conformidad con los artículos 12 a 22 del RGPD. Eso sí, el artículo 89.2, del RGPD permite al legislador nacional

(9) En principio, se cumple con el principio de proporcionalidad, optando preferentemente por las soluciones menos invasivas, teniendo en cuenta el objetivo específico que se pretende alcanzar con el tratamiento. Se desecharon medidas de rastreo de personas con tratamiento de datos de localización no anonimizados.

(10) Véase Wendehorst, C., "COVID-19 Apps and Data Protection", en *Coronavirus and the Law in Europe,* disponible en la siguiente URL: https://www.intersentiaonline.com/publication/coronavirus-and-the-law-in-europe/10 (último acceso: 6 de mayo de 2021).

(11) Entre la doctrina, puede verse: Troncoso Reigada, A., «Los tratamientos de datos personales para fines de salud pública y el derecho a la protección de datos personales en tiempos del COVID-19», en *Retos jurídicos ante la crisis del COVID-19,* coord. por Rodríguez Ayuso, J. F. & Atienza Macías, E., 2020, pp. 553-601; Costa, G., Peris Brines, N. & Cervera Navas, L., «La protección de datos en un verano con sombrero y mascarilla», *La Ley privacidad,* Nº. 5, 2020; Martínez Martínez, R., «Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública», *Diario La Ley,* Nº 9604, 2020; Rodríguez-Chaves Mimbrero, B., «Tratamiento de datos personales en la lucha contra la pandemia por la covid-19. Las medidas de excepción y principio de proporcionalidad», *Revista española de derecho administrativo,* Nº 209, 2020, pp. 317-356; Ortega Giménez, A., «COVID-19: un desafío para la Protección de datos de carácter personal», *Actualidad jurídica iberoamericana,* Nº. Extra 12, 2, 2020, pp. 860-867; Naval Parra, M.C., «La protección de datos personales en la lucha contra la propagación del Coronavirus», *Diario La Ley*, Nº 9638, 2020; Rodríguez Ayuso, J. F., «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*, Nº. Extra 3, 2020, pp. 137-152; Frías Martínez, E., «Covid-19. Medidas limitativas de derechos. "Arcas de Noé". Mención a la protección de datos personales. Herramientas de geolocalización», *Diario La Ley,* Nº 9619, 2020; Schneble, C.O., Elger, B.S. & Shaw, D.M., "Data protection during the coronavirus crisis", *EMBO Reports,* Volume 21, Issue 9, September 2020; Bradford, L., Aboy, M. & Liddell, K., "COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes", *Journal of Law and the Biosciences*, Volume 7, Issue 1, January-December 2020; y Ventrella, E., "Privacy in emergency circumstances: data protection and the COVID-19 pandemic", *ERA Forum* 21, 379–393 (2020).

limitar los derechos del interesado establecidos en el capítulo III de este cuerpo normativo. Además, en el citado documento del Comité Europeo de Protección de Datos se advertía que el RGPD no podía ser considerado un escollo en la toma de decisiones que impliquen el uso de datos personales para atajar la pandemia actual. (12) En paralelo, la Agencia Española de Protección de Datos (AEPD) emitía, con fecha de 12 de marzo de 2020, su Informe 0017/2020, sobre los tratamientos de datos en relación con el COVID-19. (13)

En la ponderación entre el derecho a la salud y la tutela del interés general de la salud pública y el interés particular a la protección de los datos personales, este último ha de decaer, en beneficio del primero, cuando existe una emergencia sanitaria de alcance general. (14) De ahí que, en estos supuestos excepcionales, se permita el tratamiento de datos personales por las autoridades sanitarias competentes de las distintas administraciones públicas, cuando ese uso de datos personales sea necesario por razones de interés público esencial en el ámbito de la salud pública, sin que dicho tratamiento deba basarse en el consentimiento de los afectados. (15) Ello incluye el Ministerio de Sanidad y las entidades autonómicas competentes o sujetos en los que hubieren delegado, así como el Instituto Nacional de Estadística, la Red Nacional de Vigilancia epidemiológica, de reciente creación, así como otros órganos creados a tales efectos a nivel nacional, autonómico o municipal (16). La base jurídica del tratamiento deja de ser en estos casos el consentimiento del interesado para pasar a ser la tutela de la salud colectiva. De ahí que las personas afectadas no pueden negarse a someterse al tratamiento de sus datos personales, so pena de la sanción administrativa y pudiendo llegar a cometer un delito contra la

(12) Texto accesible en la siguiente URL: https://edpb.europa.eu/our-work-tools/our-documents/other-guidance/statement-processing-personal-data-context-covid-19_es (último acceso: 6 de mayo de 2021).

(13) Texto accesible en la página web de la AEPD: https://www.aepd.es/es/documento/2020-0017.pdf (último acceso: 6 de mayo de 2021). En su párrafo primero se afirma: «la normativa de protección de datos personales, en tanto que dirigida a salvaguardar un derecho fundamental, se aplica en su integridad a la situación actual, dado que no existe razón alguna que determine la suspensión de derechos fundamentales, ni dicha medida ha sido adoptada».

(14) De acuerdo con la citada Declaración, el derecho a la salud prima frente al derecho a la protección de datos personales «cuando el tratamiento sea necesario por razones de interés público esencial en el ámbito de la salud pública». «En estas circunstancias, no es necesario basar el tratamiento de los datos en el consentimiento de los afectados». Comité Europeo De Protección De Datos, *Declaración sobre el tratamiento de datos personales en el contexto del brote de COVID-19, cit.,* p. 1.

(15) En el caso de las páginas web y aplicaciones móviles no oficiales, gestionadas por entidades privadas, ampliamente extendidas, que permiten la autoevaluación de la enfermedad o transmiten consejos relativos a la COVID-19, el tratamiento exige el consentimiento del interesado. La AEPD emitió un comunicado el 16 de marzo de 2020, en el que advertía a la ciudadanía de los riesgos que implica el facilitar categorías de datos sensibles, como son los relativos a la salud, a estas webs y apps, «incluso en aquellos casos en los que aparentemente esos datos no se asocian a la identidad del usuario que utiliza la aplicación». Ello se hace tras constatar la AEPD que muchas de estas páginas y aplicaciones no aportan información que permita identificar a los responsables del tratamiento ni detallan las finalidades de dicho tratamiento. En dicho comunicado, la AEPD anunciaba el inicio de actuaciones de investigación para identificar a los responsables e imponerles las correspondientes sanciones económicas. Texto accesible en la página web de la AEPD: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-de-la-aepd-en-relacion-con-webs-y-apps-que-ofrecen (último acceso: 6 de mayo de 2021).

(16) Rodríguez Ayuso, J. F., «Protección de datos personales en el contexto de la Covid-19. Legitimación en el tratamiento de datos de salud por las Administraciones Públicas», *cit.,* p. 141.

salud pública. Esta regla especial abarca el tratamiento de datos personales de categorías especiales, como pueden ser los datos de la salud. (17)

Téngase en cuenta la limitación subjetiva de esta regla excepcional: otros sujetos diferentes de las citadas autoridades sanitarias no entrarán dentro de esta vía de legitimación especial no basada en el consentimiento del interesado. Dado que estamos ante una regla excepcional, esta ha de interpretarse de forma restrictiva, nunca extensiva ni haciendo uso de la figura de la analogía. Piénsese, por ejemplo, en operadores de telecomunicaciones o en empresas privadas, que necesitarán del consentimiento del interesado para realizar un tratamiento lícito de datos de carácter personal. Asimismo, regirá la prohibición contenida en el considerando 54 del RGPD, referido a los datos de la salud, que impide que terceros, «como empresarios, compañías de seguros o entidades bancarias» traten los datos personales con otros fines. (18) La prohibición legal del uso de datos por terceros distintos de los gestores sanitarios públicos busca preservar el mantenimiento de los estándares éticos y legales respecto del uso de datos personales relacionados con la salud. (19) Advertencia esta última que no era necesaria, pues se podía inferir de la propia interpretación restrictiva del ámbito subjetivo al que se aplica esta regla excepcional distinta del consentimiento del interesado. (20)

Sin embargo, el tratamiento de datos personales lícito por motivos de salud pública no debe hacerse a toda costa o sin exigir ninguna garantía, sino que han de cumplirse unos principios mínimos normativos. En este sentido, el citado documento del Comité Europeo de Protección de Datos señaló que las medidas que en su caso se adoptasen y que afecten a este derecho fundamental debían ser temporales, no permanentes o irreversibles. (21) Afirmación que se infiere asimismo de la

---

(17) Se cumple, por tanto, el principio de legalidad en el tratamiento de datos de carácter personal, que exige que el tratamiento se base en una causa legitimadora de las previstas en la normativa de protección de datos para las categorías especiales de datos (artículos 6.1 y 9.2 del RGPD).

(18) Téngase presente que la gestión sanitaria, en ocasiones, se realiza por empresas privadas, si bien estas no se subsumirán en el citado considerando 54 RGPD, al actuar por delegación o en ejercicio de facultades conferidas por la autoridad pública.

(19) Por ello, en estos casos, la licitud del tratamiento de datos personales pasa por el consentimiento expreso del interesado. Pensemos, por ejemplo, en la traducción que el uso de estos datos de la salud puede tener en un aumento de la prima a pagar por el seguro de vida contratado por una persona que resulta contagiada por COVID-19, determinándose dicho incremento, por ejemplo, en la evolución del infectado y en el carácter persistente o no de sus secuelas. Yendo un paso más allá se puede pensar en la futura denegación de la celebración de este tipo de seguros si el conjunto de compañías aseguradoras pudiera hacer uso de los datos recopilados por las autoridades sanitarias durante la actual crisis sanitaria.

(20) Con todo, este considerando no está de más, ni siquiera en un sistema de salud pública altamente reglamentado y con garantías en la afectación de la privacidad, como es el español, pues es fácil, en ocasiones, difuminar la frontera entre lo público y lo privado y entre, por un lado, la declarada finalidad de la gestión de esta crisis sanitaria y, por otro lado, la persecución de otros objetivos parejos, pero no idénticos, que no podrán subsumirse en las mismas bases jurídicas de interés público mencionadas en este trabajo.

(21) «Es preciso tener en cuenta una serie de consideraciones para garantizar el tratamiento lícito de los datos personales y recordar, en todos los casos, que cualquier medida adoptada en este contexto debe respetar los principios generales del derecho y no ser irreversible. La actual pandemia es una situación jurídica que puede legitimar ciertas restricciones de las libertades siempre que estas sean proporcionadas y su duración no se prolongue más allá de la propia duración de la epidemia». Comité Europeo De Protección De Datos, *Declaración sobre el tratamiento de datos personales en el contexto del brote de COVID-19, cit.,* p. 1.

exigencia de interpretar las reglas excepcionales de forma restrictiva: la licitud del tratamiento de datos personales empleando una base jurídica excepcional distinta del consentimiento del afectado durará lo que dure la situación de excepcionalidad que lo justifica. En nuestro caso, el término final de la licitud del tratamiento habrá de ser decidido por las autoridades sanitarias en base a la duración de la situación de pandemia. Parece razonable que pueda extenderse más allá de la duración del estado de alarma, hasta el control real de la enfermedad y la terminación del proceso de vacunación. (22)

Únicamente podrán tratarse los datos necesarios para la finalidad de tutela de la salud pública, no para otros fines. En este caso, solamente podrán tratarse los datos necesarios para evitar la propagación de la enfermedad, evaluar la eficacia global de las medidas de confinamiento y para gestionar la evolución de las personas ya contagiadas y la gestión de la vacunación. La AEPD hace un llamamiento a la importancia de no confundir la conveniencia del tratamiento con la necesidad del tratamiento. El tratamiento necesario es únicamente el imprescindible. Otros tratamientos no imprescindibles, pero sí convenientes, requerirán, en todo caso, del consentimiento del interesado para resultar lícitos. (23)

Las autoridades sanitarias podrán, utilizando como base jurídica la tutela de la salud colectiva, realizar un seguimiento telefónico diario y recabar los correspondientes datos, durante 15 días o dentro del período de conservación de datos que, desde el punto de vista epidemiológico, resulten pertinentes, de la persona contagiada con COVID-19, para conocer la evolución y valorar el posible ingreso o la medicación a aplicar, como parte de una estrategia global de salud pública que incluya la realización de pruebas de detección y el tratamiento de los datos así obtenidos. Otro ejemplo subsumible en esta base jurídica excepcional es el uso de datos personales de los ciudadanos para comunicarles la fecha de citación para la vacunación, debiendo contar con una vía alternativa de aviso para no invisibilizar a las personas que no saben o no poseen un teléfono móvil. Asimismo, se engloba

(22) De ahí la prohibición general de reutilización de los datos de la salud pública una vez termine la crisis sanitaria. Prohibición general que se aplica tanto a personas físicas como jurídicas, tanto de carácter público como privado, que sean consideradas responsables del tratamiento de datos, y tanto si el tratamiento se ha llevado a cabo con el consentimiento expreso del interesado como cuando se ha realizado por aplicación de alguna de las bases jurídicas legitimadoras del tratamiento distintas del propio consentimiento y contenidas en el RGPD. No comparto, sin embargo, la postura defendida por un grupo de juristas especializados en la materia, encabezados por Manuela Battaglini, Elena Gil González, Javier Valls Prieto y José Antonio Castillo Parrilla, en su carta dirigida al Gobierno de la Nación, en la que exigían la limitación temporal del tratamiento de datos personales a un período de «19 meses» o «hasta que salga la vacuna». Texto accesible en esta URL: https://elpais.com/tecnologia/2020-03-21/expertos-en-privacidad-admiten-que-la-crisis-permite-un-uso-excepcional-de-datos-personales.html (último acceso: 6 de mayo de 2021). Valoro el esfuerzo por determinar el máximo temporal del uso, pero me parece más adecuado permitir una interpretación flexible del cumplimiento de este requisito, que permita tener en cuenta la evolución de factores sanitarios aún hoy desconocidos o inciertos que habrán de ser identificados y valorados por las autoridades sanitarias. En este sentido, no me parece inadecuado el contenido del artículo 23 del Real Decreto Ley 21/2020, de 9 de junio, que establece que las medidas serán aplicables incluso una vez finalizada la prórroga del estado de alarma, hasta que el Gobierno declare, previo informe del Centro de Coordinación de Alertas y Emergencias Sanitarias, la finalización de la situación de crisis sanitaria ocasionada por la COVID-19.

(23) Así, por ejemplo, el tratamiento que puedan hacer las entidades enunciadas en el considerando 54 del RGPD. En particular, las empresas aseguradoras y personas jurídicas relacionadas con servicios sanitarios o paralelos.

dentro de esta base legitimadora el rastreo de contactos, con la finalidad de que las personas que hayan estado muy cerca de alguien que resulte ser un portador confirmado de la enfermedad sean informadas con celeridad, a fin de romper las cadenas de transmisión lo antes posible.

Sin embargo, esta base jurídica no será suficiente, por ejemplo, para que las autoridades sanitarias obliguen a este sujeto y al resto de personas de su entorno con quien hubiera tenido contacto en la última semana a instalar en sus dispositivos una concreta aplicación móvil oficial nacional o autonómica que permita la geolocalización de personas que hubieran sido diagnosticadas y transmita los datos personales así recabados a dicha autoridad sanitaria. En este sentido, ha de tenerse en cuenta el contenido de la Directiva sobre la privacidad y las comunicaciones electrónicas. (24) Tal y como señaló el Comité Europeo de protección de Datos, en principio, los datos de localización de los usuarios de servicios telefónicos solo pueden ser utilizados por el operador «si han sido anonimizados o si se cuenta con el consentimiento de los interesados», de acuerdo con el artículo 5.3 de esta Directiva. (25)

No obstante, el artículo 15 de la Directiva sobre la privacidad y las comunicaciones electrónicas permite a los estados miembros introducir medidas legales para proteger la seguridad pública en supuestos excepcionales, siempre y cuando se cumplan con los principios mínimos o garantías a los que haremos referencia más adelante, entre ellos la limitación del tiempo de conservación de los datos personales (26). En el caso español, como se ha indicado en el apartado previo de este trabajo, la aplicación de esta norma excepcional fue necesaria, pero únicamente de forma limitada. Se optó por exigir a las empresas de comunicaciones datos de localización recogidos en el contexto de la prestación de sus servicios, pero anonimizados, que permitieran estudiar mediante técnicas de cartografía el movimiento global de la población y la concentración de dispositivos móviles en un lugar determinado, pero no se requirieron datos personales de esos usuarios. (27)

---

(24) Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (DOUE n.º 201, de 31 de julio de2002).

(25) Comité Europeo De Protección De Datos, *Declaración sobre el tratamiento de datos personales en el contexto del brote de COVID-19, cit.,* p. 2.

(26) Este artículo 15 habla en términos muy estrictos de esta potestad estatal, que habrá de quedar limitada a supuestos en los que el tratamiento de datos personales constituya «una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos».

(27) En estos casos, dado que la obligación de comunicación de los datos por parte de los operadores de telecomunicaciones se basó en un mandato legal, la base jurídica más adecuada para el tratamiento de datos es la necesidad de cumplir una misión de interés público, es decir, el artículo 6, apartado 1, letra e), del RGPD. Al no tratarse de datos personales, en realidad, su uso queda fuera del ámbito de aplicación del RGPD y no exige el consentimiento del interesado. Véase Comité Europeo De Protección De Datos, «Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-19», *cit.,* p. 8. El artículo 27.2 del Real Decreto Ley 21/2020, de 9 de junio, de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por el COVID-19, señala que la finalidad del tratamiento es «el seguimiento y vigilancia epidemiológica del COVID-19 para prevenir y evitar situaciones excepcionales de especial gravedad, atendiendo a razones de interés público esencial en el ámbito específico de la salud pública», a lo que añade también «la protección de intereses vitales de

Por tanto, se adoptaron medidas que permitieron exigir por parte de las autoridades sanitarias a los operadores de servicios de telecomunicación la captación y transmisión de datos de localización, pero se procedió al tratamiento únicamente tras la efectiva anonimización. No se optó por exigir la geolocalización de determinadas personas ubicadas, por ejemplo, en una zona específica. (28)

Más allá de los meros datos de localización facilitados por los operadores de telecomunicaciones, debemos tener en cuenta una serie de cuestiones para calificar como lícito o no el tratamiento de datos personales realizado. En primer lugar, el RGPD parte de una realidad incuestionable: el derecho a la protección de datos es un derecho fundamental, pero no es un derecho absoluto, sino que ha de ponderarse con el resto de derechos e intereses en juego (29). Además, permite, en situaciones excepcionales –como puede ser, qué duda cabe, una pandemia mundial–, el tratamiento de datos personales –incluidos los datos especialmente sensibles– sin necesidad de contar con el consentimiento de las personas afectadas. Por tanto, la propia normativa contiene una ponderación de los intereses y derechos en liza para el bien común. Así se prevé en los artículos 6 y 9 del RGPD.

Esta última norma permite el tratamiento de datos cuando lo exijan motivos de interés público esencial en el ámbito de la salud pública [artículo 9, apartado 2, letra i)] o cuando sea necesario proteger intereses vitales del interesado o de otra u otras personas físicas [artículo 9, apartado 2, letra c)] (30). Además, la letra h) de este precepto hace referencia al tratamiento de datos que sea necesario para realizar un diagnóstico médico o la gestión de servicios de asistencia sanitaria y social. Tampoco puede olvidarse la referencia que la letra j) de este artículo hace al tratamiento que sea necesario para fines de investigación científica.

El Comité de Bioética de España ha recalcado la base jurídica prevista en la Disposición Adicional 17ª de la Ley Orgánica 3/2018, apartado b): las autoridades

---

los afectados y de otras personas físicas». Otros ejemplos son el registro de viajeros de la Consejería de Sanidad de la Xunta de Galicia, creado con la finalidad de poder tener identificados a quienes hayan estado durante los últimos catorce días en territorios con alta incidencia epidemiológica por COVID-19, tanto dentro como fuera de España, o la Orden 920/2020, de 28 de julio, de la Consejería de Sanidad de la Comunidad de Madrid, que regula la obligación de llevar un registro de clientes para locales de ocio. La finalidad última es tener datos de contacto para, si fuera necesario, poder notificar a los ciudadanos afectados que han podido estar expuestos a un caso positivo.

(28) De acuerdo con la AEPD, «Con una gestión cuidadosa, el acceso apropiadamente anonimizado a dicha información no debería de representar una amenaza mayor que la que ya representaban antes. (…) Por hacer un uso mayor de estos datos anonimizados, puede haber un riesgo mayor, pero no exponencialmente mayor». AEPD, *El uso de las tecnologías en la lucha contra el COVID19, cit.,* p. 4.

(29) Véase Ventrella, E., "Privacy in emergency circumstances: data protection and the COVID-19 pandemic", *cit.,* p. 380.

(30) En particular, sobre la base jurídica de la protección de los intereses vitales del interesado u otras personas físicas, la AEPD indica que «por extensión supone que dichas personas físicas pueden ser incluso no identificadas o identificables; es decir, 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, y ello es reconocido por la normativa de protección de datos personales». Sin embargo, esta afirmación debe casar con la exigencia de la necesidad del tratamiento, es decir, con la exigencia de que el tratamiento que se haga sea el imprescindible para alcanzar el fin permitido por esta base jurídica, y no vaya más allá.

sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública. Esta excepción al requisito general del consentimiento informado se completa en el apartado d) de esta norma, que exige la seudonimización de los datos empleados para la investigación –que no la anonimización, de ahí que sigan considerándose datos personales, pues la persona física no está identificada, pero sí es identificable y siga siendo de aplicación el régimen jurídico contenido en la normativa de datos personales– y el informe previo del comité de ética de la investigación previsto en la normativa sectorial. Se requiere una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización, con un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación (31). De ahí que, en palabras, del Comité de Bioética de España, lo relevante para el uso secundario de los datos de salud y las muestras biológicas «(…) no será tanto que el individuo haya otorgado su consentimiento previo para el nuevo fin al que pretenden destinarse los datos o que el dato esté estrictamente anonimizado, como que el origen de los datos sea legítimo, que su uso secundario revista un interés muy relevante para la salud de la colectividad y que se implementen garantías suficientes que impidan que terceros no legitimados puedan acceder a través del dato a la identidad del individuo, sin exigir necesariamente dicha estricta anonimización» (32).

Por su parte, el considerando 46 del RGPD se refiere expresamente al control de epidemias como base legitimadora del tratamiento de datos personales. Respecto al tratamiento para finalidades de investigación, sobre el que posteriormente volveremos, debe destacarse una importante advertencia: el considerando 159 del RGPD permite aplicar esta base jurídica del tratamiento a la científica que se desarrolla en el ámbito de la salud pública, incluida la «investigación financiada por el sector privado» (33). Circunstancia que, al ser una norma excepcional, nuevamente no será susceptible de interpretación amplia o extensiva.

En particular, la base legal específicamente aprobada durante la pandemia para ser aplicable al tratamiento de datos personales por las autoridades públicas sanitarias se encuentra contenida en el Real Decreto Ley 21/2020, de 9 de junio, sobre medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por el COVID-19. Su artículo 22 califica el COVID-19 como enfermedad de declaración obligatoria urgente, a efectos de lo previsto en el Real Decreto 2210/1995, por el que se crea la Red Nacional de Vigilancia Epidemiológica. Esta declaración permite establecer la obligación de facilitar a la autoridad de salud pública competente en cada territorio los datos personales necesarios para el seguimiento y la vigilancia epidemiológica que le sean requeridos.

(31) Por aplicación del artículo 58.2 de la Ley 14/2007, de 3 de julio, de investigación biomédica, este régimen se extiende al uso secundario de muestras biológicas en contexto de grave peligro para la salud pública.

(32) Comité De Bioética De España, *Informe sobre los requisitos ético-legales en la investigación con datos de salud y muestras biológicas en el marco de la pandemia de COVID-19, cit.,* p. 18.

(33) El término «tratamiento de datos personales con fines de investigación científica», que, de acuerdo con el considerando 159 del RGPD, incluye, por ejemplo, «el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado», así como «los estudios realizados para el interés público en el ámbito de la salud pública».

Por su parte, el artículo 27 del Real Decreto Ley establece que en todo caso se deberán respetar las previsiones contenidas en el RGPD. (34)

La suma de las bases jurídicas reguladas en estas normas permitiría, por ejemplo, el tratamiento por las autoridades sanitarias de datos personales de una persona contagiada para comunicar a los individuos con los que la primera tuvo contacto en una determinada horquilla temporal la circunstancia del contagio, con el objetivo de salvaguardar la salud de dichas personas (base jurídica del interés vital de la persona física cuyos datos personales son tratados) y, a su vez, de reducir las posibilidades de contagio del resto de la población, al permitir a esos sujetos que eviten contribuir a expandir la enfermedad a terceros (base jurídica del interés vital de terceros e interés público esencial o cualificado en el ámbito de la salud pública). El interés vital del afectado por la enfermedad del coronavirus o de un tercero, como base legitimadora del tratamiento permite que dicho tratamiento se dirija también a proteger a aquellas personas susceptibles de ser contagiadas por el virus (35).

III. PRINCIPIOS RECTORES DEL TRATAMIENTO DE DATOS PERSONALES

Como se ha advertido en el apartado previo, la aplicación de una de las bases jurídicas estudiadas, distintas del consentimiento del interesado, para reconocer la licitud del tratamiento de datos personales no impide la vigencia de los principios contenidos en el artículo 5 del RGPD. Estos rigen con independencia de cuál sea la base jurídica del tratamiento de datos y habrán de cumplirse por la persona responsable del tratamiento. De ahí que a la afirmación anteriormente expuesta relativa al carácter no absoluto o ilimitado del derecho fundamental a la protección debe sumarse la necesidad de hacer hincapié en que no toda medida que pueda adoptarse sobre tratamiento de datos personales para contener la crisis sanitaria está justificada si infringe las garantías o principios básicos de la normativa sobre protección de datos personales.

Es importante recalcar el valor bidireccional de las anteriores afirmaciones, tanto en supuestos en los que el tratamiento se basa en el consentimiento previo del interesado como cuando parte de otra base jurídica. Por tanto, todo tratamiento de datos personales realizado tras recabar el consentimiento del afectado también habrá de cumplir todos y cada uno de los principios aquí expuestos. A falta de implementación de alguno de ellos, por ejemplo, en una concreta aplicación des-

(34) Véase Martínez Martínez, R., «Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública», *cit*.

(35) Ello es conforme con el artículo 3 de la Ley Orgánica 3/1986 de Medidas Especiales en Materia de Salud Pública, que prevé: «Con el fin de controlar las enfermedades transmisibles, la autoridad sanitaria, además de realizar las acciones preventivas generales, podrá adoptar las medidas oportunas para el control de los enfermos, de las personas que estén o hayan estado en contacto con los mismos y del medio ambiente inmediato, así como las que se consideren necesarias en caso de riesgo de carácter transmisible». Véase Rodríguez Ayuso, J. F., «Protección de datos personales en el contexto de la Covid-19. Legitimación en el tratamiento de datos de salud por las Administraciones Públicas», *cit.*, p. 150.

cargada en su dispositivo móvil por un usuario, tras la correspondiente aceptación de las condiciones de uso y las políticas de privacidad, estaremos hablando de un tratamiento ilícito de sus datos personales. Así, por ejemplo, en el caso de algunas aplicaciones móviles que surgieron de forma casi instantánea desde el inicio del estado de alarma, en algunos casos de iniciativas ciudadanas, con el objetivo de creación de mapas y estadísticas de propagación de la COVID-19 a partir de datos –sobre salud y localización– proporcionados voluntariamente por sus usuarios o con la finalidad de ofrecer autodiagnósticos y consejos sobre la enfermedad. En este caso, el tratamiento de dichos datos no está conducido, filtrado o supervisado por las autoridades sanitarias. (36) De ahí la importancia de que los responsables del tratamiento den cumplimiento a los principios previstos en el RGPD y la necesidad de que el responsable del tratamiento se identifique con claridad y haga una referencia expresa al carácter voluntario de la aplicación. (37)

También han de aplicarse estas reglas en las aplicaciones oficiales nacionales o autonómicas de rastreo de contactos, de instalación y uso voluntario para la ciudadanía, que notifican el posible riesgo de contagio por contacto con usuario diagnosticado como positivo en COVID-19. (38) Téngase en cuenta que las autoridades sanitarias han subcontratado, en ocasiones, los servicios de entidades privadas –Telefónica, Amazon o Microsoft, entre otras– para el almacenamiento de datos y tareas de gestión y administración necesarias para el éxito del funcionamiento de este tipo de aplicaciones. Recuérdese que las bases jurídicas aquí estudiadas no permiten, en territorio europeo, que el Gobierno o el legislador de un Estado miembro imponga a sus ciudadanos la obligación de instalación y uso de alguna de estas aplicaciones, porque ello supondría una clara afectación de una serie de derechos fundamentales, entre ellos, el derecho a la intimidad y el derecho

(36) El Consejo Europeo de Protección de Datos indicó que el uso de aplicaciones de rastreo de contactos debe ser siempre voluntario y no puede basarse en el rastreo de movimientos individuales, sino en información sobre la proximidad de los usuarios. Muchas de estas aplicaciones funcionan mediante tecnología *Bluetooth*, para detectar la presencia de usuarios cerca del dispositivo que está usando la aplicación, pero no envían a los usuarios datos identificativos de la persona diagnosticada como positiva en COVID-19, cerca de la cual hayan podido estar en una horquilla temporal. Comité Europeo De Protección De Datos, «Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID 19», *cit.,* pp. 5 y 18.

(37) Entre ellos, el principio de exactitud y el de confidencialidad adquieren una relevancia capital, sobre todo cuando las aplicaciones no tienen fines tan altruistas como los que declaran o no han desarrollado suficientes garantías para la privacidad. Ello exige implementar políticas de control de la exactitud, actualización y confidencialidad, que eviten que los usuarios proporcionen datos falsos o que terceros no autorizados accedan a ellos. Cuando la cantidad y calidad de los datos es suficiente, estas aplicaciones podrán crear mapas de barrios con alto y con bajo nivel de infección, de alto valor en el mercado para el responsable del tratamiento y para terceros. De ello nos advierte la AEPD, «El uso de las tecnologías en la lucha contra el COVID19», *cit.,* p. 7. En relación con el principio de minimización, el Consejo Europeo de protección de Datos advirtió «las aplicaciones de rastreo de contactos no requieren un seguimiento de la ubicación de los usuarios a título individual; en su lugar, deben utilizarse datos de proximidad». Comité Europeo De Protección De Datos, «Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID 19», *cit.,* p. 8.

(38) Véase la Orden del Ministerio de Sanidad SND/297/2020, de 27 de marzo, por la que se encomendó a la Secretaría de Estado de digitalización e inteligencia artificial del Ministerio de Asuntos Económicos y Transformación Digital el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria.

a la protección de datos personales. (39) El responsable del tratamiento ha de llamar la atención también en estos casos sobre el carácter voluntario del uso de la aplicación, sin que se pueda condicionar el acceso a ningún derecho garantizado por ley al uso efectivo de la aplicación. (40)

Entre los principios imperativos cabe destacar el citado principio de limitación de la finalidad, el principio de exactitud y el principio de minimización de datos. (41) Además, el artículo 9 RGPD y su considerando 4 exigen la proporcionalidad del tratamiento y la finalidad perseguida por este con otros derechos fundamentales e intereses implicados.

El primer principio enunciado exige que los datos sean recogidos con fines determinados, explícitos y legítimos (en nuestro caso, como se ha señalado previamente, salvaguardar los intereses vitales de las personas físicas y del interés colectivo de la salud pública durante la crisis sanitaria), y no puedan ser tratados ulteriormente de manera incompatible con dichos fines. Un uso que vaya más allá de los citados fines exigirá, para su licitud, una nueva declaración de consentimiento del interesado o la aplicación de una nueva base legal del tratamiento. Ello se complementa con el principio de minimización, que exige no solo que no se pueda dar un uso incompatible con el fin inicial, sino también que no se pueda realizar un tratamiento que vaya más allá de lo necesario para cumplir ese fin inicial. (42)

Eso sí, el propio artículo 5 del RGPD permite que se realice un tratamiento ulterior de los datos personales «con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos» (43). Se exige, por tanto, que los fines del estudio sean de interés para la salud pública, requisito que, en muchos de los proyectos actuales, puede perfectamente acreditarse (44). Este matiz adquiere una destacable relevancia en nuestro caso, pues permitirá a las autoridades públicas sanitarias conservar los datos tratados durante la pandemia para llevar

(39) Además, supondría un claro incumplimiento del principio de proporcionalidad en el tratamiento de datos personales, al existir otras medidas alternativas menos invasivas en la intimidad del individuo. En este sentido, véase Wendehorst, C., "COVID-19 Apps and Data Protection", *cit.*

(40) Para ambos tipos de aplicaciones móviles de rastreo, el Comité Europeo de protección de Datos aconsejó que se deba proceder a informar de manera automática a las personas que podrían haber estado expuestas al virus, sin identificar al sujeto confirmado como portador de la COVID-19 en dicha comunicación. Esta información ha de basarse en la proximidad a un usuario infectado en un intervalo de «x» días (determinado por la autoridad sanitaria) antes de la prueba de detección que haya dado positivo y durante un período «y» de tiempo, suficiente como para entender que ha existido contacto. Además, el uso de la aplicación no debe permitir que los usuarios obtengan información de otros usuarios, como, por ejemplo, información sobre si son o no portadores del virus. Véase Comité Europeo De Protección De Datos, «Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID 19», *cit.,* pp. 14, 16 y 20.

(41) AEPD, *Informe 0017/2020, sobre los tratamientos de datos en relación con el COVID-19, cit.,* p. 7.

(42) De acuerdo con el Comité Europeo, el cumplimiento efectivo de este principio implica la obligación del responsable del tratamiento de informar a los interesados de la concreta finalidad o finalidades del tratamiento, de forma fácilmente accesible y utilizando para ello un lenguaje claro y sencillo, que permita su comprensión por el afectado por el tratamiento. Comité Europeo De Protección De Datos, *Declaración sobre el tratamiento de datos personales en el contexto del brote de COVID-19, cit.,* p. 2.

(43) Además, esta norma indica que «el tratamiento ulterior de los datos personales con fines de [...] investigación científica [...] no se considerará incompatible con los fines iniciales».

(44) Comité De Bioética De España, *Informe sobre los requisitos ético-legales en la investigación con datos de salud y muestras biológicas en el marco de la pandemia de COVID-19, cit.,* p. 16.

a cabo estas tareas de interés público-científico, como puede ser, por ejemplo, para mejorar la composición y combatir las reacciones o estudiar mejoras en la administración de las actuales y futuras vacunas y crear protocolos de actuación frente a potenciales nuevas olas de la enfermedad o frente a ulteriores pandemias. De ahí la importancia de identificar con precisión la finalidad de investigación perseguida, debiendo procurar una interpretación no extensiva, pues no se puede olvidar que, en la mayoría de supuestos, estaremos ante un tratamiento de datos personales realizado con una base jurídica distinta del consentimiento expreso del interesado. Además, no puede perderse de vista la advertencia contenida en el citado considerando 159 RGPD, acerca de la subsunción de la investigación financiada con cargo a fondos privados dentro de la figura de la investigación científica, para la que el artículo 5 RGPD permite el tratamiento y la conservación de los datos personales inicialmente recabados, en nuestro caso, para la finalidad de la gestión de la crisis sanitaria.

En paralelo, el citado principio de proporcionalidad exige evaluar las medidas de tratamiento de datos personales que se pretenden diseñar para dar cumplimiento a la concreta finalidad del tratamiento proyectado, debiendo implementar medidas técnicas y organizativas destinadas a minimizar el tratamiento de datos personales. Todo ello, con el objetivo de que el tratamiento realizado sea proporcional al fin legítimo perseguido.

El principio de minimización de datos exige que los datos tratados habrán de ser adecuados, pertinentes y exclusivamente los limitados a los necesarios para la finalidad pretendida (el control de la epidemia, incluida la gestión de la vacunación, en este caso, con las subfinalidades que puedan deducirse de estas, como puede ser el análisis de la evolución de la persona infectada y su entorno o la citación para la administración de las correspondientes dosis de la vacuna y seguimiento de posibles reacciones), sin que se pueda extender dicho tratamiento a cualesquiera otros datos personales no estrictamente necesarios para dicha finalidad. Esto es especialmente aplicable en los casos en los que el concreto tratamiento se realice utilizando dispositivos o técnicas que ofrezcan la posibilidad de grabar y conservar los datos o tratar información adicional, como puede ser información biométrica que no sea estrictamente necesaria, sino un añadido para el cumplimiento de la finalidad inicial. (45)

Si pensamos, por ejemplo, en las aplicaciones voluntarias de rastreo de contactos contagiados a las que se hizo referencia anteriormente debemos concluir que el principio de minimización de datos impide que la aplicación recoja información que no tenga relación con la finalidad perseguida por el tratamiento, como puede ser su estado civil, los mensajes recibidos o enviados o el registro de llamadas, así como los elementos del directorio del equipo en el que se instaló dicha aplicación, entre otros. Por su parte, el principio de limitación de la finalidad del tratamiento exigirá que las aplicaciones solamente tengan como objetivo rastrear contactos, de tal modo que las personas que puedan estar expuestas al virus sean alertadas y reciban asistencia, sin que pueda servir para controlar el cumplimiento de medidas de

(45) Así lo advirtió expresamente la AEPD en su Comunicado de 30 de abril de 2020, en relación con la toma de temperatura por parte de comercios, centros de trabajo y otros establecimientos, accesible en la siguiente URL: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-aepd-temperatura-establecimientos (último acceso: 6 de mayo de 2021).

cuarentena o de confinamiento y/o de distanciamiento social, ni extraerse conclusiones sobre la ubicación de los usuarios basadas en su interacción. (46)

Esta regla va de la mano del principio de limitación del plazo de conservación, que exige que los datos sean mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales. De acuerdo con el Comité Europeo de Protección de Datos, el cumplimiento efectivo de este principio implica la obligación del responsable del tratamiento de informar a los interesados del período de conservación de los datos recogidos (47). El término final es complejo de predecir, pero se ha visto que, en todo caso, ha de superar la horquilla temporal que dure la declaración del estado de alarma. Transcurrido ese período imprescindible, el responsable solamente podrá conservarlos si procede a su anonimización. En caso contrario, habrá de borrarlos. Ello con la misma excepción que acaba de señalarse: la posibilidad de que el responsable conserve los datos personales –sin necesidad de anonimización, pero sí de seudonimización– durante períodos más largos exclusivamente para fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

Por su parte, el principio de exactitud exige que los equipos de medición o diagnóstico empleados y el personal que realice el tratamiento, así como los criterios e intervalos de tiempo de toma de datos personales y tratamiento posterior sean los adecuados para registrar los datos con fiabilidad y precisión. Además, se exige el mantenimiento o actualización de los datos, implementando las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan. Se busca evitar el impacto negativo que sobre las personas interesadas tendría un tratamiento errado de sus datos personales, provocado por un mal desarrollo de la recogida o un fallo en el propio tratamiento o por falta de actualización posterior. Pensemos, por ejemplo, en un fallo en el sistema de almacenamiento de datos que conlleve el envío de diversos mensajes contradictorios a los teléfonos de los ciudadanos que hayan sido citados para la vacunación o el error en el cómputo del número de dosis administradas a cada uno o en el desarrollo o no de reacciones adversas que recomienden la paralización o retraso en la administración de las siguientes dosis o el cambio del suero a administrar.

Como regla de cierre, todo tratamiento ha de cumplir el principio de integridad y confidencialidad, garantizando la seguridad adecuada de los datos personales, lo que pasa por incluir protección contra el tratamiento no autorizado o ilícito e implementar políticas de confidencialidad que impidan la comunicación a terceros. Dicha comunicación, en caso de existir, ha de contar con el consentimiento del sujeto afectado por el tratamiento para ser lícita. Para el cumplimiento de este principio, el Comité Europeo de Protección de Datos exige a las autoridades públicas

(46) Comité Europeo De Protección De Datos, *Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID 19, cit.,* p. 16.

(47) Comité Europeo De Protección De Datos, *Declaración sobre el tratamiento de datos personales en el contexto del brote de COVID-19, cit.,* p. 2. La autoridad europea recuerda la importancia de fijar los períodos de conservación proporcionales, teniendo en cuenta su longitud y su propósito.

sanitarias documentar adecuadamente las medidas aplicadas para gestionar la situación de emergencia actual y el proceso de toma de decisiones subyacente. (48)

IV. EN PARTICULAR, ALGUNAS REFLEXIONES SOBRE LAS APLICACIONES DE RASTREO

Como se ha indicado previamente, aquellas aplicaciones móviles que realicen tratamiento de datos personales gestionadas por entidades privadas sin mandato de autoridad pública no podrán ser beneficiarias de ninguna de las bases legales especiales del tratamiento anteriormente estudiadas, por lo que, para ser lícito dicho tratamiento, el responsable habrá de contar con el consentimiento del usuario cuyos datos personales vayan a ser tratados. Esta afirmación también será extensible a las aplicaciones creadas por autoridades públicas sanitarias o terceros contratados por estas y cuyo uso y descarga tenga un carácter voluntario para el ciudadano, complementario al rastreo manual individualizado implementado por la autoridad sanitaria en caso de diagnóstico positivo en COVID-19. Los principios generales estudiados son aplicables a este supuesto, debiendo el responsable del tratamiento acatar las consecuencias de la aplicación de la normativa de protección de datos, que habrá de ser tenida en cuenta desde las fases iniciales de diseño de la aplicación en cuestión (49).

Especial relevancia adquieren el principio de minimización del uso de datos –que limita el uso de los datos al mínimo necesario o imprescindible para cumplir la concreta finalidad del tratamiento– y el principio de limitación temporal del tratamiento o conservación de estos datos –que exige que no se conserven los datos personales por más tiempo del necesario para el cumplimiento de esa finalidad, debiendo proceder al borrado o a la efectiva anonimización transcurrido ese período–. En ocasiones, las técnicas de anonimización empleadas dejan mucho que desear, lo que se traduce en un incumplimiento recurrente de este principio legal (50).

Asimismo, han de analizarse las características del consentimiento otorgado por el interesado para el tratamiento de sus datos personales. La primera obligación a cumplir por el responsable del tratamiento, como ya se ha indicado, es la información acerca del carácter voluntario de la aplicación móvil y, por ello, del consentimiento del interesado. Dicho consentimiento habrá de cumplir las condi-

(48) *Idem,* p. 2.

(49) Con todo, algunas de estas aplicaciones han sido diseñadas siguiendo un modelo descentralizado de almacenamiento de datos, en el que los datos sobre personas expuestas al riesgo de contagio por haber estado en contacto con una persona diagnosticada como positivo en COVID-19 no pasan por un servidor, sino que permanecen en el teléfono móvil del usuario, tras un proceso de encriptación, en la mayoría de los casos. Estos supuestos plantean muchos menos problemas desde el punto de vista de la normativa de protección de datos personales, pues permiten el borrado de datos con la mera desinstalación de la aplicación. Siguiendo el símil empleado por WENDEHORST, puede compararse el almacenamiento del mensaje de aviso de la aplicación con el almacenamiento en el disco duro de un dispositivo de un documento Word en el que esté escrito «Puede que sea positivo en Covid-19». WENDEHORST, C., "COVID-19 Apps and Data Protection", en *Coronavirus and the Law in Europe, cit.*

(50) Véase BRADFORD, L., ABOY, M. & LIDDELL, K., "COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes", *cit.* p. 7.

ciones de ser libre, específico e informado, en el sentido de los artículos 4.11, 6.1.a y 7 del RGPD. Por tanto, debe ser una manifestación de voluntad no viciada, referida a uno o varios fines identificados previamente por el responsable del tratamiento utilizando un lenguaje claro y sencillo, ya sea mediante una declaración o una clara acción afirmativa, pero en todo caso ha de tratarse de un consentimiento inequívoco.

La información previamente aportada por el responsable habrá de cubrir asimismo, de acuerdo con el artículo 13 del RGPD, la identidad y los datos de contacto del responsable y, en su caso, de su representante, los destinatarios o las categorías de destinatarios de los datos personales, en su caso, y el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo, debiendo cumplir el principio de limitación del tiempo de conservación, que ha sido estudiado en el anterior apartado de este trabajo. Además, el responsable debe informar previamente al interesado de su derecho a retirar su consentimiento en cualquier momento con la misma facilidad con la que otorgó ese consentimiento (artículo 7.3 del RGPD), así como información sobre la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado y su rectificación, supresión o limitación de su tratamiento, así como el derecho a oponerse al tratamiento y el derecho a la portabilidad de los datos. Eso sí, la retirada del consentimiento no afectará a la licitud del tratamiento realizado hasta ese momento, basada en el consentimiento previo a su retirada. Precisamente, este derecho de retirada del consentimiento, que en ningún caso queda limitado durante la vigencia de la crisis sanitaria, convierte en poco fiable el tratamiento de datos personales que pueda realizar la aplicación en cuestión, dada la volatilidad de la manifestación de voluntad así prestada y retirada.

La aplicación móvil de alerta de contagios del virus con mayor recorrido en nuestro país, Radar Covid, utiliza tecnología *Bluetooth Low Energy* y fue desarrollada por el Gobierno de España y, en particular, por la Secretaría General de Administración Digital, dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, que es el sujeto responsable del tratamiento.(51) Como se ha indicado, el tratamiento de datos personales derivado del uso de esta aplicación exige el consentimiento del interesado, que tendrá para ello que descargar la aplicación y aceptar las condiciones de uso.

El usuario de Radar Covid recibirá una notificación en caso de que en los 14 días anteriores haya estado expuesto a contacto con otro usuario de la aplicación positivo en COVID-19, durante más de 15 minutos y con una distancia inferior a dos metros. La aplicación únicamente informa del día en el que se produjo la expo-

(51) En otros países también se optó por desarrollar aplicaciones que emplean la tecnología *Bluetooth.* Así, por ejemplo, *Corona-Warn-App* en Alemania, *Stopp-CoronaApp* en Austria, *StopCovid* en Francia y *ProteGo* en Polonia. Véase Bradford, L., Aboy, M. & Liddell, K., "COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes", *cit.* p. 3. Sobre los tipos de tecnología disponibles en la actualidad: geolocalización no anonimizada, geolocalización anonimizada y *Bluetooth,* véase Schneble, C. O., Elger, B. S. & Shaw, D. M., "Data protection during the coronavirus crisis", *cit.,* p. 1; y Comité Europeo De Protección De Datos, «Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID 19», *cit.,* pp. 5 y 18.

sición al virus, pero no de la identidad del usuario positivo, ni del usuario que resultó expuesto, ni identifica los dispositivos de los usuarios, ni transmite datos sobre el momento o lugar en que la exposición se haya producido. La aplicación no solicita ni almacena datos de carácter personal de los usuarios, tal y como se desprende de su política de privacidad (52). Recibida la notificación sobre la alerta de posible contagio, la aplicación facilitará al usuario expuesto información para la adopción de medidas preventivas y asistenciales.

Otra de las aplicaciones móviles más destacadas, en este caso de carácter autonómico, es Coronamadrid, una de las pioneras de nuestro país. Es la aplicación móvil oficial de la Comunidad de Madrid y en su política de datos figura como responsable del tratamiento la Viceconsejería de Asistencia Sanitaria de la Consejería de Sanidad. La finalidad de Coronamadrid es muy diferente a la señalada anteriormente para Radar Covid. En este caso se busca realizar la autoevaluación diaria del usuario sobre la base de los síntomas médicos que comunique a la aplicación e integrar sus datos en los sistemas públicos de gestión de historias clínicas de la Comunidad de Madrid con la finalidad de prestar la adecuada asistencia sanitaria. Además, se prevé, tras su anonimización, el uso de los datos con fines estadísticos, de investigación biomédica, científica o histórica y para archivo en interés público.

A diferencia de la aplicación nacional, esta aplicación autonómica sí hace tratamiento de datos personales. En particular, nombre y apellidos, número de teléfono, DNI, fecha de nacimiento, dirección postal completa, género, datos de la salud relacionados con los síntomas del virus y, de manera opcional, geolocalización. Cuesta entender que el principio de minimización del uso de datos se cumpla con el tratamiento del dato del género, si bien la autoridad sanitaria, con mejor criterio que la autora de este trabajo, pueda argumentar que, al igual que la fecha de nacimiento, este dato puede permitir ponderar síntomas y determinar si se trata de un grupo de riesgo. En cuanto a la geolocalización (localización vía GPS del teléfono móvil del usuario), se indica que, en caso de consentimiento, solamente se utilizará este dato a la hora de registrarte y para realizar las autoevaluaciones del

(52) Domínguez Álvarez, J. L., «La necesaria protección de las categorías especiales de datos personales. Una reflexión sobre los datos relativos a la salud como axioma imprescindible para alcanzar el anhelado desarrollo tecnológico frente al Covid-19», *Revista de Comunicación y Salud*, 2020, Vol. 10, n.º 2, p. 619. La tecnología en la que se basa esta aplicación permite crear identificadores efímeros *Bluetooth* por cada teléfono cada 10-20 minutos, que se transmiten a dispositivos cercanos en los que se haya descargado la aplicación y tengan activado el *Bluetooth*, sin que contengan información que pueda identificar al teléfono ni al usuario del mismo. Una vez el usuario recibe un diagnóstico positivo por COVID-19, se abre la posibilidad de introducir voluntariamente en la aplicación el «código de confirmación de un solo uso» facilitado por el Servicio Público de Salud y se le solicitará su consentimiento para remitir al servidor las últimas claves de exposición temporal almacenadas en el teléfono, con el objetivo de componer un listado diario de claves de exposición temporal de personas contagiadas por COVID-19. Por tanto, solamente si el usuario emplea la función de comunicar un diagnóstico positivo tras someterse a la preceptiva prueba se consigue maximizar la eficacia de esta aplicación. La aplicación descarga periódicamente esas claves de exposición temporal compartidas, para compararlas con los códigos registrados en los días anteriores como resultado de contactos con otros usuarios. Si se encuentra una coincidencia, la aplicación ejecuta un algoritmo que, en función de la duración y la distancia estimada del contacto, evalúa el riesgo de exposición al virus y, en su caso, muestra una notificación advirtiendo del contacto de riesgo al usuario e invitándolo a auto-confinarse y contactar con las autoridades sanitarias.

usuario (53). El objetivo, conforme a la política de privacidad de la aplicación, es «garantizar la calidad de los datos y su análisis epidemiológico y así poder entender la distribución de los síntomas con datos lo más fiables posibles», pero no está claro el efectivo cumplimiento del principio de minimización del uso de datos. En el apartado de preguntas frecuentes se señala que la recogida de «información poblacional [...] puede ayudar a las autoridades a la adopción de medidas o diferentes protocolos en el marco de la crisis surgida con el COVID-19». Por tanto, no se prevé un uso por las Fuerzas y Cuerpos de Seguridad a efectos sancionatorios o de vigilancia del cumplimiento de las medidas de confinamiento, ni otros tipos de usos secundarios, lo cual es acorde con el principio de minimización del uso de datos personales. Asimismo, el responsable del tratamiento de datos se compromete a garantizar el máximo nivel de protección en el acceso que los terceros puedan tener a los datos, estableciendo las correspondientes medidas de aseguramiento de la confidencialidad.

En cuanto al principio de limitación del tiempo de uso de los datos personales, en la política de privacidad actualmente se indica que Coronamadrid solamente conservará los datos «durante el período que dure la situación de emergencia sanitaria» (54). A la vista de la lenta evolución de la crisis sanitaria, se ha corregido la anterior mención prevista en este apartado, vigente durante 2020, que señalaba «el plazo de conservación será de un máximo de dos años, todo ello de conformidad con los principios legales de tratamiento de datos, en particular el de minimización de datos».

V. TUTELA DE LA BASE DE DATOS POR UN DERECHO DE PROPIEDAD INTELECTUAL MUY ESPECIAL: EL DERECHO SUI GENERIS

Antes de concluir, es importante destacar las voluminosas inversiones que están detrás de la constitución de las muchas bases de datos que han proliferado durante la crisis sanitaria y cuyo régimen jurídico referido a la protección de datos personales ha sido estudiado en este trabajo. Inversiones públicas, en unos casos, y privadas, en otros. Ambos tipos pueden ser tutelados por un derecho específico de propiedad intelectual: el llamado derecho *sui generis*. Su propio nombre indica que, dentro del conjunto de derechos de propiedad intelectual, se trata de una *rara avis*. La razón de ser de esta tutela es antagónica al objeto tradicionalmente protegido por el derecho de autor. Mientras que el derecho de autor tutela la originalidad del autor plasmada en la confección de una obra, el derecho *sui generis* protege aquellas bases de datos en las que el fabricante hubiera invertido una cantidad sustancial.

Si bien, por motivos de longitud de este trabajo, no podemos extendernos en el análisis de esta especial forma de protección de las bases de datos, han de hacerse

(53) En el apartado «Condiciones de uso» se aclara: «La aplicación no recoge información continua de localización de los usuarios, ni rastrea su localización, ni tampoco realiza *geofencing* para determinar si el ciudadano se encuentra en su domicilio».

(54) Seguidamente se indica: «En el momento en que finalice el periodo de conservación de tus datos, estos serán anonimizados y/o bloqueados conforme a los requisitos establecidos en la normativa aplicable».

varias indicaciones relevantes. La primera se refiere a la aptitud para la tutela por el derecho *sui generis* de la mayoría de bases de datos creadas durante la pandemia como consecuencia del funcionamiento de las aplicaciones móviles estudiadas en apartados previos de este trabajo o de la implementación de los sistemas de rastreo manual de posibles contactos con personas contagiadas, entre otras. En todos estos casos no cabe ninguna duda de que la inversión destinada al tratamiento de los datos personales albergados en ellas ha sido sustancial y, por ello, merecedora de tutela.

En segundo lugar, ha de destacarse la identidad del sujeto titular del derecho: la persona pública o privada que realizó la inversión. Este derecho, como cualquier otra facultad de un derecho de propiedad intelectual, es, por definición, susceptible de transmisión, tanto *inter vivos* como *mortis causa*, durante los 15 años que dura. De ahí la relevancia que pueda tener, siempre que la efectiva transmisión del derecho case con la normativa de protección de datos personales, para que quienes realizaron importantes inversiones en la fabricación de estas bases de datos puedan ver amortizadas dichas cuantías (55).

VI. **ALGUNAS CONCLUSIONES**

En este estudio se ha tratado de exponer una serie de reflexiones de corte general sobre la afectación del derecho fundamental a la protección de datos personales durante la crisis sanitaria provocada por el COVID-19. En paralelo, se han analizado casos concretos de tratamiento de datos personales referidos a la salud de las personas llevados a cabo en los últimos meses. Sin embargo, en la fecha de cierre de este trabajo es difícil predecir el momento en el que volveremos a la normalidad y las indicaciones aquí realizadas acerca de los matices en la aplicación del régimen de tutela de los datos personales dejarán de tener vigencia. También es complicado augurar si las lecciones aprendidas durante la crisis sanitaria conducirán a nuestros legisladores a regular nuevas reglas excepcionales o si considerarán, por el contrario, que las actuales pueden ser suficientes en potenciales nuevas pandemias. En todo caso, de decidir regular una regla nueva, el éxito de esta pasará por su carácter comunitario, no siendo plausible una norma especial nacional en un ámbito –el de la protección de los datos personales– que se ha convertido en una seña de identidad europea.

Tras identificar las bases legales del tratamiento, distintas del consentimiento del interesado y referidas al interés general de la salud pública, se han expuesto los límites infranqueables que todo tratamiento –basado o no en el consentimiento del interesado y permitido o no por un interés general tan relevante como la salud colectiva– debe cumplir. La situación de crisis sanitaria sirve para dar pie a un volumen importante de tratamientos de datos necesarios para la gestión de la pandemia, pero no puede ser entendida como una carta blanca que permita cualquier tipo de tratamiento extensivo y por tiempo excesivo de los datos personales de la ciudadanía. Ello, tanto en tratamientos llevados a cabo por las autoridades públicas

(55) Para un análisis detallado de las implicaciones prácticas del derecho *sui generis*, véase Minero Alejandre, G., *La protección jurídica de las bases de datos en el ordenamiento europeo,* Tecnos, 2014.

sanitarias –o por terceros a los que se les hubiera encomendado este mandato, incluidas entidades privadas–, como los realizados por empresarios.

A modo de conclusión, puede afirmarse que no es cierto que la regulación sobre protección de datos personales haya supuesto un obstáculo o un elemento de obstrucción a la implementación de tratamientos de datos personales necesarios para la adopción de medidas eficaces frente al COVID-19. No cabe hablar de un enfrentamiento entre salud pública y protección de datos, sino de dos piezas fundamentales que han de convivir en situaciones de pandemia. Además, este estudio busca llamar la atención sobre la sinrazón de algunas de las feroces críticas vertidas durante los meses de pandemia acerca del incumplimiento total de la normativa de protección de datos personales por las decisiones tomadas por las autoridades sanitarias españolas o autonómicas. En particular, en materia de investigación científica, como uso secundario de los datos personales recabados durante la gestión de la crisis sanitaria, es especialmente importante tratar de conciliar la urgencia que permita alcanzar con más eficacia resultados de la investigación que nos permitan combatir esta pandemia y epidemias futuras y la necesidad de desarrollar una investigación rigurosa, tanto en sus parámetros científicos como jurídico-éticos.

Sirva este trabajo para reiterar la importancia del compromiso europeo y nacional con el derecho fundamental a la protección de datos y para recordar que toda medida que excepcionalmente se adopte en materia de protección de datos durante la crisis sanitaria ha de ser, por definición, temporal. Esta afirmación permite hacer una advertencia sobre la necesidad de mejora de las técnicas de anonimización actualmente existentes, como alternativa al borrado de datos muy valiosos, en particular, en nuestro caso, con enorme valor para la investigación científica y la gestión sanitaria de potenciales pandemias futuras. Terminada la situación excepcional, el cuerpo normativo estudiado, que impone el consentimiento del interesado como base de la legalidad del tratamiento, ha de volver a aplicarse en su integridad, recuperando los ciudadanos interesados la normalidad del ejercicio de este derecho fundamental.

Como nota de cierre, también deben destacarse los enormes beneficios que para la gestión de la pandemia y para el interés colectivo de la salud pública, en general, han traído algunas de las medidas de tratamiento de datos personales –y, en particular, datos relativos a la salud– implementadas por las autoridades públicas sanitarias en los últimos meses. Entre ellas, puede destacarse el requerimiento del Gobierno español a los teleoperadores de comunicaciones para detectar movimientos de población. De la ponderación realizada en este trabajo puede destacarse que, en un país en el que la normativa europea exige unos principios generales de privacidad que se han exigido y cumplido, con carácter general, esta medida ha traído más beneficios que contraindicaciones, resultando su aplicación equilibrada si se tienen en cuenta los diferentes derechos e intereses en juego.

VII. **BIBLIOGRAFÍA**

Bradford, L., Aboy, M. & Liddell, K., "COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes", *Journal of Law and the Biosciences,* Volume 7, Issue 1, January-December 2020.

COSTA, G., PERIS BRINES, N. & CERVERA NAVAS, L., «La protección de datos en un verano con sombrero y mascarilla», *La Ley privacidad,* n.º 5, 2020.

DOMÍNGUEZ ÁLVAREZ, J. L., «La necesaria protección de las categorías especiales de datos personales. Una reflexión sobre los datos relativos a la salud como axioma imprescindible para alcanzar el anhelado desarrollo tecnológico frente al Covid-19», *Revista de Comunicación y Salud*, 2020, Vol. 10, n.º 2.

FRÍAS MARTÍNEZ, E., «Covid-19. Medidas limitativas de derechos. «Arcas de Noé». Mención a la protección de datos personales. Herramientas de geolocalización», *Diario La Ley,* n.º 9619, 2020.

LUCAS MURILLO DE LA CUEVA, P., «La Constitución y el derecho a la autodeterminación informativa», *Cuadernos de Derecho Público,* n.º 19-20, 2003, p. 27 y ss.

MARTÍNEZ MARTÍNEZ, R., «Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública», *Diario La Ley,* n.º 9604, 2020.

NAVAL PARRA, M. C., «La protección de datos personales en la lucha contra la propagación del Coronavirus», *Diario La Ley,* n.º 638, 2020.

ORTEGA GIMÉNEZ, A., «COVID-19: un desafío para la protección de datos de carácter personal», *Actualidad Jurídica Iberoamericana,* n.º Extra 12, 2, 2020, pp. 860-867.

PINAR MAÑAS, J. L, «Día Europeo de Protección de Datos: las lecciones de la pandemia», página web de la Abogacía Española, https://www.abogacia.es/actualidad/opinion-y-analisis/dia-europeo-de-proteccion-de-datos-las-lecciones-de-la-pandemia/

RODRÍGUEZ AYUSO, J. F., «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,* n.º Extra 3, 2020, pp. 137-152.

RODRÍGUEZ-CHAVES MIMBRERO, B., «Tratamiento de datos personales en la lucha contra la pandemia por la COVID-19. Las medidas de excepción y principio de proporcionalidad», *Revista Española de Derecho Administrativo,* n.º 209, 2020, pp. 317-356.

SCHNEBLE, C. O., ELGER, B. S. & SHAW, D. M., "Data protection during the coronavirus crisis", *EMBO Reports,* Volume 21, Issue 9, September 2020.

TRONCOSO REIGADA, A., «Los tratamientos de datos personales para fines de salud pública y el derecho a la protección de datos personales en tiempos del COVID-19», en *Retos jurídicos ante la crisis del COVID-19,* coord. por RODRÍGUEZ AYUSO, J. F. & ATIENZA MACÍAS, E., 2020, pp. 553-601.

VENTRELLA, E., "Privacy in emergency circumstances: data protection and the COVID-19 pandemic", *ERA Forum,* 21, 2020, pp. 379-393.

WENDEHORST, C., "COVID-19 Apps and Data Protection", en *Coronavirus and the Law in Europe,* https://www.intersentiaonline.com/publication/coronavirus-and-the-law-in-europe/10