TRATAMIENTO DE DATOS PERSONALES EN LA LUCHA CONTRA LA PANDEMIA POR LA COVID-19. LAS MEDIDAS DE EXCEPCIÓN Y PRINCIPIO DE PROPORCIONALIDAD

BLANCA RODRÍGUEZ-CHAVES MIMBRERO

Profesora Contratada Doctora de Derecho Administrativo (Acreditada titular).
Universidad Autónoma de Madrid

Revista Española de Derecho Administrativo 209
Octubre – Diciembre 2020
Págs. 317–356

SUMARIO: I. LA PANDEMIA COVID-19, PRIMERA GRAN PRUEBA QUE HA TENSIONADO "LAS COSTURAS" DEL RGPD. II. TRATAMIENTOS DE DATOS PERSONALES EN SITUACIONES DE EMERGENCIA. III. DESARROLLOS TECNOLÓGICOS PARA EL CONTROL Y SEGUIMIENTO DE LA PANDEMIA POR LA COVID-19 Y LA GARANTÍA DEL DERECHO A LA PROTECCIÓN DE DATOS. 1. *El control de la temperatura manual o mediante cámaras térmicas.* 2. *COVID-19: Los establecimientos comerciales solo podrán tomar la temperatura a los clientes si las autoridades sanitarias publican una norma que fije los requisitos, según la AEPD.* 2.1. Criterios de interpretación marcados por la Unión Europea. 2.2. Criterios de interpretación articulados por la AEPD. 2.3. Aplicaciones de rastreo de contactos. IV. LAS GARANTÍAS DEL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL QUE DEBEN TENERSE EN CUENTA CUANDO ENTRA EN COLISIÓN CON OTRO DERECHO O BIEN JURÍDICAMENTE PROTEGIDO. 1. *Plano normativo (regulación del derecho a la protección de datos).* 1.1. La reserva de ley en la regulación de los derechos fundamentales. 1.2. La limitación de los derechos fundamentales. Contenido esencial. 2. *Plano aplicación del Derecho vigente. El juicio de proporcionalidad y la ponderación.* 3. *Recapitulación. El principio de proporcionalidad. La figura jurídica en la que se sustentan las decisiones normativas y resolutivas ante las situaciones de emergencia. aplicación a las medidas que implican usos de datos personales para la gestión de la pandemia.* V. UNAS ÚLTIMAS REFLEXIONES Y CONCLUSIONES. 1. *El "consentimiento".* 2. *Los principios de "licitud, lealtad y transparencia".* 3. *Los principios de "limitación de la finalidad" y "minimización de datos".*

RESUMEN: Este trabajo tiene como objeto analizar las garantías del tratamiento de los datos de carácter personal realizados desde los desarrollos tecnológicos articulados para la gestión de la pandemia causada por la COVID-19. El análisis de dichas garantías se afronta desde dos perspectivas que terminan convergiendo. Desde la primera perspectiva, el estudio de las garantías del derecho a la protección de datos personales se realiza a partir de los documentos emanados tanto desde las instituciones europeas, especialmente el Comité Europeo de Protección de Datos, como desde la Agencia Española de Protección de Datos, que interpretan la aplicación del Reglamento General de Protección de Datos en esta situación de pandemia. El estudio se complementa con una segunda perspectiva en la que se analizan sistemáticamente las exigencias que conlleva el respeto a los derechos fundamentales, como es el derecho a la protección de datos de carácter personal, tomando como referencia la STC 76/2019, aún en situaciones de emergencia e incertidumbre científica. Dicho análisis se realiza desde dos planos: el plano normativo y plano de aplicación del Derecho vigente.

PALABRAS CLAVE: Datos de salud – Aplicaciones de rastreo de contactos – Limitación de derechos – Ponderación – Consentimiento.

ABSTRACT: The purpose of this work is to analyze the guarantees for the processing of personal data for the management of the pandemic caused by COVID-19, from the technological developments articulated for the control of the virus. The analysis of these guarantees is approached from two perspectives that end up converging. From the first perspective, the study of the guarantees of the right to the protection of personal data is carried out from the documents issued both from the European institutions, especially the European Data Protection Committee, and from the Spanish Agency for Data Protection, which interpret the application of the General Data Protection Regulation in this pandemic situation. The study is complemented with a second perspective in which the demands that the respect for fundamental rights entails, such as the right to the protection of personal data, are systematically analyzed, taking as reference STC 76/2019, even in emergency and scientific uncertainty situations. This analysis is carried out from two levels: the normative level and the application of current Law.

KEYWORDS: Health data – Contact tracing applications – Limitation on rights – Weighting – Consent.

I. LA PANDEMIA COVID-19, PRIMERA GRAN PRUEBA QUE HA TENSIONADO "LAS COSTURAS" DEL RGPD

El Reglamento general de protección de datos (RGPD)[1] ha establecido un modelo europeo de protección de datos personales muy exigente para garantizar el derecho a la protección de datos de carácter personal con un destacado componente proactivo aplicable a los responsables en el tratamiento de datos personales. En este marco jurídico, las autoridades de control, como la Agencia Española de Protección de Datos (AEPD), tienen un papel de mucha preminencia en la interpretación de la normativa vigente sobre la protección de datos personales. En una situación tan grave como la que se ha planteado en la lucha contra la pandemia por COVID-19, las decisiones interpretativas de las autoridades de control sobre la admisibilidad del uso de datos personales para facilitar los avances en la investigación clínica o el rastreo de personas que hayan podido ser contagiadas, han adquirido aún más relevancia[2].

1. 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.
2. Algunos autores en los inicios de la crisis plantearon la responsabilidad que tenían, dada su preminencia, las autoridades de control, indicando que tendrían que abandonar su enfoque reactivo y plantear opciones que posibiliten el uso de datos personales en la lucha contra la COVID-19, al mismo tiempo que se protege el derecho a la protección de datos personales,

Nuestra sociedad ha cambiado en pocas semanas. Desde marzo de 2020 hemos visto distintas *iniciativas* para hacer un seguimiento de los usuarios y poder enfrentarse mejor a la pandemia[3]. Desde aplicaciones de diagnóstico, hasta un *estudio de movilidad* con datos de los operadores que gestionará el INE. Diferentes proyectos, cada uno con su propia forma de tratar los datos, pero con la necesidad de analizar de dónde proviene y cómo se expande la infección. Todas estas iniciativas implican un elevado volumen de tratamientos de datos personales y, especialmente, de datos sensibles como los de salud.

Esta monitorización por parte de las autoridades ha vuelto a reabrir el debate sobre la privacidad. Para entender el debate de privacidad entorno al coronavirus primero debemos distinguir distintos casos de monitorización entre las iniciativas que se han propuesto durante estos últimos meses, que podrían clasificarse de la siguiente manera:

- Las *aplicaciones de autoevaluación* como *CoronaMadrid* o *Stop covid-19 CAT* de Cataluña. Se trata de aplicaciones que piden de manera opcional el número de teléfono móvil y la localización para determinar en qué comunidad autónoma nos encontramos. Estas aplicaciones no geolocalizan la posición del usuario de manera continua.
- Las *aplicaciones de control de cuarentena* como las que hemos visto en *Corea del Sur* o la española *Open Coronavirus*. Se trata de aplicaciones que pueden solicitar acceso al GPS del móvil y sirven a las autoridades para saber si el infectado ha salido de casa.
- El *estudio de movilidad* que ha trabajado el Gobierno junto al INE, donde se utilizarán los datos anonimizados de las operadoras. Este estudio se encuentra en línea con la iniciativa gestionada por la Comisión Europea donde se ha seleccionado un operador de cada país. En total, *ocho grandes operadores* (Telefónica, Vodafone, Deutsche Telekom, Orange, Telecom Italia, Telenor, Telia y Telekom Austria) cederán sus datos para realizar un seguimiento del flujo de movilidad de la población.
- Y las *aplicaciones de rastreo de contactos* (aplicaciones móviles de trazabilidad de contactos) varias de ellas basadas en Bluetooth. Aquí se engloban iniciativas como *TraceTogether de Singapur* o *PEPP-PT* y el más reciente, Radar Covid[4]. El objetivo es identificar a las personas que hayan estado en contacto.

---

dado que nuestro ordenamiento europeo e interno así lo permite. En este sentido vid. por todos MARTÍNEZ MARTÍNEZ, R., "Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública", *Diario La Ley*, núm. 9601, Sección Doctrina, 25 de marzo de 2020.

3. Sobre los conceptos de Epidemia y Pandemia, así como sobre la Red de Vigilancia de Salud Pública, prevista en el art. 13.3 de la Ley 33/2011 vid. el interesante trabajo de BESTARD PERELLÓ, J., "La pandemia del COVID-19 y el tratamiento de datos personales (I)", *Actualidad del Derecho Sanitario*, núm. 283, (Julio-agosto 2020), pp. 845 a 849.
4. En septiembre de 2020 esta aplicación está implantada en Alemania, Dinamarca, Suiza, Estonia, Irlanda y Portugal. En España se está implantando. La Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA) ha lanzado la aplicación Radar COVID, desarrollada en colaboración con Indra Sistemas, S.A. La aplicación se lanzó en Google Play, el 29 de junio

Tanto en el ámbito europeo (el Parlamento, la Comisión y el Comité Europeo de Protección de Datos, CEPD) como en el ámbito interno español (la AEPD) se ha determinado que existen base jurídica para hacer posible el tratamiento de datos para contribuir a la gestión de la crisis contra la COVID-19. En este sentido, el Comité Europeo de Protección de Datos ha subrayado que el marco jurídico de la protección de datos "fue diseñado como un instrumento flexible que, por tanto, puede aportar una respuesta eficiente en la contención de la pandemia y, al mismo tiempo, proteger los derechos humanos y las libertades fundamentales"[5].

Por tanto, la protección de datos no debe ser un obstáculo para limitar la efectividad de las medidas que adopten las autoridades, especialmente las sanitarias, en la lucha contra la pandemia[6].

No obstante, tanto las instituciones europeas, como la propia AEPD, han señalado la importancia que tiene que en este tratamiento de datos se respeten unas garantías mínimas. En este trabajo se realizará una exposición esquemática de esas garantías mínimas a las que no se puede renunciar, pues su renuncia supondría renunciar a nuestro Estado de Derecho.

En orden al respeto de unas garantías en el tratamiento de los datos personales en la gestión de la pandemia, lo primero que habría que señalar es que el marco jurídico en el que se adoptan las medidas de excepción tiene que mantener su conexión con el Derecho y con el orden constitucional[7] (en el que se regula las garantías de los derechos fundamentales y el sistema de fuentes). Se consideran en estos casos admisibles las

---

2020, y se inició una prueba piloto en La Gomera. Tras analizar los resultados del piloto, considerados positivos, la SEDIA ha puesto la aplicación a disposición de todos los españoles, supeditada a su previa integración por parte de los servicios de salud de las Comunidades Autónomas. La aplicación ha sido descargada ya por más de 3,4 millones de españoles, y está integrada en más de la mitad de las Comunidades Autónomas. Radar COVID es ya parte de la nueva generación de infraestructura de sanidad pública. El 1 de septiembre de 2020, la Secretaría de Estado de Digitalización e Inteligencia Artificial ha anunciado que el código de la aplicación se abrirá al público el día 9 de septiembre 2020.

5. Vid. Directrices 04/2020 del Comité Europeo de Protección de Datos, de 21 de abril, sobre el uso de datos de localización de herramientas de rastreo de contactos en el contexto de pandemia de COVID-19, pueden consultarse en línea en: *https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_es.pdf*.
6. En este mismo sentido se pronuncia la AEPD en su informe de 12 de marzo de 2020, en el que *analiza el tratamiento de datos personales en relación con la situación derivada de la extensión del virus COVID-19*, disponible en: *https://www.aepd.es/es/documento/2020-0017.pdf*. En concreto, en este informe con base en el art. 6.1.e) y d), se afirma: "… el RGPD contiene reglas necesarias para permitir legítimamente tratamiento de datos personales en situaciones de emergencia sanitaria", a lo que añade que "en consecuencia, la protección de datos no debería utilizarse para obstaculizar o limitar la efectividad de las medidas que adopten las autoridades". En los primeros momentos de la pandemia, en el mismo sentido se pronunciaron autores como MARTÍNEZ MARTÍNEZ, R., "Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública", *Diario La Ley*, núm. 9601, Sección Doctrina, 25 de marzo de 2020.
7. Muy acertadamente así lo señala ESTEVE PARDO, J., "La apelación a la ciencia en el Gobierno y gestión de la crisis COVID-19", *Revista de Derecho Público: Teoría y Método*, vol. 2, 2020, p. 42.

medidas que excepcionan un régimen jurídico sectorial[8]. "Otra cosa es la excepción de un régimen general, básico, de enunciado constitucional, articulado fundamentalmente en torno a unos derechos y libertades fundamentales, también a unos deberes, afirmados con carácter general y básico"[9].

II. TRATAMIENTOS DE DATOS PERSONALES EN SITUACIONES DE EMERGENCIA

Como se acaba de señalar, el Reglamento general de protección de datos (RGPD) contiene las reglas necesarias para permitir legítimamente tratamientos de datos personales en situaciones en las que existe una emergencia sanitaria de alcance general. El RGPD reconoce explícitamente en su Considerando 46 la base jurídica para el tratamiento lícito de datos personales en casos excepcionales[10] como el control de epidemias y su propagación: la misión realizada en interés público (art. 6.1.c) y e); o los intereses vitales del interesado u otras personas físicas [art. 6.1.d)][11].

En lo que concierne a los datos de salud, estos datos están catalogados en el RGPD como categorías especiales de datos a los que se aplica una especial protección, por lo que se prohíbe su tratamiento salvo que pueda ampararse en alguna de las excepciones recogidas en el artículo art. 9.2. RGPD:

- El cumplimiento de obligaciones en el ámbito del Derecho laboral y de la seguridad y protección social [art. 9.2.b)][12].

---

8. Respecto de esta distinción entre las medidas sectoriales y las medidas que afectan al estatus general de los derechos incide NOGUEIRA LÓPEZ, A., "Confinar el virus. Entre el viejo derecho sectorial y el derecho de excepción", *El Cronista del Estado Social y Democrático de Derecho*, núm. 86-87 (2020), pp. 6 a 22.
9. Vid. ESTEVE PARDO, J., "La apelación a la ciencia…", op.cit., p. 42.
10. En concreto, el Considerando (46) del Reglamento (UE) 2016/679 dice, en relación con las epidemias:

    "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".
11. Sin perjuicio de que puedan existir otras bases jurídicas como, por ejemplo, el cumplimiento de una obligación legal (para el empleador en la prevención de riesgos laborales de su personal). Estas bases jurídicas permiten el tratamiento de datos sin consentimiento de los afectados.
12. En materia de prevención de riesgos laborales existen obligaciones tanto para los empleadores como su personal, de tal manera que corresponde a cada trabajador velar por su propia seguridad y salud en el trabajo y por la de aquellas personas a las que pueda afectar su actividad profesional a causa de sus actos y omisiones en el trabajo. Ello supone que el personal 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

- El interés público en el ámbito de la salud pública [art. 9.2.i)], que en este caso se configura como interés público esencial [art. 9.2.g)].
- Cuando sea necesario para la realización de un diagnóstico médico [art. 9.2.h)].
- Cuando el tratamiento es necesario para proteger intereses vitales del interesado o de otras personas, cuando el interesado no esté capacitado para prestar su consentimiento [art. 9.2.c)].

En lo que se refiere al ámbito interno español, se optó en marzo por afrontar la gestión de la Pandemia desde la aplicación de la Ley Orgánica 4/1981, de 1 de junio, de los Estados de Alarma, Excepción y Sitio, que autoriza al Gobierno para dictar las medidas necesarias a fin de contener la pandemia. En concreto, su art. 11 a) autoriza al Gobierno, con una formulación muy abierta, para "limitar la circulación o permanencia de personas o vehículos en horas y lugares determinados, o condicionarlas al cumplimiento de ciertos requisitos". En aplicación de esta Ley por Real Decreto 463/2020, de 14 de marzo, se declaró el Estado de Alarma por la COVID-19 (que fue sucedido por el Real Decreto 514/2020 y el Real Decreto 537/2020)[13].

---

para que se puedan adoptar las medidas oportunas. Así lo recuerda la AEPD en su informe de 12 de marzo de 2020, en el que *analiza el tratamiento de datos personales en relación con la situación derivada de la extensión del virus COVID-19*, disponible en: *https://www.aepd.es/es/documento/2020-0017.pdf*.

13. Sobre la excepcionalidad que conlleva la declaración del Estado de Alarma vid. VELASCO CABALLERO, F., "Estado de Alarma y distribución territorial del poder", *El Cronista del Estado Social y Democrático de Derecho*, núm. 86-87 (2020), pp. 66 a 78 y VELASCO CABALLERO, F., "Derecho Local y COVID-19", *Revista Galega de Administración Pública (REGAP)*, núm. 59 (2020), pp. 5 a 33. Ha sido cuestionado la sucesión de prorrogas del Estado de Alarma, dado que tiene marcados en la propia normativa que se aplica unos límites temporales claros (art. 6.2 Ley Orgánica 4/1981, prescribe que será por 15 días que sólo se podrá prorrogar con autorización expresa del Congreso que establecerá el alcance y las condiciones vigentes durante la prórroga). De forma inédita se ha prorrogado cuatro veces sin fijarse un plazo límite claro, cuando "el Estado de Alarma, por su grave y generalizada afectación a los derechos fundamentales, así como la profunda alteración al orden competencial (la nota más característica del Estado de Alarma ha sido subordinación de todas las autoridades de España a las decisiones del Gobierno) comporta una sustancial modificación de la Constitución", así lo afirma muy atinadamente ESTEVE PARDO, J., "La apelación a la ciencia…", op. cit. pp. 43 y 44. Por todo ello, el Estado de Alarma tiene que tener un carácter claramente provisional y no debería utilizarse como un medio ordinario para la gestión de la crisis epidémica. Así ha sido señalado por CRUZ VILLALÓN, P., "Estados excepcionales y suspensión de garantías", Tecnos, Madrid, 1984. Algunos autores defendieron la procedencia de la declaración del Estado de Excepción, por todos, ALEGRE ÁVILA, J.M, y SÁNCHEZ LAMELAS, A., "Nota en relación a la crisis sanitaria generada por la actual emergencia vírica", se puede consultar en *http://www.aepda.es/AEPDAEntrada-2741-Nota-en-relacion-a-la-crisis-sanitaria-generada-por-la-actual-emergencia-virica.aspx*.

Este tiempo de provisionalidad ha dado lugar al planteamiento de una multitud de recursos y demandas, un exhaustivo recorrido se encuentra en FERNÁNDEZ DE GATTA SÁNCHEZ, D., "El Estado de Alarma y las medidas contra el coronavirus ante jueces y tribunales", *Diario La Ley*, núm. 9651, sección Tribuna, 11 de junio de 2020.

Además, el art. 12 de la Ley Orgánica 4/1981 remite directamente a lo que establecen las leyes sanitarias[14]. Esta remisión hay que entenderla dirigida, en la actualidad, al art. 3 de la Ley orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública[15], y al art. 54 de la Ley 33/2011, de 4 de octubre, General de Salud Pública. La primera establece: "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". Por su parte, el art. 54 de la Ley 33/2011, de 4 de octubre, General de Salud Pública autoriza a adoptar "cuantas medidas sean necesarias para asegurar el cumplimiento de la ley". Ambos preceptos recogen una cláusula muy abierta[16] que permiten la adopción de medidas no tasadas para afrontar una situación de emergencia que, por definición, se caracterizan por su imprevisibilidad. Esta normativa (Ley Orgánica 4/1981 y Ley Orgánica 3/1986), que permite poner límite a derechos fundamentales, como la libre circulación, ha sido la que se ha seguido aplicando por las diferentes Comunidades Autónomas una vez finalizada la vigencia del Estado de Alarma[17].

14. Sobre la virtualidad de estas normas vid. el interesante artículo de NOGUEIRA LÓPEZ, A., "Confinar el virus…", op. cit., pp. 6 a 22.
15. Modificada mediante Real Decreto-ley 6/2020, de 10 de marzo, por la que se adoptan medidas urgentes en el ámbito económico y para la protección de la salud pública.
16. En este sentido, el art. 14 Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana y el art. 7 bis de la Ley 17/2015, del Sistema Nacional de Protección Civil establecen que para situaciones de emergencia en general, ante posibles peligros y riesgos para el orden público o para los derechos fundamentales, las leyes deben contener cláusulas generales de actuación gubernativa, que permitan actuaciones muy diversas en función de cuál sea el riesgo o peligro emergente cada caso concreto.
17. Una vez finalizado el Estado de Alarma se han seguido adoptando medidas que limitan seriamente los derechos fundamentales a través de normas que no tienen el rango normativo (normas reglamentarias) que exige la Constitución de 1978. Estas normas, en algunos casos, se han sometido a la previa ratificación por los Tribunales Contencioso-Administrativos, en aplicación de los arts. 8.6 y 10.8 LJCA. Considero que es muy cuestionable la procedencia de esta ratificación por los tribunales, dado que no se trata de actos administrativos cuya ejecución forzosa se controla sino de disposiciones administrativas de carácter reglamentario (normas) y los tribunales no son cotitulares de la potestad reglamentaria para que puedan "entrar a colaborar" con el ejecutivo autonómico en la aprobación de dichas normas reglamentarias. Con esta ratificación entiendo que se compromete la separación de poderes. En este mismo sentido se ha venido pronunciando incansablemente el profesor Juan Manuel ALEGRE ÁVILA: "Inadmisión de la solicitud gubernativa de ratificación jurisdiccional de las medidas sanitarias adoptadas por razón de la crisis vírica [Una nota a propósito del Auto del Juzgado de lo Contencioso-Administrativo número 1 de Logroño 102/2020, de 22 de septiembre (JUR 2020, 290463)]", publicado el 27 de septiembre de 2020; "Una sucinta nota en relación a la intervención jurisdiccional sobre las decisiones del poder ejecutivo que inciden en la libertad y o derechos fundamentales de los ciudadanos", publicado el 30 de septiembre de 2020; y "Denegación judicial de ratificación de medidas sanitarias y declaración de estado de alarma", publicado el 11 de octubre de 2020. Todos estos trabajos están disponibles en internet en: *http://www.aepda.es/AEPDACategoria-92-Otras%20publicaciones.aspx*.

En materia de riesgo de transmisión de enfermedades, epidemia y crisis sanitarias esta normativa citada, interpretada de forma sistemática, otorga a las autoridades sanitarias de las distintas administraciones públicas las competencias para adoptar las medidas necesarias previstas por la ley cuando así lo exijan razones sanitarias de urgencia o necesidad. Desde un punto de vista de tratamiento de datos personales, la protección de los intereses vitales de las personas físicas corresponde, en el ámbito de la salud, a las distintas autoridades sanitarias de las diferentes administraciones públicas, quienes podrán adoptar las "medidas necesarias" para salvaguardar la salud de las personas en situaciones de emergencia sanitaria, incluso cuando ello suponga un tratamiento de datos personales de salud[18]. Estas autorizaciones legales generales dan entrada al protagonismo del principio de proporcionalidad a la hora de la toma de decisiones por parte del Gobierno y la Administración Pública que adoptan las "medidas de alarma". Más adelante nos adentraremos en este aspecto.

Pero todo ello sin olvidar que, como señala la propia AEPD[19], los tratamientos de datos personales, aún en estas situaciones de emergencia sanitaria, deben seguir siendo tratados de conformidad con la normativa de protección de datos personales (RGPD y Ley Orgánica 3/2018, de protección de datos personales y garantía de los derechos digitales), ya que estas normas han previsto esta eventualidad, por lo que le son de aplicación sus principios, y entre ellos el de tratar los datos personales con licitud, lealtad y transparencia, limitación de la finalidad (en este caso, salvaguardar los intereses de las personas ante esta situación de pandemia), principio de exactitud, y el principio de minimización de datos.

III. DESARROLLOS TECNOLÓGICOS PARA EL CONTROL Y SEGUIMIENTO DE LA PANDEMIA POR LA COVID-19 Y LA GARANTÍA DEL DERECHO A LA PROTECCIÓN DE DATOS

La gestión de la pandemia ha generado múltiples iniciativas y pronunciamientos en el ámbito europeo (Comité Europeo de Protección de Datos, Comisión Europea,

Sobre las medidas que se han venido adoptando para combatir la pandemia son muy reveladores los trabajos de COTINO HUESO, L., "Confinamientos, libertad de circulación y personal, prohibición de reuniones y actividades y otras restricciones de derechos por la pandemia del Coronavirus", Diario La Ley, núm. 9608, 2020 y FERNÁNDEZ DE GATTA SÁNCHEZ, D., "Los problemas de las medidas jurídicas contra el coronavirus: las dudas constitucionales sobre el Estado de Alarma y los excesos normativos", Diario La Ley, núm. 9641, 2020.

18. Vid. Informe de la AEPD de 12 de marzo de 2020, en el que *analiza el tratamiento de datos personales en relación con la situación derivada de la extensión del virus COVID-19*, se puede consultar en: *https://www.aepd.es/es/documento/2020-0017.pdf*. Del mismo modo, y en aplicación de lo establecido en la normativa de trabajo y de prevención de riesgos laborales, los empleadores podrán tratar, de acuerdo con dicha normativa y con las garantías que dichas normas establecen, los datos necesarios para garantizar la salud de todo su personal, y evitar contagios en el seno de la empresa y/o centros de trabajo.
19. Vid. El Informe de la AEPD de 12 de marzo de 2020, en el que *analiza el tratamiento de datos personales en relación con la situación derivada de la extensión del virus COVID-19*, se puede consultar en: *https://www.aepd.es/es/documento/2020-0017.pdf*.

Parlamento Europeo) y en el ámbito interno español (AEPD), para garantizar la protección de datos personales a la vista de los desarrollos tecnológicos que se han puesto al servicio de la gestión de la crisis, centrados principalmente en dos grandes grupos: control de la temperatura y aplicaciones móviles dedicadas al seguimiento de la COVID-19.

Tal y como señala el Comité Europeo de Protección de Datos (CEPD)[20] el tratamiento automatizado de datos y las tecnologías digitales pueden ser componentes esenciales de la lucha contra la COVID-19. No obstante, debemos ser cautelosos con el carácter irreversible de ciertas medidas. Es nuestra responsabilidad garantizar que cada una de las medidas adoptadas en estas circunstancias extraordinarias sea necesaria, limitada en el tiempo y de alcance mínimo, y que se someta a una verdadera revisión periódica y a evaluación científica.

1. EL CONTROL DE LA TEMPERATURA MANUAL O MEDIANTE CÁMARAS TÉRMICAS

El día 30 de abril 2020, la Agencia Española de Protección de Datos, publicó en su web el Comunicado de la AEPD en relación con la toma de temperatura por parte de comercios, centros de trabajo y otros establecimientos[21]. La AEPD mediante este documento hace pública su preocupación por la aplicación de estas medidas que pueden ir en contra de la protección de los datos de las personas. Es decir, alerta a las Administraciones Públicas de la dudosa legalidad de la toma de la temperatura a las personas por parte de comercios, centros de trabajo y otros establecimientos.

La AEPD entiende que esta acción, la toma de temperatura en espacios públicos, tendría efectos sobre ciertos derechos inalienables. Esta toma de datos relativos a la salud de las personas además de devenir en eventuales denegaciones de acceso (centro laboral, educativo o comercial) desvelaría a terceros la temperatura corporal de la persona interesada[22], lo que estaría por encima del estándar establecido por lo que se contraviene el RGPD. No cumpliría el principio de confidencialidad, artículo 5.5 y artículo 36.1.c) del Reglamento (UE) 2016/679.

Afirma la AEPD que, en todo caso, tal y como establece el art. 9.2.i) RGPD cualquier acción en este sentido requeriría una regulación legislativa que establezca la existencia de intereses generales en el terreno de la salud pública que deben ser protegidos y a los que contribuye esta medida y que determine las garantías adecuadas y específicas para proteger el derecho a la protección de datos: estableciendo límites y garantías, plazos de

20. Vid. Directrices 04/2020 del Comité Europeo de Protección de Datos, de 21 de abril, sobre el uso de datos de localización de herramientas de rastreo de contactos en el contexto de pandemia de COVID-19.
21. Se puede consultar en línea: *https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-aepd-temperatura-establecimientos*.
22. Este tratamiento de toma de temperatura supone una injerencia particularmente intensa en los derechos de los afectados. Por una parte, porque afecta a datos relativos a la salud de las personas, que son datos especialmente protegidos, no sólo porque el valor de la temperatura corporal es un dato de salud en sí mismo sino también porque, a partir de él, se asume que una persona padece o no una concreta enfermedad, como es en estos casos la infección por coronavirus.

conservación y de destrucción de los datos, para el tratamiento de los datos personales relativos a la salud de las personas afectadas, tal como consta en el artículo 9.2, letras g), h) e i) del RGPD[23].

La toma de temperatura puede realizarse de forma manual o a través de medios tecnológicos. Las cámaras de video sensibles a los rayos infrarrojos, cámaras térmicas[24], son uno de estos elementos tecnológicos cuyos datos están bajo el manto normativo del RGPD. En el caso de que la técnica de toma del dato fuera la de la cámara, activa otro principio del RGPD, el principio de limitación de la finalidad y minimización de datos, artículo 5.1.b) del Reglamento (UE) 2016/679[25], de tal modo que bajo ningún concepto, estos datos obtenidos mediante cámaras podrían ser usados para otro fin o lo que es peor, no podría usarse el dispositivo (cámaras térmicas) para captar o tratar otros datos distintos a la temperatura corporal de la persona.

Otro principio del Reglamento (UE) 2016/679, el principio de exactitud de los datos, artículo 5.1.d), obligaría a que la norma de legitimación que debería aprobarse a instancia del Ministerio de Sanidad incluyera las condiciones de calibración y recalibración de los medidores.

En cuanto al consentimiento de las personas, este no sería un criterio legitimador del artículo 6.1.a) del Reglamento (UE) 2016/679, dado que incumpliría la exigencia de ser un consentimiento libremente dado, con base en el artículo 7.4. RGPD. Un consentimiento dado bajo la amenaza de denegación de un derecho (del derecho al acceso), no se considera un consentimiento libremente dado[26].

No obstante, se considera que, en algún caso (sería necesario analizarlo de forma individualizada), podría justificarse la toma de temperatura a clientes o visitantes en el

23. La AEPD, el 7 de mayo de 2020, publicó un estudio en el que analiza distintas tecnologías para luchar contra el coronavirus y sus riesgos para la privacidad, entre ellas analiza las cámaras de infrarrojos para la realización de lecturas masivas de temperatura manifestando *su preocupación por el uso de estos dispositivos y la necesidad de contar con el criterio previo de las autoridades sanitarias antes de proceder a su instalación*. Alerta de un posible riesgo de discriminación, de difusión pública de datos de salud y de crear una falsa sensación de seguridad que facilite el contacto con personas realmente infectadas.
24. Dichas cámaras identifican mediante algoritmos de inteligencia artificial los rostros humanos, los discriminan del resto de elementos que aparecen en la imagen y revelan la temperatura corporal aproximada de cada individuo.
25. Este principio hace constar que: "recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales".
26. Para que el consentimiento sea válido debe consistir en una manifestación de voluntad libre, específica, informada e inequívoca. El RGPD ha dejado bien claro que el consentimiento no debe considerarse libremente prestado cuando no se goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno (considerando 42), o cuando exista un desequilibro claro entre las partes (considerando 43).

cumplimiento de la legislación de prevención de riesgos laborales[27]. Esto no ocurrirá en todos los casos, sino solo cuando el contacto entre cliente y empleados sea más estrecho y en atención a las demás circunstancias existentes. Además, será necesario valorar si existen otras medidas menos invasivas de la intimidad. Esta aproximación, no obstante, requiere de una adecuada ponderación entre el impacto sobre los derechos de los clientes o usuarios de estas medidas y el impacto en el nivel de protección de las personas empleadas. Esa ponderación debe basarse en diferentes factores. Ante todo, los criterios establecidos por las autoridades sanitarias. Pero también los relacionados con el mayor o menor riesgo que se pueda producir en cada caso concreto o con la posibilidad de aplicar medidas alternativas de protección para el personal. Por ejemplo, el riesgo será menor en un establecimiento en el que las personas empleadas estén físicamente separadas de la clientela que en otro en que esa barrera física no exista o sea más precaria.

2. COVID-19: LOS ESTABLECIMIENTOS COMERCIALES SOLO PODRÁN TOMAR LA TEMPERATURA A LOS CLIENTES SI LAS AUTORIDADES SANITARIAS PUBLICAN UNA NORMA QUE FIJE LOS REQUISITOS, SEGÚN LA AEPD

Las aplicaciones móviles dedicadas al seguimiento de la COVID-19.

Las aplicaciones y tecnologías para controlar los patrones de propagación de la pandemia por COVID-19 *podrían desempeñar un papel clave en la lucha contra la pandemia*, no obstante su utilización debe realizarse sin quebrantar las garantías mínimas que protegen el derecho a la intimidad.

Las tecnologías más destacadas hasta la fecha son las aplicaciones que tienen la función de comprobación de síntomas[28] y las aplicaciones que tienen las funcionalidades de rastreo de contactos[29].

27. Y es que en lo que respecta a la toma de temperatura en el marco laboral, se considera que el tratamiento jurídico podría ser distinto dado que podría encajar dentro de lo dispuesto en el artículo 9.2.b) con base en las obligaciones que tiene el empleador en cuanto a la seguridad y protección de la salud del trabajador. Vid el art. 15 de la Ley 31/1995, de 8 de noviembre, de prevención de riesgos laborales. Al respecto, precisa la AEPD, en el informe que publico el 7 de mayo de 2020, en el que analiza distintas tecnologías para luchar contra el coronavirus y sus riesgos para la privacidad, que en algunos entornos, como el de la normativa de prevención de riesgos laborales, la toma de la temperatura podría ser de utilidad dentro del marco de un tratamiento más extenso del que formen parte otras comprobaciones y garantías adicionales que, en todo caso, respeten los derechos y libertades establecidos en el RGPD.
28. Es una herramienta que permite a las autoridades sanitarias públicas proporcionar a los ciudadanos orientaciones sobre las pruebas de la COVID-19 e información sobre el autoaislamiento, la manera de evitar la transmisión a otras personas y el momento en que deben pedir asistencia sanitaria.
29. Las funcionalidades de rastreo de contactos y alerta son herramientas que permiten identificar a las personas que han estado en contacto con alguien infectado por la COVID-19 e informarles de las medidas que conviene adoptar después, como someterse a autocuarentena o a pruebas, o proporcionar asesoramiento sobre qué hacer en caso de experimentar tal o cual síntoma.

Ambas funcionalidades pueden ser una fuente pertinente de datos para las autoridades sanitarias públicas, además de facilitar la transmisión de ese tipo de datos a las autoridades epidemiológicas nacionales y al Centro Europeo para la Prevención y el Control de las Enfermedades. Y, en combinación con las estrategias de pruebas adecuadas, pueden proporcionar información sobre el nivel de circulación del virus y ayudar a determinar el efecto de las medidas de distanciamiento físico y de confinamiento.

2.1. Criterios de interpretación marcados por la Unión Europea

En el ámbito Europeo[30] se han producido comunicaciones tanto por parte del Parlamento Europeo, como de la Comisión Europea, además de Directrices dictadas por el Comité Europeo de Protección de Datos[31].

El *Parlamento Europeo, mediante resolución, de 17 de abril de 2020,* recalcó la necesidad de que estas aplicaciones estén diseñadas cuidadosamente para no exponer los datos confidenciales de los usuarios y cumplir plenamente con la legislación de protección de datos y privacidad. Además, señalo que el uso de aplicaciones no debería ser obligatorio y que deberían incluir cláusulas de cancelación para que concluyan una vez que termine la pandemia, además de que se garantice que los datos sean anónimos. Y, por último, para limitar el riesgo potencial de abuso, los datos generados no deberían almacenarse en bases de datos centralizadas.

Por su parte, el documento de la *Comisión Europea "Orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia del COVID-19 en lo referente a la protección de datos", Bruselas, 16 de abril 2020 (Comunicación 2020/C 124 I/01 de la Comisión, DOUE de 17 de abril de 2020)*[32] detalla una serie de elementos que han de servir de orientación sobre la manera de limitar la intrusión en la privacidad de las funcionalidades de las aplicaciones y, de este modo, garantizar el cumplimiento de la legislación de la UE en materia de protección de datos personales y de la intimidad:

– Las autoridades sanitarias nacionales deberían aprobar las aplicaciones, además de ser responsables del cumplimiento de las normas de protección de datos personales de la UE. Para ello, los estados miembros deben aprobar un

30. Vid. PADÍN, A., "COVID-19. Opiniones de las autoridades de supervisión europeas en materia de protección de datos personales". Disponible en *http://www.padin.com/2020/03/listado-de-recursos-online-con-las.html*.

31. Vid. Directrices 04/2020 del Comité Europeo de Protección de Datos, de 21 de abril, sobre el uso de datos de localización de herramientas de rastreo de contactos en el contexto de pandemia de COVID-19 y Directrices 03/2020 del Comité Europeo de Protección de Datos, de 21 de abril, sobre el tratamiento de datos relativos a la salud con fines de investigación científica en el contenido del brote de COVID-19.

32. La Comisión ha elaborado sus Orientaciones partiendo de la Recomendación adoptada por la Comisión el 8 de abril de 2020, relativa a un conjunto de instrumentos comunes de la UE para la utilización de la tecnología y los datos a fin de combatir y superar la crisis de la COVID-19, en particular en lo que respecta a las aplicaciones móviles y a la utilización de datos de movilidad anonimizados.

instrumentario legislativo nacional, que constituirá la "base jurídica" para el tratamiento de los datos por parte de las autoridades sanitarias nacionales. Esta normativa legal debe contener medidas específicas y adecuadas para salvaguardar los derechos y las libertades de los titulares de los datos relativos a la salud (que, además, son datos especialmente protegidos). Esta base jurídica contribuiría a la seguridad jurídica.

- Los usuarios mantienen el control total de los datos personales. La instalación de la aplicación debe ser voluntaria y debe desmontarse tan pronto como ya no sea necesaria.
- Limitación del acceso a los datos y su divulgación.
- Limita el uso de datos personales: solo datos relevantes para el propósito en cuestión, y no debe incluir el seguimiento de la ubicación.
- Límites estrictos en el almacenamiento de datos: los datos personales no deben conservarse más tiempo del necesario.
- Seguridad de los datos: los datos deben almacenarse en el dispositivo de un individuo y encriptarse.
- Las autoridades nacionales de protección de datos deben involucrarse y consultarse por completo.
- Interoperabilidad: las aplicaciones deberían ser utilizables a través de las fronteras de la UE. La Comisión aprobó el 13 de mayo las directrices de interoperabilidad aplicables en la UE a las aplicaciones de rastreo de contactos, determinando que tienen que ser interoperables para que las personas puedan usarlas para recibir alertas en cualquier lugar de Europa en el que se encuentren[33]. Estas *directrices de interoperabilidad* tienen como objetivo permitir que las aplicaciones nacionales funcionen perfectamente entre sí, al tiempo que cumplen con los estándares de privacidad y protección de datos.

El Comité Europeo de Protección de Datos (CEPD) aprobó las Directrices 04/2020 del Comité Europeo de Protección de Datos, de 21 de abril, sobre el uso de datos de localización de herramientas de rastreo de contactos en el contexto de pandemia de COVID-19[34]. Estas directrices determinan las condiciones y principios que deben guiar el uso proporcionado

33. En junio de 2020, cuando los Estados miembros comenzaron a suavizar las restricciones de viaje, *acordaron que se mantendría un intercambio de información seguro entre las aplicaciones nacionales de rastreo de contactos*.
34. Pueden consultarse en línea en: *https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_es.pdf*. Con la misma fecha de 21 de abril, el Comité Europeo de Protección de Datos publicó también las "Directrices 03/2020 del, de 21 de abril, sobre el tratamiento de datos relativos a la salud con fines de investigación científica en el contenido del brote de COVID-19", disponibles en línea en: *https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_es.pdf*.

de datos de localización y de herramientas de rastreo de contactos para dos fines específicos[35], a saber:

– El *uso de datos de localización* para apoyar la respuesta a la pandemia mediante la modelización de la propagación del virus, a fin de evaluar la eficacia global de las medidas de confinamiento;

– El *rastreo de contactos*, cuyo objetivo es que las personas que hayan estado muy cerca de alguien que resulte ser portador confirmado del virus sean informadas al respecto, a fin de romper las cadenas de transmisión lo antes posible.

Estas aplicaciones deben formar parte de una estrategia global de salud pública dirigida a combatir la pandemia que incluya, entre otras cosas, la realización de pruebas de detección y el subsiguiente rastreo manual de contactos para eliminar las dudas.

El uso de estas aplicaciones debe ser voluntario y no puede basarse en el rastreo de movimientos individuales, sino más bien en información sobre la proximidad de los usuarios.

Como el virus no conoce de fronteras, el CEPD se inclina por adoptar un enfoque europeo común en respuesta a la crisis actual o, por lo menos, establecer un marco interoperable.

Los principios generales de eficacia, necesidad y proporcionalidad deben dirigir cualquier medida adoptada por los estados miembros o las instituciones de la UE que implique el tratamiento de datos personales para combatir la COVID-19.

Uso de datos de localización

Las directrices señalan las dos fuentes principales de datos de localización[36] disponibles para modelizar la propagación del virus y la eficacia global de las medidas de confinamiento:

– Los datos de localización recogidos por proveedores de servicios de comunicaciones electrónicas (como los operadores de comunicaciones móviles) en el contexto de la prestación de servicios; y

– Los datos de localización recogidos por las aplicaciones de los proveedores de servicios de la sociedad de la información cuya funcionalidad requiere el uso de dichos datos (aplicaciones de navegación, servicios de transporte, etc.).

35. No obstante, asevera el CEPD, que las recomendaciones y obligaciones contenidas en este documento no deben considerarse exhaustivas. Toda evaluación debe realizarse caso por caso, y determinadas aplicaciones podrían requerir la adopción de medidas adicionales no incluidas en estas directrices.

36. Se consideran datos de localización todos los datos contenidos en una red de comunicaciones electrónicas o en un servicio de comunicaciones electrónicas que indican la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público, así como los datos de otras posibles fuentes, relativos a: la latitud, longitud o altitud del equipo terminal; la dirección del desplazamiento del usuario; o el momento en el que se registró la información sobre la localización.

Tal y como señala el CEPD el tratamiento de los datos de localización[37] obtenidos de los proveedores de servicios de comunicaciones electrónicas está sujeto a los límites de los artículos 6 y 9 de la Directiva 2002/58/CE. Esto significa que esos datos solo puede transmitirse a las autoridades o a terceros si han sido anonimizados por el proveedor o, en el caso de los datos que indican la posición geográfica del equipo terminal de un usuario, o de los datos de tráfico, si se cuenta con el consentimiento previo de los usuarios[38]. En todo caso, CEPD afirma que a la hora de utilizar datos de localización, debe darse siempre preferencia al tratamiento de datos anonimizados[39], en lugar de datos personales. Si se trata de datos anonimizados, estos ya no están sujetos a la regulación del RGPD.

Aplicaciones de rastreo de contactos

El CEPD parte de que el seguimiento sistemático y masivo de la localización o los contactos de las personas físicas en el que consiste la funcionalidad de las aplicaciones de rastreo de contactos[40] supone un grave injerencia en su privacidad. Estas prácticas solo pueden legitimarse sobre la base de su adopción voluntaria por parte de los usuarios para cada uno de los fines respectivos, lo que implica, entre otras cosas, que las personas que decidan no utilizar esas aplicaciones, no deben sufrir ninguna desventaja.

Para garantizar la rendición de cuentas, debe definirse con claridad quiénes son los responsables del tratamiento de datos en este tipo de aplicaciones. En opinión del CEPD podrían serlo las autoridades sanitarias nacionales, aunque cabe prever otras fórmulas.

---

37. Vid. art. 2.c) de la Directiva 2002/58/CE.
38. Vid. arts. 6 y 9 de la Directiva 2002/58/CE.
39. Por anonimización se entiende el uso de un conjunto de técnicas destinadas a suprimir la capacidad de asociar los datos a una persona física identificada o identificable mediante un esfuerzo "razonable". Esta "prueba de razonabilidad" debe tener en cuenta tanto los aspectos objetivos (tiempo, medios técnicos) como los elementos contextuales, que pueden variar de un caso a otro (carácter excepcional de un fenómeno teniendo en cuenta, por ejemplo, la densidad de la población y la naturaleza y volumen de los datos). Si los datos no superan esta prueba, no se han anonimizado y, por tanto, se mantienen bajo la aplicación de RGPD. El CEPD hace mucho hincapié en distinguir entre anonimización y seudonimización. Los datos seudonimizados sí entran en el ámbito de aplicación del RGPD. El CEPD afirma que la anonimización eficaz es harto difícil que se consiga y que, en todo caso, no se pueden anonimizar datos aislados; solo son susceptibles de anonimización serie de datos completas. En este sentido, toda intervención en un patrón de datos único (mediante cifrado o cualquier otra transformación matemática) puede calificarse como máximo de seudonimización. Afirma el CEPD que para conseguir la anonimización el tratamiento de los datos de localización ha de ser cuidadoso para superar la prueba de razonabilidad. Y, por último, dada la complejidad de los procesos de anonimización el CEPD recomienda encarecidamente la transparencia en lo que respecta a la metodología de anonimización.
40. También llamadas aplicaciones de trazabilidad de contactos. Las personas que han estado en estrecho contacto (según los criterios que definan los epidemiólogos) con una persona infectada por el virus corren un riesgo significativo de infectarse también y, a su vez, de infectar a otras personas. El rastreo de contactos es una metodología de control de enfermedades que registra a todas las personas que han estado muy cerca de un portador del virus, con el fin de comprobar si están expuestas al riesgo de infección y aplicarles las medidas sanitarias adecuadas.

En lo que concierne al principio de limitación de la finalidad, las finalidades deben ser lo suficientemente específicas como para excluir un tratamiento ulterior con fines ajenos a la gestión de la crisis sanitaria de la COVID-19.

Del mismo modo, se tienen que cumplir el principio de minimización de datos, así como el principio de la protección de datos desde el diseño y por defecto[41]:

- 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;
- Como se trata de aplicaciones que pueden funcionar sin la identificación directa de personas, conviene establecer medidas adecuadas para prevenir la reidentificación;
- La información recogida debe alojarse en el equipo terminal del usuario y solo debe recogerse la información pertinente cuando sea absolutamente necesario.

Una cuestión importante que precisa el CEPD es que el mero hecho de que el uso de tales aplicaciones tenga carácter voluntario no significa que el tratamiento de datos personales se base necesariamente en el consentimiento. Cuando las autoridades públicas prestan un servicio basado en un mandato atribuido por la legislación, y acorde con los requisitos legales vigentes, la base jurídica más adecuada para el tratamiento de datos es la necesidad de cumplir una misión de interés público, es decir, el art. 6.1.e) RGPD.

En este sentido, el art. 6.3 RGPD precisa que la base del tratamiento indicado en el art. 6.1.e) debe ser establecida por el Derecho de la UE o el Derecho de los estados miembros que se aplique al responsable del tratamiento. La finalidad del tratamiento debe estar fijada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1.e), debe ser necesaria para el cumplimiento de una misión realizada en el interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (vid. considerando 41 RGPD).La base jurídica o medida legislativa que proporcione la base legítima para el uso de aplicaciones de rastreo de contactos debe incorporar salvaguardias significativas, incluida una referencia al carácter voluntario de la aplicación. Procede incluir una especificación clara de la finalidad y limitaciones explícitas respecto a la utilización ulterior de datos personales, y debe identificarse con claridad al responsable o los responsables del tratamiento. También deben definirse las categorías de datos y las entidades a las que pueden transmitirse los datos personales, y para qué fines. En función del nivel de interferencia, conviene incorporar salvaguardias adicionales, teniendo en cuenta la naturaleza, el alcance y los fines del tratamiento. Por último, el CEPD recomienda que, en la medida de lo posible, se incluyan los criterios que determinen cuándo se desmantelará la aplicación y qué entidad será responsable de esa determinación y rendirá cuentas al respecto.

41. Vid. Directrices 4/2019 del CEPD sobre la protección de datos desde el diseño y por defecto. Este principio exige que los datos objeto de tratamiento deben reducirse a los mínimos estrictamente necesarios y la aplicación no debe recoger información que no tenga relación con el objeto específico o no sea necesaria.

Además, si el tratamiento de datos se apoya para combatir la pandemia por COVID-19 podría conllevar también la recogida de datos sanitarios (por ejemplo, sobre el estado de una persona infectada). El tratamiento de estos datos está permitido cuando es necesario por razones de interés público en el ámbito de la salud pública y, por tanto, siempre que se cumplan las condiciones del art. 9, 2.i) RGPD, o para los fines de asistencia sanitaria descritos en su art. 9.2.h). En este caso, dependiendo de la base jurídica, el tratamiento de datos podría también fundamentarse en el consentimiento explícito (art. 9.2.a) RGPD).

De conformidad con la finalidad inicial, el art. 9.2.j) RGPD también permite el tratamiento de datos sanitarios cuando resulte necesario para fines de investigación científica o fines estadísticos.

Lo que debe tenerse presente es que la crisis sanitaria actual no ha de servir de oportunidad para establecer mandatos desproporcionados de conservación de datos. En la limitación del almacenamiento han de considerarse las necesidades reales y la importancia médica, y los datos personales solo deben conservarse durante la crisis de la COVID-19. Después, como regla general, todos los datos personales deberían borrarse o anonimizarse.

El CEPD entiende que esas aplicaciones no pueden sustituir, sino meramente apoyar, el rastreo manual de contactos realizado por personal sanitario cualificado (en particular, con entrevistas con personas infectadas) que puede determinar si los contactos estrechos pueden o no dar lugar a una transmisión del virus. Es decir, debe formar parte de un programa de salud pública de mayor alcance. Además, precisa el CEPD, que estas aplicaciones han de utilizarse exclusivamente hasta el momento en que las técnicas de localización manual de contactos puedan gestionar por sí solas el volumen de nuevas infecciones. El CEPD subraya que los procedimientos y procesos ejecutados por las aplicaciones de rastreo de contactos, incluidos sus respectivos algoritmos, han de estar sujetos a una estricta supervisión por parte personal cualificado, a fin de limitar la aparición de falsos positivos y negativos[42]. En concreto, la labor de facilitar asesoramiento sobre los pasos que han de darse a continuación no puede depender exclusivamente de un tratamiento automatizado.

Para asegurar su equidad, la rendición de cuentas y, más en general, su consonancia con la ley, los algoritmos deben ser auditables y han de ser revisados periódicamente por expertos independientes. El código fuente de la aplicación debe hacerse público con miras a un control lo más amplio posible.

Por último, el CEPD considera que ha de llevarse a cabo una evaluación de impacto relativa a la protección de datos (EIPD) antes de empezar a utilizar una aplicación de este

42. Siempre aparecerán falsos positivos, y, teniendo en cuenta que, probablemente, la identificación de un riesgo de infección tendrá repercusiones significativas para la persona afectada (como la de mantenerse aislada hasta dar negativo en una prueba de detección), la capacidad de corregir datos y/o de realizar los consiguientes análisis es necesaria. Lógicamente, esto solo debe aplicarse a los escenarios y usos en los cuales los datos se tratan y/o almacenan de tal manera que este tipo de corrección es técnicamente viable.

tipo por cuanto se considera que el tratamiento puede entrañar un alto riesgo (datos sanitarios, adopción previa a gran escala, seguimiento sistemático, utilización de una nueva solución tecnológica[43]).

Deben aplicarse las técnicas criptográficas más avanzadas para garantizar la seguridad de los datos almacenados en los servidores y aplicaciones y los intercambios entre las aplicaciones y el servidor remoto. También conviene proceder a la autenticación mutua entre la aplicación y el servidor.

La notificación de los usuarios infectados por COVID-19 en la aplicación debe someterse a una autorización adecuada, por ejemplo, mediante un código de un solo uso unido a una identidad seudónima de la persona infectada y vinculado con un laboratorio de pruebas de detección o con un profesional de atención sanitaria. Si no se puede obtener confirmación de forma segura, no debe tener lugar ningún tratamiento de datos que presuponga la validez del estado del usuario. De igual modo, el hecho de que un usuario sea diagnosticado de infección por COVID-19 únicamente se debe comunicar a las personas con las que el usuario haya estado en estrecho contacto dentro del período de conservación de datos que, desde el punto de vista epidemiológico, resulte pertinente a efectos del rastreo de contactos.

A más tardar, cuando las autoridades públicas competentes decidan "volver a la normalidad", debe establecerse un procedimiento para detener la recogida de identificadores (desactivación global de la aplicación, instrucciones para desinstalarla, desinstalación automática, etc.) y para activar la eliminación de todos los datos recogidos de todas las bases de datos (aplicaciones móviles y servidores).

2.2. Criterios de interpretación articulados por la AEPD

Webs y apps que ofrecen autoevaluaciones y consejos sobre el Coronavirus.

La AEPD publicó el 26 de marzo de 2020, un Comunicado sobre apps y webs de autoevaluación del Coronavirus[44]*,* que incide en los criterios que deben aplicarse para que el tratamiento de datos personales de la salud sea lícito.

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

Los fundamentos que legitiman dichos tratamientos de datos personales y de salud por apps o páginas web de autoevaluación son la necesidad de atender las misiones

43. Vid. las Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del RGPD, Grupo de Trabajo del Artículo 29.
44. Disponible en: *https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-apps-webs-autoevaluacion-coronavirus-privacidad*.

realizadas en interés público, así como la de garantizar los intereses vitales de los propios afectados o de terceras personas. Las finalidades para las que pueden tratarse los datos son, únicamente, las relacionadas con el control de la epidemia, entre ellas, las de ofrecer información sobre el uso de las aplicaciones de autoevaluación realizadas por las administraciones públicas o la obtención de estadísticas con datos de geolocalización agregados para ofrecer mapas que informen sobre áreas de mayor o menor riesgo.

Los datos que pueden obtenerse y utilizarse han de ser los que las autoridades públicas competentes consideren proporcionados y necesarios para cumplir con dichas finalidades.

Estos datos sólo podrán ser facilitados por quienes sean mayores de 16 años. En el caso de tratar datos de menores de 16 años, se requeriría de la autorización de sus padres o representantes legales.

Únicamente podrán tratar dichos datos las autoridades públicas competentes[45] para actuar conforme a la declaración del Estado de Alarma, es decir, el Ministerio de Sanidad y las Consejerías de Sanidad de las Comunidades Autónomas, que podrán cederse datos entre ellas, y a los profesionales sanitarios que traten a los pacientes o que intervengan en el control de la epidemia. Las entidades privadas que colaboren con dichas autoridades sólo podrán utilizar los datos conforme a las instrucciones de estas y, en ningún caso, para fines distintos de los autorizados.

En cuanto a la previsión de que todos aquellos ciudadanos que hayan dado positivo en la prueba del COVID-19 puedan ser geolocalizados a través del teléfono móvil que hayan facilitado previamente, de modo que se pueda llevar a cabo un seguimiento de su cuarentena, hay que partir de nuevo de las amplias competencias que en situaciones excepcionales, como sin duda lo es la presente epidemia, tienen las autoridades sanitarias, teniendo en cuenta, además, que una de las medidas excepcionales para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 es la de limitar la libertad de circulación de las personas.

No obstante, el único dato que a los efectos de la geolocalización debería facilitarse a los operadores de telecomunicaciones, en su caso, sería el correspondiente al número de teléfono móvil que se tiene que geolocalizar, salvo que el Ministerio de Sanidad considerara que fuera imprescindible facilitar algún otro dato a los efectos del seguimiento de la enfermedad.

En todo caso, quienes pretendan obtener y tratar los datos de los ciudadanos deberán informarles de forma clara, accesible y fácilmente comprensible de todos los aspectos que se han descrito.

2.3. Aplicaciones de rastreo de contactos

La AEPD, el 7 de mayo de 2020, publicó un estudio en el que analiza distintas tecnologías para luchar contra el coronavirus y sus riesgos para la privacidad[46]. En este estudio realiza

45. Si los ciudadanos utilizan aplicaciones o webs de las que no son titulares las autoridades públicas, sino que son ofrecidos por entidades o personas privadas, no concurrirá la legitimidad para el tratamiento de los datos.
46. Disponible en: *https://www.aepd.es/sites/default/files/2020-05/analisis-tecnologias-COVID19.pdf*.

un análisis preliminar de siete sistemas: geolocalización recogida por los operadores de telecomunicaciones; geolocalización en redes sociales; apps, webs y chatbots para autotest o cita previa; apps de información voluntaria de contagios; apps de seguimiento de contactos por Bluetooth; pasaportes de inmunidad y cámaras infrarrojas.

En el documento, la Agencia pone de manifiesto que nos encontramos en un punto de inflexión crítico, no solo debido a la situación de pandemia, sino en relación con nuestro modelo de derechos y libertades[47].

La AEPD recuerda que la utilización de la tecnología no puede ser entendida de forma aislada, sino en el marco de un tratamiento de datos personales con un propósito claramente definido. En la medida en que este propósito debe ser para la lucha efectiva contra la COVID-19, el tratamiento ha de implementar una estrategia coherente basada en evidencias científicas, evaluando su proporcionalidad en relación con su eficacia y eficiencia y teniendo en cuenta de forma objetiva los recursos organizativos y materiales necesarios. En todo caso, la utilización de estas tecnologías debe realizarse en el marco de los criterios establecidos por las autoridades sanitarias y, en particular, del Ministerio de Sanidad. Además, como en cualquier tratamiento de datos personales, deben cumplirse los principios establecidos en el Reglamento General de Protección de Datos (RGPD).

En cuanto a las *apps de seguimiento de contactos por Bluetooth*, el informe detalla que los riesgos para la privacidad provienen, entre otros, de la posible realización de mapas de relaciones entre personas, la reidentificación por localización implícita, la recogida de datos de terceros o la fragilidad de los protocolos a la hora de intercambiar información. Cuanto mayor sea el tratamiento que se realice en un servidor que recoja los datos de los usuarios, menos control tienen éstos sobre sus propios datos, por lo que las soluciones centralizadas siempre parecen menos respetuosas con la privacidad que las distribuidas. Otras de las amenazas, debida a la acumulación de los datos de forma centralizada, pueden ser; que se produzca un abuso, se amplíen los propósitos del tratamiento o se sufra una quiebra de seguridad.

El documento precisa que el éxito de este tipo de soluciones se basa en factores que no dependen sólo de la tecnología. Existen otros factores determinantes para su eficacia, como, por ejemplo, la implicación de un elevado número de usuarios o la garantía de una declaración responsable. Finalmente, es necesario disponer de acceso a una comprobación fiable del estado de salud para poder actualizar la información recogida por estos sistemas y que, además, se realice periódicamente, especialmente para aquellos que sean notificados de haber estado en contacto con un infectado.

47. El 11 de junio de 2020 la AEPD informó que había recibido 86 reclamaciones por el tratamiento de datos relacionados con el COVID-19, manteniendo a su vez 14 actuaciones de investigación en marcha. Sobre esta información se puede consular en: *https://www.europapress.es/sociedad/noticia-aepd-recibe-86-reclamaciones-tratamiento-datos-relacionados-covid-19-20200611163944.html*.

Ha de señalarse del mismo modo que en junio de 2020 la AEPD publicó las *Recomendaciones de la Agencia Española de Protección de Datos (AEPD), de junio de 2020, para el despliegue de aplicaciones móviles en el acceso a espacios públicos*[48].

Las recomendaciones contenidas en esta nota de la AEPD están dirigidas a los tratamientos basados en apps no sanitarias como las de reserva o control de aforo en playas, espacios naturales y otros lugares públicos y se cifran en las que siguen:

- La finalidad debe estar claramente definida y limitarse a la gestión de medidas de control de aforo.
- La implementación de tratamientos basados en apps deberá fundamentarse en un análisis de necesidad y proporcionalidad que determine tanto la utilización de la app como el conjunto de datos mínimo necesario para conseguir los fines que se persiguen.
- Las funcionalidades de la app deben ser exclusivamente las necesarias para las finalidades concretas que se persiguen, no mezclando funcionalidades como fidelización, publicidad o redes sociales.
- El uso de la app debe ser de carácter voluntario, basado en el consentimiento del usuario para el tratamiento de los datos personales necesarios para cada una de las funcionalidades que se persiguen. Y debe concurrir un consentimiento libre, informado y específico.
- El responsable del tratamiento será la Administración Pública que deberá garantizar el cumplimiento de los principios del RGPD y Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPD) en todos los tratamientos que se realicen.
- Los datos personales tratados no deben almacenarse más allá del tiempo necesario para cumplir con las finalidades que se persiguen y en todo caso deben ser eliminados cuando estas se extingan.

IV. LAS GARANTÍAS DEL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL QUE DEBEN TENERSE EN CUENTA CUANDO ENTRA EN COLISIÓN CON OTRO DERECHO O BIEN JURÍDICAMENTE PROTEGIDO

En el tiempo durante el que estuvo vigente el Estado de Alarma se han dictado un elevado número de normas de rango reglamentario con base en el Real Decreto 463/2020[49], como la Orden SND/297/2020, de 27 de marzo, del Ministerio de Sanidad por

48. Disponible en: *https://www.aepd.es/sites/default/files/2020-06/recomendaciones-apps-espacios-publicos.pdf*.
49. La proliferación de normativa tras la declaración del Estado de Alarma ha llevado a que a mediados de mayo de 2020 fueran más de 200 las normas dictadas al respecto: 13 Decretos-Leyes; 6 Reales

la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA), del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19.

Esta Orden Ministerial en su punto segundo sobre DataCOVID-19: estudio de la movilidad aplicada a la crisis sanitaria, determina:

> "Encomendar a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, siguiendo el modelo emprendido por el Instituto Nacional de Estadística en su estudio de movilidad y a través del cruce de datos de los operadores móviles, de manera agregada y anonimizada, el análisis de la movilidad de las personas en los días previos y durante el confinamiento.
>
> En la ejecución de este estudio, se velará por el cumplimiento de lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE; la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos[50]".

Ante esta norma nos podemos plantear la siguiente pregunta: ¿Se trata de una norma con rango normativo suficiente dado que afecta directamente al derecho fundamental a protección de datos[51]?

Nos proponemos dar respuesta a esta pregunta en el presente apartado.

En esta crisis por la COVID-19 las medidas que se han adoptado persiguen una finalidad constitucional y legítima: la preservación del derecho a la vida y la protección de la salud pública. Pero la forma en que se han adoptado ¿han podido suponer una vulneración de los principios fundamentales del Estado de Derecho?

Partimos de que, conforme a los artículos 9 y 53 CE, todos los poderes públicos, incluidas las diferentes Administraciones Públicas, se encuentran vinculados por los derechos fundamentales. La función que cumplen los derechos fundamentales en la estructura de la Constitución es, *prima facie,* establecer para los ciudadanos espacios de autodeterminación de la conducta, indisponibles a todos los poderes públicos. Se configuran, así como ámbitos de autodeterminación, de libertad subjetiva (dimensión

---

Decretos, incluidos los que activó el Estado de Alarma y sus cuatro prórrogas; 113 Órdenes Ministeriales; 71 Resoluciones de Ministerios (más una del Banco de España), y cinco Instrucciones.

50. Aunque la Orden SND/297/2020 no lo diga expresamente, como se ha señalado, es el artículo 6 del Reglamento (UE) 2016/679 y el artículo 8 de la Ley Orgánica 3/2018, los que legitiman la excepción de estas normas.

51. Algunos autores han planteado esta misma cuestión sobre la insuficiencia del rango normativo reglamentario en la regulación de medidas que afectan a los datos de carácter personal, en este sentido vid. BESTARD PERELLÓ, J., "COVID-19 y pruebas diagnósticas y protección de datos personales", *OTROSÍ*, 7.ª Época, núm. 6 (Número especial dedicado a Justicia y Derecho en tiempos de pandemia), (Julio 2020), pp. 62 a 65.

subjetiva de los derechos). Por ello, los derechos fundamentales son origen inmediato de derechos y obligaciones y no meros principios programáticos.

Cualquier cuestión relativa a derechos fundamentales en el marco de nuestro Estado constitucional de derecho debe ser analizada teniendo en cuenta cuatro premisas. La primera, que ninguno de ellos es absoluto o ilimitado. Todos los derechos son limitados y además pueden entrar en conflicto unos con otros. El derecho a la vida puede así limitar el derecho a la protección de datos de carácter personal. La segunda, que no existe una jerarquía de derechos fundamentales que permita de forma automática establecer en caso de conflicto la prevalencia de uno sobre otro. La igualdad de valor y rango de todos los derechos fundamentales exige llevar a cabo en cada caso conflictivo una ponderación. La tercera, que las limitaciones de derechos fundamentales tienen que ser establecidas por normas con rango de Ley que han de respetar el contenido esencial de aquellos. Sólo así se garantiza que el Parlamento –los representantes de los ciudadanos– legitima democráticamente la limitación. En consecuencia, en ningún caso es admisible que un Gobierno dicte normas de rango reglamentario para establecer con carácter general limitaciones de derechos. La cuarta y última, que el régimen de los derechos fundamentales está reservado a la Ley Orgánica, es decir, a las Cortes Generales. Las comunidades autónomas no tienen competencia para establecer dicho régimen.

En lo que a este estudio nos interesa, a raíz de la pandemia por la COVID-19 se plantea un conflicto entre dos bienes jurídicamente protegidos. En este caso, dos derechos: derecho a la protección de datos de carácter personal (art. 18 CE) *versus* derecho a la salud (art. 43 CE). La resolución de este conflicto se debe afrontar desde dos planos perfectamente diferenciables: el plano normativo (regulación del derecho) y el plano en la aplicación del Derecho (de las normas vigentes).

1. PLANO NORMATIVO (REGULACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS)

En este plano las claves que se tienen que tener presentes son:

- Rango normativo de la norma que regula el derecho fundamental: reserva de Ley (art. 53.1 CE y art. 81 CE, que determina que tiene que ser regulado por Ley Orgánica). Se admite la colaboración reglamentaria siempre que sea claramente dependiente y subordinada a la ley (SSTC 83/1984 (RTC 1994, 83), 111/2014 (RTC 2014, 111) y 139/2016 (RTC 2016, 139)). Jerarquía normativa: el reglamento no puede modificar lo establecido en la ley.
- Respeto al contenido esencial por el legislador (STC 76/2019 (RTC 2019, 76)).

1.1. La reserva de ley en la regulación de los derechos fundamentales

La Constitución establece una reserva de Ley, arts. 53.1 y 81 CE para el establecimiento de la regulación esencial y límites de cada derecho fundamental del Capítulo II del Título I[52]. Conforme a la jurisprudencia constitucional (entre otras, STC 14/2014

52. Por el contrario, los derechos reconocidos en el Capítulo III del Título I, como el derecho a la salud, no están sometidos a esa reserva de Ley.

(RTC 2014, 14)), toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas que incida directamente sobre su desarrollo (art. 81.1 CE, Ley Orgánica) o límite o condicione su ejercicio (art. 53.1 CE, Ley Ordinaria, estatal o autonómica en función de la competencia material *ex* arts. 148 y 149 CE), precisa de una habilitación legal. La reserva de Ley se configura, así, como requisito para garantizar formal y materialmente la seguridad jurídica en el ámbito de los derechos fundamentales y las libertades públicas. Por ello, debe ser la Ley la que defina las modalidades y extensión del ejercicio del poder otorgado con la suficiente claridad para aportar al individuo una protección adecuada contra la arbitrariedad. En este sentido resulta muy reveladora la STC 76/2019, de 22 de mayo (RTC 2019, 76)[53] que se detiene a analizar las exigencias para que el legislador respete la reserva de ley en materia de protección de datos de carácter personal[54].

En este sentido, la STC 76/2019 (RTC 2019, 76) sienta los siguientes parámetros que tiene que cumplir la disposición legal para que respete la reserva de Ley en materia de datos personales:

– Debe determinar por sí misma la finalidad del tratamiento de datos personales, sin que baste por sí sola la genérica mención al "interés público" (FJ 7º).

53. Esta STC (RTC 2019, 76) analiza la constitucionalidad de Ley Orgánica 3/2018, de protección de datos y garantía de los derechos digitales, que introdujo un nuevo artículo 58 bis en la Ley Orgánica 5/1985 del régimen electoral general que en su apartado 1 disponía que "La recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas". Es decir, se permitía a los partidos políticos recabar datos personales de cualquier fuente (internet, redes sociales, páginas web, tratamientos no automatizados…) con el fin de perfilar a las personas en función de sus opiniones políticas, y todo ello sin el consentimiento de las personas afectadas. Dicha previsión no se encontraba en el proyecto de ley que el Gobierno remitió al Congreso en noviembre de 2017, sino que se introdujo a través de la enmienda n.º 331 presentada por el Grupo Parlamentario Socialista en el Congreso de los Diputados durante la tramitación parlamentaria de la Ley. Hay que decir que el texto final fue aprobado por unanimidad de todos los diputados. Sobre el art. 58. bis de la Ley Orgánica 5/1985 vid. los siguientes trabajos: POLO ROCA, A., "Protección de datos y elaboración de perfiles: el nuevo artículo 58.bis de la Ley Orgánica 5/1985, de 19 de junio, del régimen electoral general", *Revista Galega de Administración Pública* (REGAP), núm. 58 (julio-diciembre 2019), pp. 507-527; y PASCUA MATEO, F.A., "Un nuevo capítulo en la tutela del derecho a la protección de datos personales: los datos de contenido político. Comentario a la Sentencia del Tribunal Constitucional 76/2019, de 29 de mayo (RTC 2019, 76), en el recurso de inconstitucionalidad núm. 1405-2019 (BOE núm. 151, 25 de junio de 2019", *Revista de las Cortes Generales*, núm. 106, Primer semestre (2019), pp. 549 a 558.

54. En palabras del Tribunal (FJ 2º): "El enjuiciamiento constitucional que nos demanda la impugnación central se circunscribe, pues, a resolver si el legislador ha vulnerado la reserva de ley y el contenido esencial del derecho fundamental a la protección de datos personales (art. 18.4 CE en conexión con el art. 53. l CE), por renunciar a establecer el marco en el que se habilita el tratamiento, la finalidad del mismo y las garantías adecuadas frente al concreto uso de la informática previsto en la norma impugnada".

– Debe limitar el tratamiento regulando pormenorizadamente las restricciones al derecho fundamental. De otra manera no se cumple con las exigencias de certeza y precisión que cabe exigir (FJ 7º).

– Debe establecer las garantías adecuadas para proteger los derechos fundamentales afectados. Y, desde luego, "la previsión de las garantías adecuadas no puede deferirse a un momento posterior a la regulación legal del tratamiento de datos personales de que se trate (mediante normas reglamentarias o de incluso normas de rango inferior al reglamentario, como una Circular o Instrucción[55]. Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado" (FFJJ 7º y 8º). De ninguna manera basta con una remisión implícita al RGPD y a la LOPD: la insuficiencia de la ley no puede ser colmada por vía interpretativa a partir de las pautas e indicaciones que se puedan extraer de los citados textos normativos. Tampoco puede ser colmada por el titular de una potestad normativa limitada como es la Agencia Española de Protección de Datos o mediante una interpretación conforme[56]. Finalmente, una remisión implícita como la pretendida tampoco resultaría coherente con el marco regulador europeo. No puede admitirse una hipotética remisión al Reglamento Europeo y a la nueva Ley Orgánica de Protección de Datos, pues esto equivaldría a una suerte de "remisión en blanco"[57] que dejaría en manos, no del legislador, sino exclusivamente a disposición de la determinación reglamentaria del Gobierno o bien, en

55. En el caso enjuiciado por la STC (RTC 2019, 76) se aprobó la Circular 1/2019 por parte de la AEPD, que, en palabras del TC en STC 76/2019 (RTC 2019, 76) en ningún caso puede colmar la insuficiencia legal del precepto impugnado. Desde la perspectiva de la Administración, la primera garantía de los derechos fundamentales frente a la Administración Pública es el respeto a la reserva de Ley, a la que se superpone el respeto al principio de legalidad. Ello supone la ilegalidad de cualquier regulación adoptada por la Administración (estatal, autonómica o local) que carezca de la necesaria cobertura legal que afecte a un derecho fundamental. Así lo reitera el Tribunal Constitucional (STC 83/84 (RTC 1984, 83), reiterado en sentencias recientes como SSTC 111/2014 (RTC 2014, 111) y 139/2016 (RTC 2016, 139)). Al respecto, vid., por todos, MENÉNDEZ REXACH, A., "Ley y Reglamento en España", en Rosado Pacheco, S. (coord..): Derecho Europeo Comparado sobre Ley y Reglamento, Madrid, 2003, pp. 93 a 119 y 193 a 196.

56. La técnica de la "interpretación conforme" no es admisible pues no estamos ante "varias interpretaciones posibles igualmente razonables", sino ante la insuficiencia de regulación detectada en una norma de desarrollo de un derecho fundamental.

57. Aclara la STC 76/2019 (RTC 2019, 76) que el Reglamento General de Protección de Datos establece las garantías mínimas, comunes o generales para el tratamiento de datos personales que no son especiales. En cambio, no establece por sí mismo el régimen jurídico aplicable a los tratamientos de datos personales especiales, ni en el ámbito de los Estados miembros ni para el Derecho de la Unión. Por tanto, si la norma interna que regula el tratamiento de datos personales relativos a opiniones políticas (el nuevo artículo 58 bis de la Ley 5/1985), no prevé esas garantías adecuadas, sino que, todo lo más, se remite implícitamente a las garantías generales contenidas en el Reglamento General de Protección de Datos, no puede considerarse que haya llevado a cabo la tarea normativa que aquel le exige.

ausencia de este último, del aplicador del derecho, la determinación de cuáles de las garantías previstas en ambas normas de remisión resultan aplicables al tratamiento en cuestión.

En resumen, la STC 76/2019 (RTC 2019, 76) es contundente y de manera pormenorizada señala que los arts. 18.4 en conexión con el 53.1 de la CE exige, para que el legislador respete la reserva de ley en materia de protección de datos de carácter personal, la suficiente adecuación de la norma legal a los requerimientos de: a) certeza en la recopilación y tratamiento de los datos personales; b) la determinación de la finalidad del tratamiento; y c) la existencia de las garantías adecuadas o las mínimas exigibles por la Ley.

1.2. La limitación de los derechos fundamentales. Contenido esencial

El TC ha reiterado que los derechos fundamentales no son ilimitados (STC 96/2010 (RTC 2010, 96)). Todo derecho tiene sus límites (internos), impuestos por razones de interés generales o de protección de otros bienes constitucionales. En unos casos son fijados directamente por la propia Constitución[58], mientras que en otras ocasiones tales límites o restricciones se contienen en la ley que regula el concreto derecho fundamental o en otra Ley que limite el contenido de este derecho. En el caso que estamos analizando, podrían ser leyes sanitarias en relación con el RGPD y la Ley Orgánica 3/2018, de protección de datos personales y garantía de los derechos digitales. La constitucionalidad de tales límites radica en que esos límites legales respeten a su vez el contenido esencial del derecho (art. 53.1 CE) y sean proporcionados. Entramos en el terreno de la ponderación en la regulación del derecho (ponderación por el legislador). Al legislador se le exige que sus decisiones sean ponderadas en su resultado[59]. Las exigencias de esta ponderación puede llegar a suponer un límite negativo del ejercicio de su competencia normativa o legislativa[60]. En materia de derechos fundamentales, la especial sujeción a los mismos que impone el art. 53.1 CE hace que la competencia del legislador para regular su ejercicio se vea sometida a condicionamientos más estrictos que los que encuentran los órganos legislativos en otros ámbitos materiales. La posibilidad de ponderar por parte del legislador para establecer límites a los derechos fundamentales está estrictamente condicionada. En efecto, en primer término, el contenido de los derechos fundamentales, en principio, sólo pueden limitarse en virtud de una ponderación con otros bienes,

58. Vid. por ejemplo, el art. 18 CE, inviolabilidad del domicilio, salvo existencia de un delito flagrante.

59. La ponderación como resultado se refiere a la ponderación de la decisión en sí misma, es decir, a la solución correctamente argumentada, conforme al criterio de que cuanto mayor sea el grado de perjuicio del principio que ha de retroceder, mayor ha de ser la importancia del cumplimiento del principio que prevalece. Vid. RODRÍGUEZ DE SANTIAGO, J.M, "La ponderación de bienes e intereses en el Derecho administrativo", Marcial Pons, Madrid, 2000, pp. 48 y 49.

60. No hay que olvidar que existen ámbitos vedados a la ponderación por el legislador; son aquellos en los que la propia Constitución ha adoptado una decisión precisa relativa a la precedencia de un principio sobre otro que cierra la vía a ulteriores decisiones impuestas por ley. Es el caso del art. 18.2 CE. Vid. STC 341/1993, de 18 de noviembre (RTC 1993, 341), FJ 8 A) y B).

derechos o principios que cuenten con reconocimiento constitucional[61]. Como consecuencia de esa ponderación podrá resultar el establecimiento por el legislador de límites a un derecho fundamental justificados por la necesidad de dar prevalencia, en determinadas circunstancias, al derecho, bien o principio constitucional que se encuentra en situación de tensión o contraposición con aquél.

En segundo lugar, es constitucionalmente obligado que la decisión del legislador por la que se establezca límites a un derecho fundamental por exigencias derivadas de otro derecho fundamental, o de otro bien o principio con apoyo constitucional sea, en sí misma (en su resultado), ponderada. Esto es, la decisión a la que aquí se alude ha de cumplir con lo que se ha denominado "ley de ponderación", esto es: cuanto mayor sea el grado de perjuicio del derecho fundamental de que se trate, mayor ha de ser la importancia del cumplimiento del bien, derecho o principio contrapuesto[62]. Esta exigencia forma parte del contenido del principio de proporcionalidad, que, como se sabe, vincula al legislador en el ejercicio de su competencia a la hora de establecer límites en los ámbitos de libertad de los ciudadanos para permitir la satisfacción de otros bienes constitucionalmente amparados.

Y, en tercer lugar, hay que conjugar la exigencia de la "ley de la ponderación" con la exigencia del respeto al "contenido esencial". En algún caso en el que, sin duda, fuera posible argumentar que la importancia del cumplimiento de cierto bien constitucional es tal que justifica una determinada restricción en un derecho fundamental (esto es, que se cumple con la "ley de la ponderación"), habría que considerar contraria a la Constitución la limitación a este derecho si con ella se traspasa la línea de lo que deba considerarse como contenido esencial del mismo (art. 53.1 CE).

Las limitaciones establecidas por la Ley en ningún caso puede afectar al contenido esencial del derecho fundamental (límite de los límites)[63]. En el caso del derecho a la

---

61. Vid. MEDINA GUERRERO, M., "La vinculación negativa del legislador a los derechos fundamentales", Madrid, 1996, págs. 71,72, 75,89 y 115. Vid. STC 120/1990, de 27 de junio (RTC 1990, 120), FJ 8 y STC 57/1994, de 28 de febrero (RTC 1994, 57), FJ 6.
62. Vid. RODRÍGUEZ DE SANTIAGO, J.M., "La ponderación de bienes e intereses…", op. cit., p. 61.
63. La STC 101/1991 (RTC 1991, 101) ha precisado que el concepto de contenido esencial sólo es aplicable a los derechos del Capítulo I y del Capítulo II del Título I CE. Está conformado por aquella parte del derecho (facultades) que es ineludiblemente necesaria para que su titular pueda satisfacer los intereses para cuya consecución el derecho se otorga. En este sentido, la STC 112/2006 (RTC 2006, 112) precisa que "La determinación del contenido esencial de cualquier tipo de derecho subjetivo –y, por tanto, también de los derechos fundamentales de la persona- viene marcada en cada caso por el elenco de facultades o posibilidades' de actuación necesarias para que el derecho sea recognoscible como perteneciente al tipo descrito y sin las cuales deja de pertenecer a eses tipo y tiene que pasar a quedar comprendido en otro, desnaturalizándose, por decirlo así. Todo ello referido al momento histórico de que en cada caso se trata y a las condiciones inherentes a las sociedades democráticas cuando se trate de derechos constitucionales". Del mismo modo, se define también por el TC el contenido esencial como "aquella parte del contenido del derecho que es absolutamente necesaria para que los intereses jurídicamente

protección de datos de carácter personal (art. 18 CE), la STC 76/2019, de 22 de mayo (RTC 2019, 76), ha fijado con precisión cual es el alcance del contenido esencial del derecho a la protección de datos de carácter personal. En cuanto al contenido esencial del derecho a la protección de datos el TC, remitiéndose a la capital STC 292/2000 (RTC 2000, 292), recuerda que consiste en un "poder de disposición y de control sobre los datos personales" y que tiene "una doble perspectiva": "El art. 18.4 CE no solo consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona' (SSTC 11/1998, de 13 de enero (RTC 1998, 11), FJ 5; 96/2012 (RTC 2012, 96), FJ 6; y 151/2014, de 25 de septiembre (RTC 2014, 151), FJ 7), sino también, como se desprende de su último inciso (para garantizar […] el pleno ejercicio de sus derechos'), un derecho instrumental ordenado a la protección de otros derechos fundamentales, esto es, un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos' (STC 292/2000, de 30 de noviembre (RTC 2000, 292), FJ 5)". El derecho así concebido no tiene carácter absoluto, claro está. Puede estar sujeto a límites, pero éstos han de respetar al menos dos requisitos: primero, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas debe responder a un fin constitucionalmente legítimo o encaminarse a la protección o la salvaguarda de un bien constitucionalmente relevante; segundo, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas, ora incida directamente sobre su desarrollo (art. 81.1 CE), ora limite o condicione su ejercicio (art. 53.1 CE), precisa una habilitación legal. Es pues necesario que una ley defina los límites de los derechos y en particular del derecho a la protección de datos. Pero esta ley, para cumplir con el principio de seguridad jurídica, debe cumplir al menos dos exigencias: previsibilidad y certeza de las medidas restrictivas en el ámbito de los derechos fundamentales. Es decir, la ley que limite un derecho fundamental ha de establecer las garantías mínimas exigibles y adecuadas que permitan dicho límite sin menoscabar el contenido esencial del derecho.

2. PLANO APLICACIÓN DEL DERECHO VIGENTE. EL JUICIO DE PROPORCIONALIDAD Y LA PONDERACIÓN

Cuando, en la aplicación de una determinada norma, se establece que cuando exista un conflicto entre dos derechos la Administración puede limitar uno de esos derechos en favor del otro, esta limitación no constituirá una vulneración cuando resista un juicio de ponderación[64]. Todo acto o resolución que limite derechos fundamentales ha de asegurar que las medidas limitadoras sean "necesarias para conseguir el fin perseguido" (SSTC 62/1982 (RTC 1982, 62), FJ 5º) y ha de atender a la "proporcionalidad entre el sacrificio

protegibles, que dan vida al derecho, resulten real, concreta y efectivamente protegidos. De este modo, se rebasa o se desconoce el contenido esencial cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección".

64. Vid. art. 4 de la Ley 40/2015, de 1 octubre, de Régimen Jurídico del Sector Público.

del derecho y la situación en que se halla aquel a quien se le impone" (STC 37/1989 (RTC 1989, 37), FJ 7º).

El principio de proporcionalidad requiere que cualquier decisión que afecte a los derechos fundamentales de los particulares sea la estrictamente indispensable para la consecución de otros derechos o valores constitucionales a los que la limitación sirve. Estos tres subprincipios se enunciaron por primera vez en la STC 66/1995 (RTC 1995, 66): toda medida restrictiva debe ser *idónea, necesaria, y ponderada*[65]:

1. Idoneidad o juicio de adecuación: Para adoptar una medida restrictiva de un derecho, ésta debe ser adecuada e idónea, es decir, apta para lograr la finalidad legítima prevista por la norma.

2. Necesidad o juicio de indispensabilidad: Si la finalidad es legítima y la norma adecuada, se procede a analizar si la medida es la menos gravosa para la consecución del fin, identificando su existen otras menos lesivas.

3. Proporcionalidad en sentido estricto o ponderación: Deben valorarse los intereses en presencia a fin de determinar si la injerencia en el derecho ocasiona más beneficios en el interés que se intenta proteger que daños en el derecho afectado. La ponderación, en cuanto método de resolución de la colisión entre derechos fundamentales o bienes constitucionales implica establecer un orden de preferencia relativo para el concreto supuesto, y de acuerdo a las concretas circunstancias presentes. Y tal orden se establece idealmente a través de tres fases sucesivas:

   1.ª Se identifican los principios (valores, bienes, intereses) en conflicto[66].

   2.ª Se atribuye a cada uno de ellos la importancia que le corresponda, según las circunstancias del caso[67].

---

65. Vid. RODRÍGUEZ DE SANTIAGO, J.M., "La ponderación de bienes e intereses…", op. cit., pp. 121-138.

66. El presupuesto de cualquier ponderación es el conflicto entre dos (o más) principios. En relación con cada posible medida contra el contagio, es necesario identificar qué concretos bienes y derechos (en principio, constitucionales) entran en conflicto, y en qué medida los sacrificios en unos compensan los beneficios en otros. Esto es lo que se ha llamado la "regla de oro de la ponderación". No se incluyen los llamados "falsos problemas de ponderación", que se refieren a la delimitación del ámbito que protegen las normas. En este sentido puede citarse como un falso problema de ponderación, si una información no cumple los requisitos mínimos para considerarla veraz, no se encuentra protegida por el art. 20.1.d CE. Por tanto, no podrá plantearse una ponderación con la intimidad. Esta primera fase, donde se identifican los principios en conflicto, es fundamental para la solución de la ponderación. Piénsese, por ejemplo, en que la solución puede ser distinta si en un conflicto frente al honor o intimidad, se contrapone la libertad de expresión o la libertad de información. La solución correcta de un caso de ponderación depende fundamentalmente de la adecuada identificación de los principios en conflicto.

67. En esta fase se trata de argumentar sobre el peso o la importancia atribuible a cada uno de los principios en conflicto, teniendo en cuenta las circunstancias concretas del caso. Estos

3.ª Se otorga prevalencia a uno (o unos) sobre el otro (los otros). Juicio de proporcionalidad en sentido estricto[68].

Las exigencias de la ponderación para los órganos aplicativos del Derecho presentan peculiaridades con respecto a las que se imponen al legislador. La exigencia de ponderación por el Gobierno y la Administración supone una imposición positiva de un riguroso deber de motivación racional de sus decisiones estructurada en el cumplimiento de una serie de fases, es lo que se ha distinguido como "ponderación como procedimiento" en el que hay que explicitar los principios en conflicto, atribuir importancia a cada uno de ellos conforme a una correcta argumentación que debe recogerse en el correspondiente acto jurídico-público como fundamentación. Esta distinción tiene consecuencias porque si se trata de ponderación en la aplicación del derecho, la falta del requisito formal de la ponderación (ponderación como procedimiento) supone la vulneración del derecho fundamental. Esta ponderación con sus tres fases se tiene que evidenciar en la motivación suficiente de la decisión o acto administrativo (art. 35 de la Ley 39/2015, de 1 octubre, del Procedimiento Administrativo Común de las Administraciones Públicas).

3. RECAPITULACIÓN. EL PRINCIPIO DE PROPORCIONALIDAD. LA FIGURA JURÍDICA EN LA QUE SE SUSTENTAN LAS DECISIONES NORMATIVAS Y RESOLUTIVAS ANTE LAS SITUACIONES DE EMERGENCIA. APLICACIÓN A LAS MEDIDAS QUE IMPLICAN USOS DE DATOS PERSONALES PARA LA GESTIÓN DE LA PANDEMIA

Tal y como se ha señalado en este trabajo, tanto el art. 3 de la Ley orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública como el art. 54 de la Ley 33/2011, de 4 de octubre, General de Salud Pública, contienen en su redacción una cláusula muy abierta que permiten la adopción de "medidas necesarias", no tasadas,

---

argumentos pueden basarse en datos de hecho extraídos de las circunstancias del caso, argumentos de derecho que apoyen uno u otro principio, etc. Hay que tener en cuenta que lo que se ponderan son los principios, derechos, valores o intereses protegidos por el ordenamiento. Los hechos, como tales, ni se ponderan ni pueden ponderarse. Aunque sí se pueden utilizar para dar prevalencia a un derecho o a un interés (con apoyo normativo) sobre otro.

68. Tercera fase: decisión de prevalencia conforme al criterio de que "cuanto mayor sea el grado de perjuicio a uno de los principios mayor ha de ser la importancia del cumplimiento de su contrario". En esta fase se llega a la decisión de hacer prevalecer un derecho, principio, interés, etc., frente al otro (u otros), que retroceden. Esta decisión tiene su fundamento, principalmente, en la segunda fase de la ponderación. La solución del conflicto debe cumplir el criterio (ley de la ponderación) de que cuanto mayor sea el grado de perjuicio del principio que retrocede mayor debe ser la importancia del que prevalece en el caso determinado. Como resultado de cada ponderación es posible formular una regla de prevalencia condicionada, en la que se expresen las condiciones bajo las que se ha dado prevalencia a un principio frente al otro. Esta regla permite un cierto grado de generalización o abstracción que facilita su aplicación a futuros conflictos planteados en términos semejantes a los del caso que se acaba de resolver. Pero si los hechos son sustancialmente distintos, la nueva ponderación efectuada puede arrojar un resultado diverso.

para afrontar una situación de emergencia que por definición se caracterizan por su imprevisibilidad. Estas determinaciones contenidas en la Ley conlleva que el aplicador de estos artículos, el Gobierno o la Administración, tendrán que adoptar medidas necesarias proporcionales[69] de acuerdo con las circunstancias que tendrán que ser motivadas de forma suficiente siguiendo las tres fases del procedimiento de ponderación[70], en el caso de que tal motivación concurra, la medida será ajustada al ordenamiento jurídico y en el caso en el que esté en juego la limitación de un derecho fundamental dicha limitación será proporcional. Y, en este contexto, ninguna medida puede considerarse a priori y per sé ilegal e inconstitucional, siempre claro está, en el caso del derecho a la protección de datos de carácter personal se respete las garantías mínimas contenidas en el RGPD y Ley Orgánica 3/2018, de protección de datos personales y garantía de los derechos digitales, con los presupuestos establecidos en la referenciada STC 76/2019 (RTC 2019, 76), ya aquí expuestos.

En el caso contrario, en el que la medida exceda en su contenido por imponer limitaciones al derecho desproporcionados y no justificados de acuerdo con las circunstancias, la medida será ilegal e inconstitucional. Y recalcamos, de acuerdo con las circunstancias, lo que hace que tome una relevancia capital el conocimiento preciso de cada situación concreta. Dicho de otra forma, el principio de proporcionalidad sólo actúa correctamente si hay un conocimiento preciso de cada situación concreta, pues sólo así es posible saber si una limitación del derecho es necesaria. Sólo en cada concreto contexto fáctico es cuando se puede valorar en qué medida una concreta prohibición o limitación es idónea para un concreto fin, no tiene una alternativa menos restrictiva, y contiene un sacrificio justificable por la magnitud del beneficio que produce en otro bien jurídico relevante. Por ello, podríamos decir que, por definición, el principio de proporcionalidad se opone

69. Entiéndase que, en este caso, el principio de proporcionalidad no se aplica al alcance de la autorización legal para adoptar "medidas necesarias", sino para la aplicación de esa autorización legal por el Gobierno o la Administración. Sobre la aplicación del principio de proporcionalidad en la gestión de la pandemia por COVID-19 vid. DE LA SIERRA, S., "Lectura de urgencia de las reacciones frente al COVID-19 desde la óptica jurídica internacional comparada", *El Cronista del Estado Social y Democrático de Derecho*, núm. 86-86, marzo-abril (2020); RICARD MARTÍNEZ MARTÍNEZ, R., "Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública", *Diario La Ley*, núm. 9601, Sección Doctrina, (25 de marzo 2020);ARROYO JIMENEZ, L., "El Derecho público en situaciones de emergencia" (disponible en: *http://www.cepc.gob.es/cepc/blog/blog_cepc/2020/05/04/el-derecho-publico-en-situaciones-de-emergencia*); y VELASCO CABALLERO, F., "Libertad, Covid-19 y proporcionalidad (I): fundamentos para un control de constitucionalidad" (disponible en: *https://franciscovelascocaballeroblog.wordpress.com/2020/05/30/libertad-covid-19-y-proporcionalidad-i-fundamentos-para-un-control-de-constitucionalidad/* y "Libertad, Covid-19 y principio de proporcionalidad (II): indicadores para el control de constitucionalidad." (disponible en: *https://franciscovelascocaballeroblog.wordpress.com/2020/05/31/libertad-covid-19-y-principio-de-proporcionalidad-ii-indicadores-para-el-control-de-constitucionalidad/*).

70. Recordemos: 1.ª: Se identifican los principios (valores, bienes, intereses) en conflicto; 2.ª: Se atribuye a cada uno de ellos la importancia que le corresponda, según las circunstancias del caso; y 3.ª. Se otorga prevalencia a uno (o unos) sobre el otro (los otros). Juicio de proporcionalidad en sentido estricto.

por principio a medidas restrictivas indefinidas. Este conocimiento preciso, en el caso de la situación creada por la COVID-19 ha de entenderse circunscrito al conocimiento posible, dado que no se puede obviar que tanto el juicio de idoneidad como el de necesariedad se realizará en un contexto de incertidumbre sanitaria y científica[71].

En este sentido, el momento de llevar a cabo la recogida de datos, y en particular datos de carácter personal, hay que tener en cuenta que no todos los datos serán de utilidad para hacer frente a una emergencia. No sólo hay que seleccionar las categorías de datos relevantes y adecuadas para el problema que se ha de abordar, sino que hay que extraer datos que sean de calidad, fiables y contrastados. Ese subconjunto de datos que realmente tiene valor se denomina información. La recogida masiva e indiscriminada de datos personales no solo incumple con los principios de necesidad y proporcionalidad, sino que conduce a la generación de ruido, la agresión contra los derechos y libertades de los ciudadanos y el riesgo que dichos datos acaben en las manos equivocadas que, con un plan claro, recursos y decisión suficiente, vuelvan esos datos contra nosotros. El conocimiento es el que permite la toma de decisiones adecuadas[72].

V. UNAS ÚLTIMAS REFLEXIONES Y CONCLUSIONES

De acuerdo con los criterios interpretativos aplicados por el CEPD y la AEPD, en esta situación de pandemia los datos personales deben seguir siendo tratados de conformidad con la normativa de protección de datos personales (RGPD y Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales), ya que estas normas han previsto esta eventualidad (arts. 6 y 9 RGPD). Estos arts. 6 y 9 RGPD son los artículos que proporcionan la base jurídica para que se puedan regular medidas legitimas para el uso de datos de carácter personal para la lucha contra la pandemia[73].

---

71. Y, precisamente, porque se trata de un contexto de incertidumbre sanitaria y científica, entra en juego también el "principio de precaución". La problemática que conlleva la adopción de decisiones públicas en entornos de incertidumbre científica es analizada de forma magistral por ESTEVE PARDO, J. "La apelación a la ciencia…", op. cit. pp. 35 a 50. ESTEVE en este trabajo, muy acertadamente señala (p. 41): "El principio de precaución, al excepcionar el régimen jurídico vigente, conduce a una situación de anomia en la que la única referencia que se reconoce para modular y dimensionar esas medidas de excepción es la que aporta otro principio, muy en boga también, el principio de proporcionalidad. Este principio, el de proporcionalidad, es entonces la única conexión que resta con el Derecho, con el orden jurídico, la única referencia para mesurar y controlar las actuaciones de las autoridades".
72. Así se asevera en la nota publicada por la AEPD el 14 de abril de 2020, sobre "Tratamientos de datos personales en situaciones de emergencia", se puede consultar en: *https://www.aepd.es/es/prensa-y-comunicacion/blog/tratamientos-datos-personales-situaciones-emergencia*.
73. El art. 6.1.e) RGPD establece que el tratamiento de datos personales será lícito si dicho tratamiento es "necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento". El art. 6.3 RGPD precisa que la base del tratamiento indicado en el art. 6.1.e) debe ser establecida por el Derecho de la UE o el Derecho de los estados miembros que se aplique al responsable del tratamiento. La finalidad del tratamiento debe estar fijada en dicha base jurídica o, en lo relativo al tratamiento

La regulación de esas medidas que conlleva el uso de datos personales (art. 6 RGPD), incluso datos personales especialmente protegidos, como los datos de salud (art. 9 RGPD), debería realizarse mediante Ley Orgánica. La STC 76/2019 (RTC 2019, 76) es contundente al respecto, señalando que los arts. 18.4 en conexión con el 53.1 de la CE exige que la norma con rango de ley cumpla con los siguientes parámetros para que se pueda considerar que el legislador respeta la reserva de ley en materia de protección de datos de carácter personal:

- Debe determinar por sí misma la finalidad del tratamiento de datos personales, sin que baste por sí sola la genérica mención al "interés público" (FJ 7º).
- Debe limitar el tratamiento regulando pormenorizadamente las restricciones al derecho fundamental. De otra manera no se cumple con las exigencias de certeza y precisión que cabe exigir (FJ 7º).
- Debe establecer las garantías adecuadas para proteger los derechos fundamentales afectados. Y, la previsión de las garantías adecuadas no puede deferirse a un momento posterior a la regulación legal del tratamiento de datos personales de que se trate (mediante normas reglamentarias o de incluso normas de rango inferior al reglamentario, como una Circular o Instrucción). Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado (FFJJ 7º y 8º). Y, de ninguna manera basta con una remisión implícita al RGPD y a la LOPD: la insuficiencia de la ley no puede ser colmada por vía interpretativa a partir de las pautas e indicaciones que se puedan extraer de los citados textos normativos. Tampoco puede ser colmada por el titular de una potestad normativa limitada como es la Agencia Española de Protección de Datos o mediante una interpretación conforme.

Siendo, por tanto, muy discutible que una norma con rango reglamentario sea suficiente cuando se trata de una norma que va a regular derechos fundamentales, como es la protección de datos de carácter personal, sobre el que la Constitución Española (art. 53 CE) establece una reserva de ley. En los casos de materias reservadas a la Ley, como es este caso, cabe la colaboración reglamentaria, pero siempre que la ley haya

---

a que se refiere el apartado 1.e), debe ser necesaria para el cumplimiento de una misión realizada en el interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (vid. considerando 41 RGPD).

Si el tratamiento de datos para combatir la pandemia de COVID-19 conlleva la recogida de datos de salud (por ejemplo, sobre el estado de una persona infectada). El tratamiento de estos datos está permitido cuando es necesario por razones de interés público en el ámbito de la salud pública y, por tanto, se cumplen las condiciones del art. 9, 2.i) RGPD, o para los fines de asistencia sanitaria descritos en su art. 9.2.h). Dependiendo de la base jurídica, el tratamiento podría fundamentarse también en el consentimiento explícito (art. 9.2.a) RGPD). De conformidad con la finalidad inicial, el art. 9.2.j) RGPD también permite el tratamiento de datos sanitarios cuando resulte necesario para fines de investigación científica o fines estadísticos.

establecido previamente los aspectos nucleares o esenciales de la regulación y siempre que esa regulación reglamentaria sea "claramente dependiente y subordinada a la ley" tal y como viene reiterando de forma asentada y univoca desde la aprobación de la Constitución Española el Tribunal Constitucional[74].

De tal modo, que a las Consejerías de Salud de las distintas Comunidades Autónomas les correspondería la aplicación y ejecución de esa Ley Orgánica aprobada por las Cortes. En ningún caso resultaría admisible que, sin cobertura legal alguna, mediante simples disposiciones reglamentarias autonómicas, se establecieran medidas limitadoras del derecho a la protección de datos personales. En otro caso nos podríamos encontrar ante una conculcación de unas de las garantías jurídicas formales básicas del Estado de derecho: la reserva de ley.

Además, la base jurídica o medida legislativa que proporcione la base legítima para el uso de los datos personales debe incorporar salvaguardias significativas para garantizar los derechos y las libertades de los titulares de los datos. Así es reiterado en las declaraciones interpretativas del CEPD y de la AEPD, en las que se afirma y repite que en esta situación de pandemia los datos personales deben seguir siendo tratados de conformidad con la normativa de protección de datos personales. Lo que supone que, en todo caso, son de aplicación los principios del RGPD, y entre ellos el de tratar los datos personales con: licitud, lealtad y transparencia; limitación de la finalidad (en este caso, salvaguardar los intereses de las personas ante esta situación de pandemia, tratamiento de datos para fines precisos[75]); consentimiento; principio de exactitud[76]; principio de minimización de datos[77]; y la determinación de los plazos de conservación y destrucción de los datos[78].

Todas estas garantías tienen que estar fijadas en la norma legal que regule el uso de datos para combatir la pandemia por COVID-19:

---

74. Vid. STC 83/1984 (RTC 1994, 83), y reiterada en otras recientes, así STC 111/2014 (RTC 2014, 111) y 139/2016 (RTC 2016, 139).
75. Deben definirse las categorías de datos y las entidades a las que pueden transmitirse los datos personales, y para qué fines.
76. Vid. artículo 5.1.d) RGPD.
77. El principio de limitación de la finalidad y minimización de datos, está previsto en el artículo 5.1.b) RGPD.
78. El CEPD recomienda que, en la medida de lo posible, se incluyan los criterios que determinen cuándo se desmantelará la aplicación y qué entidad será responsable de esa determinación y rendirá cuentas al respecto. La crisis sanitaria actual no ha de servir de oportunidad para establecer mandatos desproporcionados de conservación de datos. En la limitación del almacenamiento han de considerarse las necesidades reales y la importancia médica y los datos personales solo deben conservarse durante la crisis de la COVID-19. Después, como regla general, todos los datos personales deberían borrarse o anonimizarse. A más tardar cuando las autoridades públicas competentes decidan "volver a la normalidad", debe establecerse un procedimiento para detener la recogida de identificadores (desactivación global de la aplicación, instrucciones para desinstalarla, desinstalación automática, etc.) y para activar la eliminación de todos los datos recogidos de todas las bases de datos (aplicaciones móviles y servidores).

1. EL "CONSENTIMIENTO"

En cuanto al consentimiento de las personas, este no sería un criterio legitimador del artículo 6.1.a) del Reglamento (UE) 2016/679, dado que incumpliría la exigencia de ser un consentimiento libremente dado, con base en el artículo 7.4. Reglamento (UE) 2016/679. Y en muchos supuestos, el consentimiento se daría bajo la amenaza de denegación de un derecho, derecho al acceso, lo que no podría considerarse un consentimiento libremente dado[79]. Por lo tanto, los fundamentos que legitiman los tratamientos de datos personales y de salud por apps o páginas web de autoevaluación, aplicaciones de rastreo o procedimientos de toma de temperatura son la necesidad de atender las misiones realizadas en interés público, así como la de garantizar los intereses vitales de los propios afectados o de terceras personas. Las finalidades para las que pueden tratarse los datos son, únicamente, las relacionadas con el control de la epidemia. En este sentido, el CEPD considera que el mero hecho de que el uso de tales aplicaciones tenga carácter voluntario no significa que el tratamiento de datos personales se base necesariamente en el consentimiento. Cuando las autoridades públicas prestan un servicio basado en un mandato atribuido por la legislación y acorde con los requisitos legales vigentes, la base jurídica más adecuada para el tratamiento de datos es la necesidad de cumplir una misión de interés público, es decir, el art. 6.1.e) RGPD.

Esta aproximación, no obstante, requiere de una adecuada ponderación entre el derecho a la protección de datos personales y el impacto en el nivel de protección de las personas frente a la pandemia.

Sin perjuicio de lo anterior, el CEPD considera que pueden existir circunstancias en las que el consentimiento pueda configurarse como una base jurídica que legitime los tratamientos.

2. LOS PRINCIPIOS DE "LICITUD, LEALTAD Y TRANSPARENCIA"

El art. 5.1.a) RGPD al consagrar el "principio de licitud, lealtad y transparencia" exige que todo tratamiento de datos se realice siempre de "manera lícita, leal y transparente en relación con el interesado".

El principio de "licitud" significa que el tratamiento de datos personales sólo será lícito si puede justificarse en alguna de las bases jurídicas previstas en el art. 6.1 RGPD y en el art. 9, para el caso de datos de la salud[80].

79. De acuerdo con el Considerando 32 RGPD y las directrices específicas marcadas por el GT29, el consentimiento deberá ser otorgado libremente, de forma específica, informada e inequívoca, mediante una acción terminante afirmativa y sin que el silencio o la inacción del interesado signifiquen aceptación del tratamiento. Vid. GT29, Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, WP259 y rev. 01, revisadas por última vez y adoptadas el 10 de abril de 2018.

80. Vid. PUYOL MONTERO, J., "Los principios del derecho a la protección de datos", en PIÑAR MAÑAS, J.L. (Dir.) (2016), Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad, Reus, Madrid, p. 141.

En lo que se refiere a los principios de "lealtad y transparencia" ha de decirse que la lealtad se concreta en el cumplimiento formal y material de los derechos de los afectados por el tratamiento[81], de tal forma que este principio se verá infringido en el caso de que los datos personales hayan sido obtenidos de una manera engañosa para el interesado. Para asegurar que el interesado no sea engañado a la hora de ceder sus datos es imprescindible el conocimiento necesariamente informado por parte del interesado de la finalidad o finalidades concretas del tratamiento al que se van a someter sus datos[82], esta garantía no es otra cosa que una proyección del principio de transparencia, que es el presupuesto necesario para el ejercicio de todos los derechos de los titulares de datos personales reconocidos por el RGPD.

3. LOS PRINCIPIOS DE "LIMITACIÓN DE LA FINALIDAD" Y "MINIMIZACIÓN DE DATOS"

Además de que el tratamiento de datos personales se fundamente en una adecuada base jurídica, tanto el CEPD como la AEPD determinan que debe darse cumplimiento estricto a los principios de limitación de la finalidad (art. 5.1.b RGPD) y minimización de datos (art. 5.1.c RGPD).

El art. 5.1.b) RGPD dispone que los datos personales serán "recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; […] el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales (limitación de la finalidad')"[83].

---

81. Vid. LÓPEZ ALVÁREZ, L.F., "Protección de datos personales: adaptaciones necesarias al nuevo Reglamento Europeo", Madrid, 2016, p. 31.
82. La información al interesado debe realizarse tanto en el momento de recogida de los datos, como durante su tratamiento, y con ocasión del ejercicio de los derechos por el titular. Vid. GÓMARA HERNÁNDEZ, J.L., "Protección de Datos: el RGPD en las Entidades Locales, Barcelona", 2018, p. 85.
83. El GT29 ha analizado ampliamente los dos requisitos concurrentes para el cumplimiento efectivo de este principio: Por un lado, "la especificación de finalidad" (los datos personales deben ser recabados para finalidades "específicas, explícitas y legítimas") y, por otro lado, y de manera concurrente, el "uso compatible" con aquellas finalidades. En GT29, Opinión 03/2013 *on purpose limitation*, 2 de abril de 2013, apartado III, se determina que una finalidad "específica" significa que la finalidad de la recogida de los datos debe estar claramente y específicamente definida y ser lo suficientemente detallada para determinar qué clase de tratamiento está incluido o no en la finalidad específica y posibilitar el cumplimiento de la ley y la aplicación de garantías adecuadas. Por su parte, una finalidad "explícita" significa que dicha finalidad debe estar expresada de un modo suficientemente claro e inequívoco. Lo que significa que la finalidad o finalidades del tratamiento deben ser dadas a conocer, explicadas o expresadas de una forma inteligible a los interesados con anterioridad o, en todo caso, en el momento en que se recaban los datos. La finalidad última de este requerimiento es asegurar que las finalidad o finalidades están especificadas sin vaguedad o ambigüedad según su significado o intención

Respecto del requerimiento relativo al "uso o tratamiento compatible", significa que los datos personales no pueden ser tratados de una manera incompatible con la finalidad para la cual fueron recabados inicialmente en un tratamiento ulterior[84].

En lo que se refiere al principio de "minimización de datos" en el art. 5.1.c) RGPD se concreta en que los datos personales serán "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados". Esto es, los datos tratados habrán de ser exclusivamente los limitados a los necesarios para la finalidad pretendida, sin que se pueda extender dicho tratamiento a otros datos personales no estrictamente necesarios para dicha finalidad. La determinación de si una organización cumple con el principio de minimización exige la verificación de dos aspectos: El primero es delimitar cuál es la finalidad para la que se recaba y el segundo consiste en determinar si cada actividad de tratamiento es realmente necesaria para conseguir la finalidad propuesta.

El principio de minimización se encuentra íntimamente conectado con los principios de limitación de la finalidad, necesidad y proporcionalidad. En este sentido, la minimización introduce, por un lado, un elemento de razonabilidad, en el sentido de que los datos que se traten deberán ser los oportunos y apropiados para la finalidad que justifique el tratamiento; y por otro, un elemento de proporcionalidad, de manera que el exceso de los datos tratados resultaría ilícito[85].

Además, ha de señalarse que tanto el CEPD como la AEPD entienden que las aplicaciones que se están poniendo en marcha para el seguimiento del COVID no pueden sustituir, sino meramente apoyar, el rastreo manual de contactos realizado por personal sanitario cualificado (en particular, de las entrevistas con personas infectadas)

---

real de manera comprensible para cualquier interesado, con independencia de su entorno cultural o lingüístico, nivel de comprensión o necesidades especiales. Y, en lo que respecta a una "finalidad legítima", esta exigencia va más allá del simple cumplimiento del art. 6 RGPD y significa que las finalidades "deben ser conformes a la ley" en un sentido amplio, no sólo en cuanto al cumplimiento de la normativa de protección de datos, sino también de otras normas aplicables (por ejemplo, laboral, contratos, protección de consumidores, etc.) de cualquier rango legal y de los principios generales del ordenamiento. Asimismo, otros elementos como la costumbre, los códigos de conducta, los códigos éticos, los acuerdos contractuales y, en general, el contexto general y las circunstancias concretas del tratamiento, pueden coadyuvar a determinar si una finalidad específica es legítima.

84. De acuerdo con el GT29, por "tratamiento ulterior" debe entenderse cualquier tratamiento subsiguiente a la recogida de los datos personales, ya sea de acuerdo con las finalidades inicialmente especificadas o para finalidades adicionales. Pues bien, cualquier tratamiento ulterior, debe ser compatible con la finalidad inicial. Vid. GT29, Opinión 03/2013, *on purpose limitation*, 2 de abril de 2013, apartado III.2.2.

85. Vid. FERNÁNDEZ RODRÍGUEZ, J.J., "Aproximación general a la reforma normativa: el Reglamento Europeo. Principios Generales", en CAMPOS ACUÑA, C. (Dir.), Aplicación Práctica y Adaptación de la Protección de Datos en el Ámbito Local. Novedades tras el Reglamento Europeo, Wolters Kluwer, Madrid, 2018, p. 49.

que puede determinar si los contactos estrechos pueden o no dar lugar a una transmisión del virus. Es decir, debe formar parte de un programa de salud pública de mayor alcance. Ha de utilizarse exclusivamente hasta el momento en que las técnicas de localización manual de contactos puedan gestionar por sí solas el volumen de nuevas infecciones. El CEPD subraya que los procedimientos y procesos ejecutados por las aplicaciones de rastreo de contactos, incluidos sus respectivos algoritmos, han de estar sujetos a una estricta supervisión por parte personal cualificado, a fin de limitar la aparición de falsos positivos y negativos. En concreto, la labor de facilitar asesoramiento sobre los pasos que han de darse a continuación no puede depender exclusivamente de un tratamiento automatizado.

En definitiva, una vez pasados los primeros meses en la gestión de la pandemia, se tenía que haber aprobado una Ley Orgánica que regulara la adopción de las medidas necesarias referidas al tratamiento de datos personales que adoptará el Gobierno y la Administración, medidas que tendrán que respetar las garantías mínimas contenidas en el RGPD.

Cuando el Tribunal Europeo de Derechos Humanos (TEDH) ha tenido que interpretar las restricciones de derechos fundamentales[86], ha sentado unos principios que deben respetar los estados miembros del Consejo de Europa, España entre ellos[87]:

- Deben estar previstos por una norma, acorde con el sistema de fuentes del Derecho de cada estado, anterior a la imposición del límite, que sea clara y precisa, para que la ciudadanía pueda acomodar su conducta a la previsión legal.
- Deben ser necesarias en la sociedad democrática para cumplir objetivos legítimos.
- Deben cumplir con el principio de proporcionalidad.

No hay que perder nunca de vista que se protege a las personas protegiendo los datos, no caigamos en el "confinamiento digital". En la medida de que el tratamiento de datos personales se haga necesario para la gestión de la pandemia de COVID-19, la protección de datos será imprescindible para generar confianza y sentar las condiciones para la aceptación social de cualquier solución y, así, garantizar la eficacia de las medidas adoptadas. Del mismo modo, debe subrayarse que la normativa europea en materia de

86. El Convenio Europeo de Derechos Humanos (CEDH) establece, para casos como la pandemia a la que nos enfrentamos, que cualquier Alta Parte Contratante podrá tomar medidas que deroguen las obligaciones previstas en el Convenio en la estricta medida en que lo exija la situación, a condición de que tales medidas no estén en contradicción con las restantes obligaciones que dimanan del Derecho Internacional. Ello significa que es posible suspender derechos, cumpliendo con la debida proporcionalidad e informando al Consejo de Europa. Además, excepto los denominados "derechos inderogables", los derechos del Convenio pueden estar sometidos a límites porque no se trata de derechos absolutos y, cumpliendo con determinados requisitos, pueden ser objeto de restricciones.

87. Vid. por todas, STEDH de 22 de octubre de 1981 (TEDH 1981, 4) (Caso Dudgeon) y STEDH de 2 de agosto de 1984 (TEDH 1984, 1) (Caso Malone.)

protección de datos permite el uso responsable de datos personales para fines de gestión sanitaria, al tiempo que garantiza que en ese proceso no se erosionen los derechos y libertades individuales[88]. Como señala la STC 76/2019 (RTC 2019, 76), garantizar el derecho a la protección de datos de carácter personal garantiza la calidad de nuestra democracia. No nos alejemos de los estándares europeos.

88. Vid. en este sentido, Directrices 04/2020 del Comité Europeo de Protección de Datos, de 21 de abril, sobre el uso de datos de localización de herramientas de rastreo de contactos en el contexto de pandemia de COVID-19, pueden consultarse en línea en: *https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_es.pdf*.