LA DERIVA DEL DERECHO A LA PROTECCIÓN DE DATOS EN TIEMPOS DE PANDEMIA

Montserrat Auzmendi del Solar

Letrada/Directora de Estudios y DPD del Parlamento Vasco

SUMARIO: I. Introducción; **II**. Configuración del derecho a la protección de datos de carácter personal; **III**. Tiempos de pandemia. Tratamiento de los derechos fundamentales durante la COVID-19; **IV**. Protección de datos de carácter personal durante los estados de alarma: **V**. Supuestos concretos de tratamientos de datos en tiempos de pandemia, V.1. Datos relativos a la salud, V.2. Supuestos concretos; **VI**: Conclusiones.

I. INTRODUCCIÓN

Mucho se ha escrito ya acerca de las limitaciones o restricciones de derechos fundamentales operadas con ocasión de la pandemia por COVID-19 que hemos vivido y que estamos aún viviendo (aunque en sus últimos coletazos, afortunadamente).

El Tribunal Constitucional se ha pronunciado en dos ocasiones, en las Sentencias 148/2021, de 14 de julio, y 183/2021, de 27 de octubre, sobre los Reales Decretos que declararon los respectivos estados de alarma[1]. En estos pronunciamientos, el Alto Tribunal establece criterios acerca de la suspensión o limitación de derechos fundamentales en estas situaciones, y se centra en derechos como el derecho de libertad deambulatoria, de reunión, de manifestación o de libertad religiosa.

Sin embargo, el derecho a la protección de datos de carácter personal no ha sido examinado al mismo nivel que otros derechos fundamentales, o quizá no se le ha concedido idéntica importancia. Y no cabe la menor duda de que este ha sido uno de los derechos que más afectación ha tenido, y tiene, en la situación vivida. En no pocas ocasiones, y con motivo de la implantación de medidas de control y contención de la situación de pandemia, el eje sobre el que se han centrado estos instrumentos ha sido el tratamiento de datos personales, incluidos datos especialmente sensibles como son los relativos a la salud.

[1] Real Decreto 463/2020, de 14 de marzo, y Real Decreto 926/2020, de 25 de octubre, prorrogado éste mediante el Real Decreto 956/2020, de 3 de noviembre.

El objeto de este breve trabajo es ofrecer una semblanza de las situaciones en las que los datos de carácter personal han sido afectados, limitados, modulados a lo largo de estos dos años, así como las conclusiones que podemos extraer de todo lo acontecido hasta el momento.

No cabe duda, por todo lo que comentaré en las siguientes páginas, de que todas las medidas implantadas con afectación al derecho a la protección de datos de carácter personal han tenido una lógica, un razonamiento y una utilidad, puesto que nos hemos encontrado en una situación inesperada, de tremenda gravedad, en la que era preciso tomar decisiones rápidas y, a ser posible, eficaces. Pero una vez pasados los peores momentos, una serena reflexión nos debe hacer pensar en la fragilidad de nuestras propias convicciones. El derecho a la protección de datos de carácter personal, un derecho que ha sido calificado como 'derecho fundamental', ha sido en cierto modo situado en una posición subordinada en relación con otros derechos fundamentales. Y quizá se nos olvida que un roce, una lesión de este derecho puede tener consecuencias a futuro mucho más graves que las limitaciones de otros derechos considerados de 'primera línea'.

II. CONFIGURACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

El artículo 18.4 de la Constitución Española, al señalar "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos" está planteando la protección de las personas físicas, en cuanto al tratamiento de datos personales, como un derecho fundamental.

Más explícitamente lo encontramos en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en cuyo artículo 1 b) segundo párrafo se indica: *"El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica"*

Es decir, cuando hablamos del derecho a la protección de datos de carácter personal no estamos hablando de un derecho de carácter instrumental o de segunda línea, sino que estamos hablando de un derecho merecedor de la más alta protección constitucional, un

derecho de los contenidos en la Sección Primera del Capítulo II del Título I de la Constitución, y, por lo tanto, al que le son aplicables todas las garantías: vinculación de todos los poderes públicos, reserva de ley, respeto a su contenido esencial, procedimiento preferente y sumario, recurso de amparo y procedimiento agravado de reforma constitucional según el artículo 168 de la Constitución.

El Tribunal Constitucional, por su parte, definió los contornos de este derecho. En su Sentencia 94/1998, de 4 de mayo, indicó que este derecho a la protección de datos garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para impedir el tráfico ilícito o lesivo para la dignidad y los derechos de los afectados. Se configuró este derecho como la facultad de la persona para oponerse a que ciertos datos personales se usen para fines diferentes a aquel que en principio justificó su obtención.

Además, en la STC 292/2000, de 30 de noviembre, se perfila este derecho como un derecho autónomo e independiente que consiste en un poder de disposición y control sobre los datos personales, y que faculta a la persona para decidir qué datos proporciona a un tercero, sea la Administración o un particular, y qué datos puede recabar este tercero. Por otra parte, permite a la persona saber quién posee estos datos personales y para qué fin, pudiendo oponerse a esa posesión o a un uso determinado.

Este derecho fue regulado en primer lugar por la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales, conocida como LORTAD. Esta ley fue reemplazada por la Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales, ley que traspuso la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo respectivo al tratamiento de datos personales y a la libre circulación de estos datos. Y esta ley, a su vez, ha sido superada por la Ley Orgánica en vigor, la LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

A nivel europeo, por otra parte, este derecho se recoge en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea. La Directiva 95/46/CE supuso un hito en la regulación de la protección de datos de carácter personal, hasta su derogación, con la aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27

de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos.

Este Reglamento[2], de directa aplicación en todos los Estados de la UE, a diferencia de la Directiva, ha supuesto en primer lugar una normación uniforme y armonizada para todo el ámbito comunitario. Por otra parte, este Reglamento atiende a la nueva realidad en la que vivimos, una realidad en la que la rápida evolución tecnológica y la globalización han hecho que los datos personales sean un recurso fundamental de la sociedad de la información, un recurso además tremendamente valioso en la economía mundial. Este Reglamento supone ante todo una revisión de las bases legales del modelo europeo de protección de datos, reforzando la seguridad jurídica y la transparencia, imprescindibles en la regulación de una materia que es verdaderamente sensible.

III. TIEMPOS DE PANDEMIA. TRATAMIENTO DE LOS DERECHOS FUNDAMENTALES DURANTE LA COVID-19.

No cabe duda de que las dos declaraciones de estado de alarma a través de los Reales Decretos 463/2020, de 14 de marzo, y 926/2020, de 25 de octubre, respectivamente, dictados para la gestión de la situación de crisis sanitaria y para contener la propagación de las infecciones causadas por el SARS-CoV-2, han supuesto limitaciones a derechos fundamentales con un claro propósito, que puede percibirse como razonable y lógico. Pero, sin duda, los derechos se han visto cuanto menos limitados y modulados.

El Tribunal Constitucional, en 2019[3], antes de la situación de pandemia, por lo tanto, ya sentó criterios relativos a la protección de datos de carácter personal – y a la limitación de derechos fundamentales en general- cuando declaró inconstitucional un precepto que se incorporó a la Ley Orgánica de Régimen Electoral General, el relativo a la posibilidad de recopilación por parte de los partidos políticos de datos personales relativos a las opiniones políticas de los ciudadanos. Se trataba del primer apartado del artículo 58 bis), que indicaba lo siguiente:

"Utilización de medios tecnológicos y datos personales en las actividades electorales.

[2] https://www.boe.es/doue/2016/119/L00001-00088.pdf
[3] https://www.boe.es/buscar/doc.php?id=BOE-A-2019-9548

1. 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."

Para expresarlo de manera extremadamente resumida, el TC entendió que este precepto limitaba el derecho fundamental de protección de datos:

- De manera genérica
- Sin especificar el interés público esencial que permitiría la limitación
- Sin establecer detalladamente las restricciones posibles del derecho ni las garantías adecuadas.

Estas circunstancias hicieron apreciar la inconstitucionalidad del artículo mencionado.

En definitiva, la cuestión no estriba en que el derecho a la protección de datos, o cualquier otro derecho fundamental, no pueda ser restringido de ninguna manera. Los derechos fundamentales no son absolutos. Pero las restricciones que se les impongan deben contar con unos requisitos estrictos e ineludibles. En primer lugar, estas restricciones han de ser amparadas por una Ley Orgánica. Pero esto tampoco es suficiente. La restricción no puede tener un carácter genérico (como sucedía en el precepto de la LOREG en cuestión). Por otra parte, es imprescindible especificar cuál es el interés público esencial que haga necesaria la concreta limitación y, por último, han de establecerse unas garantías a esas limitaciones para que las mismas no sean arbitrarias y puedan convertirse en restricciones abusivas y contrarias al Ordenamiento.

Además, y una vez que la medida restrictiva se recoge en una Ley Orgánica con todos los requerimientos mencionados, también hay que 'fiscalizar' las aplicaciones concretas que el Gobierno adopte al amparo de la norma. Es decir, una vez que el Gobierno aplica la norma (entendemos por supuesto que una norma dictada con todos los requisitos), y adopta la medida restrictiva en cuestión, se podrá juzgar su proporcionalidad, es decir, si la medida es útil, necesaria y proporcionada.

Por tanto, en toda limitación de derechos vemos que se dan dos fases necesarias: el previo amparo de una Ley Orgánica que avale la restricción, y el paso ulterior consistente en que la medida efectivamente adoptada sea proporcional y necesaria.

De este modo, centrándonos en la situación de pandemia de los últimos dos años, y dentro de esta situación, situando el foco en los derechos que han sido analizados de manera intensiva en este período (derecho de libertad de circulación, de manifestación o de reunión, entre otros) nos hemos encontrado con que solamente la Ley Orgánica de los Estados de Alarma, Excepción y Sitio, única legislación que especifica la limitación de estas libertades, ofrecía cobertura para restringir de forma generalizada tales derechos. Y es que las limitaciones de derechos fundamentales requieren un amparo legal para no romper con la base de nuestro Estado constitucional de Derecho. Por más que ciertas medidas restrictivas de libertades se establezcan para la protección para nuestra integridad física y nuestra salud, dichas medidas deben contar con todos los controles y garantías establecidas, sin fisuras.

Al hilo de lo mencionado, las anteriormente citadas Sentencias del Tribunal Constitucional 148/2021, de 14 de julio, y 183/2021, de 27 de octubre, llevaron a cabo un análisis de los dos Decretos de estado de alarma adoptados a lo largo de estos dos años, y determinaron la inconstitucionalidad de los mismos, si bien no de manera unánime, ya que hubo votos particulares en su seno.

No es finalidad de este trabajo analizar estos pronunciamientos del Alto Tribunal, que han sido y están siendo objeto de interesantes estudios, sino que la intención de estas páginas es hacer un breve análisis de las circunstancias fácticas de las limitaciones de derechos operadas, en concreto, de las limitaciones del derecho a la protección de datos de carácter personal, teniendo en cuenta el carácter de derecho fundamental del mismo, así como el marco preciso para tales limitaciones, y que ha sido resumido en el presente apartado.

IV. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL DURANTE LOS ESTADOS DE ALARMA

En primer lugar, debemos hacer una afirmación que, por más que sea obvia, debe ser resaltada: los derechos fundamentales, incluido el de protección de datos de carácter personal, han seguido siendo aplicables en todo momento. La declaración de un estado de alarma no supone la supresión de los derechos fundamentales, y tampoco permite

limitar derechos y libertades más allá de lo que dispone el artículo 11[4] de la Ley Orgánica 4/1981, de los estados de alarma, excepción y sitio. Tal como señaló la Agencia Española de Protección de Datos en su informe 0017/2020[5] (en la misma línea se pronunciaron Autoridades como el Garante italiano o la CNIL francesa), la normativa sobre protección de datos personales, en especial el Reglamento (UE) 2016/679 (en adelante, RGPD),

"en tanto que dirigida a salvaguardar un derecho fundamental, se aplica en su integridad a la situación actual, dado que no existe razón alguna que determine la suspensión de derechos fundamentales, ni dicha medida ha sido adoptada" .

En consecuencia, la protección de datos sigue existiendo en tiempos de COVID. Es cierto que este derecho, como cualquier otro, no puede suponer un obstáculo para medidas que sean imprescindibles para la lucha contra la pandemia, pero esta afirmación tampoco avala la merma de las garantías en materia de protección de datos. En este caso, como en el caso de otros derechos fundamentales de los que con afán se ha ocupado la doctrina y el propio TC, han de cumplirse rigurosamente los requisitos establecidos por la normativa para contemporizar con éxito restricción y garantía.

Pero, como ya se ha afirmado anteriormente, el derecho a la protección de datos personales no es un derecho absoluto. De hecho, el propio RGPD, en su considerando 4, señala lo siguiente:

"El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales ***no es un derecho absoluto*** *sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad*."

---

[4] Artículo once.

Con independencia de lo dispuesto en el artículo anterior, el decreto de declaración del estado de alarma, o los sucesivos que durante su vigencia se dicten, podrán acordar las medidas siguientes: a) Limitar la circulación o permanencia de personas o vehículos en horas y lugares determinados, o condicionarlas al cumplimiento de ciertos requisitos. b) Practicar requisas temporales de todo tipo de bienes e imponer prestaciones personales obligatorias. c) Intervenir y ocupar transitoriamente industrias, fábricas, talleres, explotaciones o locales de cualquier naturaleza, con excepción de domicilios privados, dando cuenta de ello a los Ministerios interesados. d) Limitar o racionar el uso de servicios o el consumo de artículos de primera necesidad. e) Impartir las órdenes necesarias para asegurar el abastecimiento de los mercados y el funcionamiento de los servicios de los centros de producción afectados por el apartado d) del artículo cuarto.

[5] https://www.aepd.es/es/documento/2020-0017.pdf

Por otra parte, también el propio RGPD nos indica que el tratamiento de los datos personales puede ser necesario por motivos importantes de interés público. Así, su considerando 46 señala:

"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"*

Según esto, la idea recta es el mantenimiento del equilibrio con otros derechos fundamentales, como indicaba el considerando 4, además de que tampoco podremos hablar de cualquier tipo de tratamiento de datos. Adviértase de que el transcrito considerando 46 nos habla de *'ciertos tipos de tratamiento'.*

En resumen, el derecho a la protección de datos de carácter personal está plenamente vigente en cualquier momento, también en tiempos de COVID, si bien no es un derecho absoluto, pero la licitud del tratamiento de datos se hará depender del cumplimiento de los principios y bases de legitimación previstas en la normativa aplicable a esta materia, como veremos, sin que sea admisible ningún tratamiento al margen de aquellos.

V. SUPUESTOS CONCRETOS DE TRATAMIENTOS DE DATOS EN TIEMPOS DE PANDEMIA.

V.1. Datos relativos a la salud.

Antes de abordar los tratamientos de datos que han suscitado dudas o problemas acerca de su adecuación a la normativa en materia de protección de datos, debemos encuadrar ciertos tipos de datos, que van a ser los más afectados en estas situaciones. Se trata, sin

duda, de los datos referentes a la salud, y que tienen una especial protección conforme al RGPD.

En primer lugar, debemos saber a qué nos referimos cuando hablamos de datos relativos a la salud. El artículo 4 del RGPD, en su apartado 15 nos lo aclara:

"'datos relativos a la salud': datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud"

Respecto de este tipo de datos, el Reglamento se muestra tajante en lo relativo a su protección. De este modo, el artículo 9.1 indica:

"Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, ***datos relativos a la salud*** *o datos relativos a la vida sexual o las orientación sexuales de una persona física"*

Es decir, el Reglamento deja clara la prohibición de tratar este tipo de datos, por ser considerados una categoría especial de los mismos que merece esa protección extraordinaria. No se trata de un dato personal cualquiera, sino un dato respecto del cual las cautelas que un responsable de tratamiento debe adoptar son máximas, hasta el punto de que, con carácter general, dicho tratamiento está prohibido.

Sin embargo, el mismo artículo que establece esta prohibición, también señala unas excepciones a la misma. Recogemos de manera resumida aquellas excepciones que pueden tener cabida en una situación de emergencia sanitaria como la que vivimos:

- <u>Podrán tratarse datos relativos a la salud para el cumplimiento de obligaciones en el ámbito del Derecho laboral y de la seguridad y protección social (art. 9.2.b RGPD).</u>

  Los empleadores y su personal tienen obligaciones en materia de prevención de riesgos laborales. 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, en ocasiones, puede suponer la obligación para el personal de informar al empleador si existe la sospecha de poder transmitir una enfermedad infecciosa, para salvaguardar la propia salud y la de los demás trabajadores del centro de que se trate, y para permitir adoptar las medidas oportunas.

- También podrán tratarse datos de salud cuando se dé un interés público en el ámbito de la salud pública (art. 9.2.i RGPD), que en este caso se configuraría como interés público esencial (art. 9.2.g RGPD).

  Esta, como parece obvio, va a ser la excepción estrella durante los estados de alarma, en tiempos COVID, pero nunca se debe olvidar que, al tiempo que el RGPD establece la excepción, también señala la cautela, puesto que también indica que este tratamiento:

  "debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado"

- Asimismo, el tratamiento será posible cuando sea necesario para la realización de un diagnóstico médico (art. 9.2.h RGPD).
- Y, finalmente, la prohibición cede 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 RGPD).

Se trata, como se aprecia, de excepciones tasadas, vinculadas a auténticas situaciones de necesidad y, por otra parte, el RGPD, cuando las enumera, señala siempre que las medidas o tratamientos que se adopten basándose en las mismas, **tienen que tener un basamento en el Derecho de la Unión o de los Estados miembros.** Es decir, requerirán de una Ley que ampare dichas excepciones.

Por lo tanto, si conectamos estas previsiones del RGPD con la doctrina de nuestro Tribunal Constitucional expuesta al principio de este trabajo, no cabe duda de que sólo una Ley Orgánica puede ser el adecuado 'paraguas' para un tratamiento de datos relativos a la salud, con base en el artículo 9.2 del RGPD.

V.2. **Supuestos concretos**.

Hechas estas precisiones, pasaremos a analizar circunstancias que se han producido en los dos últimos años, en las que el tratamiento de datos (en ocasiones de datos relativos a la salud y en otras ocasiones de datos de carácter personal de otra índole) ha suscitado dudas en cuanto a su acomodo a la normativa vigente:

a)- Obligación de proporcionar información consistente en datos de carácter personal para la trazabilidad de contactos.

El Real Decreto-ley 21/2020[6] preveía que tanto establecimientos, medios de transporte o cualquier otro lugar, centro o entidad pública o privada estaban obligados a proporcionar la información de la que dispusieran o les fuera solicitada relativa a la identificación y datos de contacto de personas potencialmente afectadas por un caso de infección.

En primer lugar, tenemos que señalar que en este caso no se está haciendo referencia a datos relativos a la salud. Son únicamente datos de identificación de personas, datos de contacto para, en caso de ser necesario, poder notificarles que habían podido estar expuestos a un caso positivo.

Pero, en todo caso, estamos hablando de un tratamiento de datos de carácter personal. Y todo tratamiento debe contar con una base de legitimación, del elenco contenido en el artículo 6 del RGPD. En este caso, podríamos contemplar fundamentalmente una base de legitimación: 'el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento' (base legitimadora contenida en el artículo 6. 1. e) RGPD). La obligación de los poderes públicos de hacer un seguimiento adecuado de la evolución de los contagios, por una parte, supone, para hacerla efectiva, la obligación, para los establecimientos, de tomar datos y cederlos a las autoridades sanitarias. Eso sí, sólo cuando las autoridades sanitarias identifiquen la necesidad de realizar la trazabilidad de contactos. No en otro caso.

[6] https://www.boe.es/buscar/act.php?id=BOE-A-2020-5895

Y también tal medida pudiera tener apoyo en otra base legitimadora: 'la protección de intereses vitales de los afectados y de otras personas físicas' (base ésta contenida en el artículo 6. 1 d) RGPD).

Una vez verificada la base jurídica para el tratamiento de estos datos de carácter personal, no podemos olvidar que la legitimación del tratamiento implica asimismo la evaluación de la proporcionalidad del mismo, que se plasma en el cumplimiento de los principios que deben presidir cualquier tratamiento de datos de carácter personal, y que encontramos en el artículo 5 del RGPD.

- En primer lugar, el Reglamento nos habla de la licitud, lealtad y transparencia de los datos recogidos, en el sentido de que, en relación con el interesado, estos datos deben ser tratados de forma lícita, leal y transparente.
- El siguiente principio es el de la limitación de la finalidad, en el sentido de que los datos recabados deben serlo con unos fines determinados, explícitos y legítimos, sin que quepa un tratamiento ulterior de forma incompatible o diferente de dichos fines. En el caso que estamos tratando, los datos de identificación de las personas únicamente tendrán la finalidad de ser aportados a las autoridades sanitarias, cuando éstas identifiquen la necesidad de realizar una trazabilidad de contactos.
- Otro principio de ineludible cumplimiento es el de la minimización de datos, lo cual significa que los datos que se recojan son los adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No cabría ninguna extralimitación, en el sentido de solicitar un dato adicional que vaya más allá de la identificación de la persona y su localización.
- Asimismo, la exactitud de los datos solicitados es imprescindible, de manera que si fuera necesario éstos serán actualizados. Por otra parte, se tomarán todas las medidas razonables para que se supriman o rectifiquen los datos personales que sean inexactos con respecto a los fines para los que se tratan.
- No menos importante es el principio de limitación del plazo de conservación, de manera que los datos recogidos se mantengan estrictamente el tiempo necesario para los fines del tratamiento de los datos personales.
- Finalmente, el principio de integridad y confidencialidad de los datos nos indica que el tratamiento debe garantizar una adecuada seguridad de los datos personales,

incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas y organizativas apropiadas.

Teniendo en cuenta todos estos requisitos, podemos concluir que la recogida por parte de establecimientos de hostelería, etc., de datos de identificación y localización de la clientela, siempre que sean los datos mínimos o justos, se informe de forma clara y transparente a la persona concernida de la finalidad de la recogida de esos datos, los cuales se conservarán el tiempo mínimo para poder cumplir con dicha finalidad (lo que implica la destrucción de los mismos pasado ese plazo), y poniendo a disposición de las personas la posibilidad de modificarlos o suprimirlos en caso de que sean inexactos, sería conforme a la normativa protectora de los datos de carácter personal.

Sin embargo, en cuanto a las bases jurídicas legitimadoras, pese a que se ha esgrimido en ocasiones la base mencionada relativa a la 'protección de intereses vitales de los afectados y de otras personas', no parece una base que pudiera ser de aplicación en este supuesto. Hemos de entender que cuando se alega esta base, se está hablando de un peligro real para intereses vitales, y no hipotético, como es el caso que nos ocupa: una mera hipótesis de que en un futuro próximo se diera un caso de infección en el mismo local al que acudió la persona que aporta sus datos personales.

Por tanto, entendemos que la única base legitimadora para el tratamiento de datos personales en este caso sería el de 'el cumplimiento de una misión realizada en interés público'.

b)- Las 'apps' de rastreo o mecanismos de notificación en caso de exposición al COVID-19.

Estas apps (cuya versión en el Estado español fue el protocolo DP3T integrado con APIs de Apple y Google -llamado Radar COVID-), tienen dos fines específicos:

- El uso de datos de localización para apoyar la respuesta a la pandemia intentando modelizar la propagación del virus, para evaluar la eficacia global de las medidas de confinamiento;

- El rastreo de contactos, que tiene como objetivo que las personas que hubieran estado próximas a alguien que resulte ser un positivo confirmado sean informadas al respecto, con la finalidad de romper las cadenas de transmisión del virus lo antes posible.

A este respecto se pronunció el Comité Europeo de Protección de Datos (CEPD a partir de ahora) a través de las Directrices adoptadas el 21 de abril de 2020[7].

Partimos, y así partió el CEPD, de la idea de que el uso de este tipo de aplicaciones debe ser, en primer lugar, voluntario, y en segundo lugar, no puede basarse en un rastreo de movimientos individuales, sino en información sobre proximidad de los usuarios, lo cual tiene consecuencias bien diferentes.

Sin embargo, el hecho de que partamos de una aplicación que se coloca en el dispositivo móvil de manera voluntaria no significa que a partir de ese uso voluntario todo lo que suceda esté cubierto con el consentimiento de la persona usuaria. Este tipo de aplicaciones tiene muchas más derivadas que es preciso analizar para ver su impacto en la protección de datos de carácter personal.

En principio, no cabe duda de que el seguimiento sistemático y masivo de la localización de las personas físicas es una grave injerencia en su privacidad. Por lo tanto, como hemos señalado, sólo puede legitimarse esta práctica sobre la base de su **adopción voluntaria** por parte de las personas usuarias para cada uno de los fines respectivos, y esto, además, implica también que las personas que decidan no utilizar estas aplicaciones no deben sufrir desventaja de ningún tipo.

Por otra parte, a las personas usuarias, una vez deciden adoptar la aplicación, no se les puede pedir que se abandonen a la suerte de lo que las autoridades públicas, o las multinacionales tecnológicas determinen una vez prestado ese consentimiento. La persona usuaria debe tener un control de lo que sucede. O, dicho de otro modo, debe haber una 'rendición de cuentas' por parte de las autoridades que ponen a nuestra disposición estas tecnologías. Y para que sea posible esta rendición de cuentas es necesario que se defina con claridad **quiénes son los responsables del tratamiento de datos** en este tipo

[7] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_es.pdf

de aplicaciones, al igual que sucede en cualquier otro ámbito en el que prestamos el consentimiento al tratamiento de nuestros datos. En buena lógica, y así opinó el CEPD, los responsables del tratamiento de datos habrían de ser las autoridades sanitarias nacionales o autonómicas, en su caso, aunque podrían arbitrarse otras fórmulas. Eso sí, siempre con transparencia y poniendo esta información a disposición del usuario. Y, además, si el despliegue de las aplicaciones de rastreo implica la intervención de diferentes agentes, es importante que sus respectivas funciones y responsabilidades queden claramente delimitadas desde el principio y se expliquen con transparencia a los usuarios.

Otra cuestión a tener en cuenta, tal como comentamos en el apartado anterior relativo a la aportación de datos por parte de establecimientos, es el principio de **limitación de la finalidad**. Esta debe ser lo suficientemente específica y concreta como para excluir un tratamiento ulterior con fines ajenos a la finalidad establecida en un principio. Nos da igual si el nuevo tratamiento que se pretende dar a nuestros datos tiene que ver con la gestión de la pandemia COVID. El tratamiento debe ser el pactado, y la finalidad la establecida en un principio, de forma estricta.

Y, por supuesto, una vez definida claramente la finalidad, es preciso que el uso de los datos personales sea adecuado, necesario y proporcionado a la finalidad señalada.

Realmente, a posteriori podemos afirmar que poco éxito tuvo esta iniciativa. Y, además, desde la perspectiva de la protección de datos de carácter personal podemos alegrarnos quizá de ello. Por una parte, todos los requisitos de cumplimiento ineludible que hemos mencionado arriba se cumplían a duras penas. Desde el desconocimiento por parte del usuario medio de quién es responsable del tratamiento de dichos datos, al desconocimiento de dónde se alojaban los mismos y la falta de constancia de la utilización específica para los fines concretados, todo en este tipo de tecnología se deja a una especie de fe ciega que poco tiene que ver con las exigencias de la normativa protectora de los datos de carácter personal.

Si nos preguntamos cuáles son las principales amenazas a la privacidad de este tipo de soluciones, podemos concluir que las amenazas vendrían derivadas de la posible realización de mapas de relaciones entre personas, la reidentificación por localización implícita y la auténtica fragilidad de los protocolos a la hora de construir ‘tarjetas’ casi

anónimas, así como la posibilidad de dispersar las señales de los contagios de forma que no se identifique en ningún caso la identidad de los contagiados. Y hemos de ser conscientes de que el tratamiento de la información no sólo afecta al usuario de la aplicación, sino también a todos los terceros con los que ha estado en contacto.

Por supuesto que los protocolos de criptografía y anonimización se pretende que sean robustos, pero también es cierto que con la habilidad suficiente es posible romper estos protocolos y hacer que se asocien los apodos anónimos con números de teléfono y personas. Además, no podemos obviar que el usuario tiene un mínimo control, es una solución centralizada, y el acúmulo de datos de esta manera centralizada puede dar lugar a abusos por parte de empresas poco éticas, e incluso se pueden dar ciberataques.

c)- Tratamientos de datos de empleados enfermos.

Como ya se comentaba al principio de este apartado, los datos de salud se categorizan como de especial protección, y con carácter general se prohíbe su tratamiento (artículo 9.1 RGPD). Pero, tal como establece el punto 2 de este mismo artículo, el tratamiento de estos datos es permitido cuando concurre alguna de las circunstancias que se detallan en el precepto, y que se han comentado en páginas anteriores.

Una de estas excepciones hacía alusión a las obligaciones en el ámbito del derecho laboral. En este sentido, la Ley de prevención de riesgos laborales establece obligaciones tanto para los empleadores como para el personal en materia de prevención de riesgos, dado que la empresa debe garantizar la seguridad y salud de todos sus trabajadores. De este modo, en caso de que exista un riesgo grave, está obligada a informar a los demás empleados de la existencia de ese riesgo y de las medidas a adoptar, consensuadas con la representación de los trabajadores.

Ahora bien, la información que se transmita, debe hacerse sin identificar a las personas afectadas, se debe mantener su privacidad. Otra cosa es que las autoridades competentes, en particular las sanitarias, exijan la transmisión de datos identificativos. Eso sí, con una correcta motivación y cuando la transmisión de estos datos sea estrictamente necesaria para la consecución de la protección del interés público correspondiente. Y, por supuesto,

con todos los requisitos de licitud, transparencia, limitación en el tiempo, limitación de la finalidad y minimización de datos.

Por otra parte, y como ya se comentó también, la normativa de prevención de riesgos laborales impone también a los trabajadores la obligación de preservar su propia seguridad y la de sus compañeros. Y por ello en un momento de emergencia sanitaria, de gran riesgo de transmisión de una enfermedad, parece razonable que un trabajador con síntomas o enfermo, comunique este extremo a su empresa, para que se implementen las medidas precisas para la protección de la salud de los trabajadores.

En todo caso, el tratamiento de esa información debe respetar escrupulosamente los principios exigidos por el RGPD, ya señalados anteriormente.

Ha de tenerse en cuenta que el tratamiento de estos datos de salud es una injerencia en la privacidad de lo más íntimo de las personas, y por lo tanto, debe someterse a un juicio de necesidad y proporcionalidad, y limitarse en el marco temporal.

VI. CONCLUSIONES

Podrían abordarse muchos otros aspectos y casos producidos durante los estados de alarma en los que el derecho a la protección de datos de carácter personal se ha visto afectado de una u otra manera. Han sido muchas las situaciones, como por ejemplo, las tomas de temperatura en empresas y diferentes establecimientos, los QR (pasaporte COVID) para la entrada en diferentes lugares, las situaciones y riesgos derivados del teletrabajo, etc.

Cada uno de estos supuestos merecería un análisis exhaustivo, pero en esta breve comunicación simplemente se ha pretendido plantear una muestra de casos en los que se aprecia que, observado de manera superficial, el desgaste del derecho a la protección de datos de carácter personal puede parecer liviano o inexistente, pero, si analizamos un poco más a fondo, nos damos cuenta de que hemos estado lejos de llevar a cabo todas las

cautelas que la normativa exige cuando tratamos datos personales, y más cuando se trata de datos relativos a la salud.

Al comienzo del trabajo resaltaba que si bien se ha puesto la atención en la afectación que la situación de pandemia ha supuesto para otros derechos fundamentales, y tanto doctrina como jurisprudencia se han aprestado a poner el foco sobre la insuficiencia, en muchos casos, de la cobertura legal para las modulaciones de derechos operadas, en lo que respecta a la protección de datos siempre se ha incidido en la cuestión de que, pese a su importancia, no puede suponer un obstáculo para la toma de medidas imprescindibles y protectoras de la población. Casi una aceptación de que, de ceder algún derecho, el menos importante sería el derecho a la protección de datos de carácter personal.

De todo esto derivan una serie de ideas a modo de conclusión:

1- El derecho a la protección de datos es un derecho fundamental, sentado en el artículo 18.4 CE.
2- Como tal derecho fundamental merece la máxima protección.
3- Los datos de carácter personal pueden ser tratados siempre que se cumplan todos los requisitos establecidos en la normativa en vigor, en particular en el RGPD.
4- En el caso de datos relacionados con la salud, el principio general es la prohibición de su tratamiento, si bien se establecen excepciones a tal prohibición.
5- Cuando se den estas excepciones, como ha podido ser el caso durante el tiempo de pandemia, es imprescindible la motivación exhaustiva del supuesto de excepción en que nos encontramos, y el tratamiento debe ser riguroso, el mínimo posible, con una finalidad establecida de manera 'quirúrgica', y restableciéndose el derecho a la mayor brevedad posible.
6- Como última conclusión, debemos reflexionar si todas esas cautelas se llevaron a cabo en los supuestos que he mencionado a modo de ejemplo. Las excepciones que se mencionan a la prohibición de tratamiento de datos de salud se recogen en el RGPD, y siempre requieren una ley estatal o norma de la Unión que les dé cobertura, cosa que no se ha producido en España durante la pandemia. El establecimiento de instrumentos como el desafortunado Radar COVID, o la actividad de los rastreadores, entre otras cuestiones, debían haberse establecido por ley, de manera que se aquilataran todas las exigencia que estos instrumentos

requieren por lo invasivas que son respecto de la privacidad de las personas. Y, recordemos, la necesidad y sobre todo, el miedo, no justifican cualquier cosa.