Universidad Internacional de La Rioja

Facultad de Derecho

Máster Universitario en el Ejercicio de la Abogacía

Legitimación para el tratamiento de datos personales en el contexto de una pandemia

Trabajo fin de estudio presentado por:	María Hinarejos Díaz
Tipo de trabajo:	Trabajo Final de Máster
Área jurídica:	Protección de Datos Personales
Director/a:	Ángela Trujillo del Arco
Fecha:	Mayo 2023

Agradecimientos

A mi familia y amigos.

Resumen

La situación mundial provocada por el COVID-19 derivó en la urgente toma de medidas excepcionales para tratar de erradicar y mitigar los posibles efectos, tanto económicos como sociales, derivados de la misma. Las medidas adoptadas por una mayoría de gobiernos del mundo dieron lugar a la limitación de derechos fundamentales, tales como la libertad de circulación de las personas.

En este sentido, se ha podido ver vulnerado el derecho fundamental de los ciudadanos europeos a la protección de su información personal como consecuencia de las medidas excepcionales para afrontar la pandemia, así como otros derechos y libertades.

En consecuencia, el presente trabajo se desarrolla con la finalidad de analizar distintos escenarios en los que el derecho fundamental a la protección de datos puede verse afectado como consecuencia de una pandemia, algo que permitirá abordar situaciones similares en el futuro con mayores garantías jurídicas.

Palabras clave: Pandemia, afectación de derechos, protección de datos.

Abstract

The global situation caused by COVID-19 led to the urgent adoption of exceptional measures to try to eradicate and mitigate the possible effects, both economic and social, stemming from it. The measures adopted by most of the world´s governments led to the limitation of fundamental rights, such as people´s freedom of movement.

In this sense, the fundamental right of European citizens to the protection of their personal data may have been violated as a consequence of the exceptional measures to deal with the pandemic, as well as other rights and freedoms.

Consequently, this paper is developed with the aim of analyzing different scenarios in which the fundamental right to data protection may be affected as a result of a pandemic, something that will enable similar situations to be addresses in the future with stronger legal guarantees.

Keywords: Pandemic, affectation of rights, personal data protection.

Índice de contenidos

1. Introducción

A finales del año 2019 se detectaron los primeros casos de COVID-19, causados por el virus SARS-COV-2 en la ciudad china de Wuhan, concretamente en un grupo de personas con sintomatología de neumonía desconocida. A pesar de que el origen del virus es incierto, la teoría que cobra más fuerza es que se trate de un patógeno que se transfiera de animales a humanos, provocándoles una enfermedad infecciosa parecida a una neumonía (ALZÍBAR 2021).

El 11 de marzo de 2020, la Organización Mundial de la Salud (OMS) reconoció como pandemia la situación sanitaria de emergencia de carácter internacional (OMS 2021). Las autoridades sanitarias indicaron que la enfermedad se transmitía por contacto directo con individuos infectados, generalmente a través de la saliva, pero también al estar en contacto con una superficie contaminada y posteriormente llevar las manos al rostro (Ministerio de Sanidad 2021).

Es por ello que los gobiernos de todo el mundo tuvieron que decretar medidas urgentes para frenar la expansión de la enfermedad, lo que derivó en la afectación de una serie de derechos fundamentales como la libertad de circulación, el derecho a la intimidad, el derecho de reunión, así como el derecho a la protección de datos personales.

El presente trabajo pretende analizar distintos escenarios en los que derechos fundamentales tales como el derecho a la protección de datos o el derecho a la intimidad, han podido verse afectados a raíz del tratamiento de los datos personales de los ciudadanos con motivo de la pandemia y su contención. Asimismo, se analiza el punto de vista de autoridades y tribunales, tanto nacionales como extranjeros, lo cual permitirá abordar situaciones similares en el futuro con mayores garantías jurídicas y medidas menos lesivas para los derechos y libertades de la ciudadanía.

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 (Reglamento General de Protección de Datos o RGPD) contiene reglas necesarias para que el tratamiento de datos personales, en una situación como la referida en el presente trabajo sea legítima, articulando una serie de principios aplicables al tratamiento de los datos personales.

En este trabajo se analiza si las reglas contenidas en las diferentes normas en materia de protección de datos son efectivas a la hora de proteger los derechos fundamentales de los ciudadanos en una situación de pandemia.

En este sentido, jugará un papel importante la sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, la cual sienta por primera vez la distinción entre el derecho fundamental a la intimidad personal y familiar y el derecho fundamental a la protección de datos personales.

Así mismo, organismos como la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos se han pronunciado sobre el abuso y vulneración de derechos humanos producidos con motivo de la implantación de medidas excepcionales o de emergencia para frenar la propagación del virus (Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos 2020).

1.1. Justificación del tema elegido

El tema desarrollado en el presente trabajo pretende arrojar luz sobre un ámbito que ha generado grandes problemas en los últimos dos años y que, de no ser solucionados, generarán problemas en situaciones similares. Se trata de un tema de gran actualidad sobre el cual todavía quedan grandes interrogantes por resolver y conflictos de intereses en el tratamiento de los datos personales de los ciudadanos.

La elección del tema viene justificada porque, a comienzos de la pandemia, el derecho fundamental a la protección de datos personales era un tema el cual los ciudadanos no éramos conscientes de hasta qué punto pueden verse afectados nuestros derechos por el simple hecho de un tratamiento concreto de nuestros datos. En este sentido y tras los últimos años en los que hemos experimentado un aumento notable en cuanto al tratamiento de datos personales, como la salud de una persona o la geolocalización, por parte de diferentes entidades, nos lleva a pararnos a pensar hasta qué punto una persona puede controlar el uso que otras hacen sobre su información.

1.2. Problema y finalidad del trabajo

El problema que se plantea es el análisis de los criterios legitimadores que permitirían tratar la información relativa a la salud de los ciudadanos atendiendo a las circunstancias concretas del caso.

Una de las mayores dificultades a la hora de afrontar este trabajo ha sido la poca información en lo que a jurisprudencia y doctrina se refiere sobre el tema desarrollado, pues se trata de una temática de reciente actualidad la cual todavía no ha podido arrojar suficientes pronunciamientos al respecto.

La finalidad del presente trabajo es llevar a cabo una contextualización histórica de la evolución del derecho fundamental a la protección de datos personales, en su regulación tanto en el ámbito nacional como en el ámbito europeo para, posteriormente, analizar las bases jurídicas del tratamiento de los datos personales y su ponderación y posible colisión con otros derechos al ser tratados en el contexto de una pandemia mundial.

1.3. Objetivos

Uno de los principales objetivos que se pretende conseguir con la realización de este trabajo es establecer la posibilidad o no de tratar datos personales por distintos responsables de tratamiento en diferentes contextos relacionados con una situación de pandemia.

En este sentido, se pretende dilucidar en qué supuestos de tratamientos de datos personales concretos las autoridades competentes se han pronunciado acerca del acceso y tratamiento de los datos personales de los interesados, la ponderación de derechos fundamentales que se ha realizado, así como las medidas adoptadas por parte de las autoridades competentes con la intención de frenar o disminuir la propagación del virus. Para ello, el trabajo se estructura en tres partes principales.

En la primera parte, se pretende contextualizar el origen y evolución del derecho fundamental a la protección de datos personales, así como los diversos instrumentos jurídicos, tanto nacionales como internacionales europeos.

En la segunda parte, se realiza un análisis del concepto de datos personales y su diferencia con las categorías especiales de datos a la hora de legitimar el tratamiento de los mismos. A tal

efecto, se han consultado diferentes tipos de fuentes, desde normativa nacional y europea, pasando por jurisprudencia de los principales tribunales europeos y españoles, hasta doctrina de autores.

En la última parte del trabajo, se exponen una serie de supuestos de tratamientos de datos personales concretos llevados a cabo en el contexto COVID-19 a través de los cuales se analiza la legitimación para el tratamiento de los mismos, así como la postura adoptada por parte de las autoridades competentes en esta materia, así como la inclinación de jueces y tribunales.

2. Marco teórico y desarrollo

2.1. INICIO Y EVOLUCIÓN HISTÓRICA DE LA PROTECCIÓN DE DATOS PERSONALES

Los orígenes de la regulación sobre la privacidad se remontan en torno a 1890 en Estados Unidos (CORRAL y HERNÁN 2000). Llama la atención que uno de los primeros países en establecer los conceptos de privacidad y protección de datos personales fuese Estados Unidos, pues se trata de un país con importantes carencias en cuanto a la privacidad de los datos personales. Es más, actualmente no cuentan con una norma concreta en cuanto a protección de datos personales se refiere, sino que existen normas en los diferentes estados federales que desarrollan esta materia, pero sin llegar a unificarla, incluyendo la regulación dentro de otras leyes como las de consumidores (FERRETJANS 2022).

La primera aproximación al concepto de privacidad fue establecida por los autores Warren y Brandeis, en un artículo titulado «The Right to Privacy», publicado en la Harvard Law Review en la última década del siglo XIX. En el mismo establecían el concepto de privacidad como un derecho a estar solo, basándose en el secreto o anonimato de las personas, cuyos pilares fundamentales eran la autonomía e inviolabilidad de la dignidad de la persona (WARREN y BRANDEIS 1890).

Uno de los hechos más relevantes, en cuanto a la privacidad se refiere, fue el tratamiento de datos que se llevó a cabo a través de las tarjetas perforadas de la compañía de tecnologías de la información International Business Machines (IBM), en los años 30. En Estados Unidos, IBM patentó un dispositivo para almacenar datos en tarjetas a través de una serie de perforaciones, cada una de las cuales representaba un dato distinto, como la edad, educación, domicilio o religión de una personal. Las tarjetas se insertaban posteriormente en una máquina la cual cruzaba toda la información (HERNÁNDEZ 2018).

La tecnología de las tarjetas perforadas fue utilizada durante la Segunda Guerra Mundial como herramienta de control social, lo que contribuyó a facilitar el avance del Holocausto nazi, al permitir que se automatizase la persecución de los judíos con el objetivo de Adolf Hitler de exterminarlos. Así mismo, estas tarjetas fueron vendidas y utilizadas en España durante la Guerra Civil (HERNÁNDEZ 2018).

Ésta fue una de las primeras causas que, en Europa, desató la conciencia y sensibilización sobre la privacidad de los individuos, pues hoy en día es impensable un tratamiento de datos considerados sensibles como es la religión a la que pertenece una persona, en estos términos.

El primer texto de carácter internacional a nivel global que recoge el ámbito de la protección de datos personales en sentido amplio, sin llegar establecer una definición concreta del concepto, es la Declaración Universal de los Derechos Humanos (DUDH) aprobada por la Asamblea General de las Naciones Unidas celebrada en París en el año 1948. En este documento no se hace mención expresa a la protección de datos personales como un derecho fundamental, sino que se hace alusión al derecho de las personas a preservar su privacidad (art. 12 DUDH). Años más tarde, con la aprobación del Convenio Europeo de Derechos Humanos (CEDH) por parte del Consejo de Europa, se volvió a reconocer el derecho que tienen las personas a su privacidad (art. 8 CEDH). Pues bien, al apartado 2 del citado artículo señala que las autoridades públicas podrán intervenir limitando el derecho a la privacidad de las personas cuando haya un interés legítimo que lo justifique, como pudiera ser la seguridad nacional, el bienestar económico del país, o la protección de la salud pública, entre otros.

En este sentido cabe destacar la sentencia del Tribunal Europeo de Derechos Humanos (TEDH) caso Halford contra Reino Unido, del año 1997, en la que se dirimía una reclamación interpuesta por una inspectora de policía donde se hace alusión a la injerencia de la autoridad pública en el derecho a la vida privada de una persona. El Tribual afirma que esta injerencia, admitida por el artículo 8.2 CEDH, debe estar prevista por la ley de manera clara, previsible y precisa, es decir que los ciudadanos sepan bajo qué circunstancias las autoridades públicas pueden limitar su derecho a la intimidad (STEDH caso Halford contra Reino Unido). De esta sentencia concluimos que, si la legislación nacional de cada país establece supuestos taxativos en los que las autoridades pueden interferir limitando nuestro derecho a la intimidad y privacidad, no se trata de un derecho que goce de protección absoluta, por lo que los legisladores de cada país deberán establecer minuciosamente cuándo va a verse afectado o limitado el derecho fundamental a la privacidad en una norma con rango de ley.

En Europa, el comienzo de la regulación del derecho a la protección de datos personales se remonta a la segunda mitad del siglo XX. Los primeros países en pronunciarse y regular la materia relativa a la protección de datos de carácter personal fueron Reino Unido y Alemania. En Reino Unido se comenzó a debatir este concepto en 1961 cuando un político de la época

presentó un proyecto de ley con el objetivo de regular y proteger la privacidad (NISA 2020). Por otro lado, en Alemania se comenzó a desarrollar la regulación legal en materia de protección de datos en el año 1970, con una ley donde se protegían los derechos de las personas cuyos datos se estaban tratando. Así mismo, regulaba ciertos aspectos relativos al secreto de las comunicaciones o el derecho sobre el control de los datos. En este sentido y a efectos de asegurar el cumplimiento de la norma, la misma creó la figura del Comisario de Protección de Datos con el objetivo de velar por la obediencia de la ley (NISA 2020).

Una vez introducido el origen del derecho a la protección de los datos personales, nos centraremos en su regulación a lo largo de los años, tanto a nivel europeo como a nivel nacional español.

2.1.1. Marco normativo europeo en el derecho a la protección de datos

La aprobación del Tratado de Funcionamiento de la Unión Europea (TFUE) en el año 1957, supuso que, por primera vez, se expusiera de manera expresa en un texto de carácter normativo que toda persona tiene derecho a la protección de sus datos de carácter personal (art. 16 TFUE). Esta norma, únicamente señalaba el concepto en cuanto al reconocimiento del derecho a la protección de datos. Si bien es cierto que otras normas posteriores proceden a regular y desarrollar este concepto de manera más amplia.

El siguiente gran hito, en lo que a materia de protección de datos respecta, fue la redacción del Convenio N.º 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (en adelante, Convenio N.º 108 o C108). El Convenio N.º 108 es considerado el primer instrumento jurídicamente vinculante en el ámbito de la protección de datos personales, a nivel internacional, si bien hace menciones al artículo 8 del CEDH. Este convenio destaca por su dimensión transfronteriza, pues no solamente pueden adherirse al mismo países europeos, sino cualquier tercer país interesado en su regulación.

El Convenio N.º 108 fue aprobado en aras de ampliar la protección de los derechos y libertades fundamentales de los individuos, en concreto, el derecho al respeto de la vida privada de los individuos, reconociendo la necesidad de conciliar los valores fundamentales del respeto a la vida y a la libre circulación de la información entre los pueblos. Protege a las personas físicas

contra los abusos que puedan llevarse a cabo en el tratamiento de sus datos personales y busca regular los flujos transfronterizos de los mismos, debido al incremento de las transferencias internacionales de datos que se estaba produciendo (C108).

En su afán por dotar a este derecho de una regulación adecuada y común para todos los Estados Miembros de la Unión Europea (UE), dada su importancia, en el ámbito de la UE se dictó 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 que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Directiva 95/46/CE). Esta Directiva fue aprobada con el objetivo de armonizar la regulación en materia de protección de datos en todo el territorio de la Unión Europea, debido al establecimiento de un mercado único interior lo que implicaría un aumento notable de los flujos transfronterizos de datos personales entre los Estados Miembros, fortaleciendo la figura de la Unión Europea (Directiva 95/46/CE).

La Directiva 95/46/CE regula las condiciones generales de licitud en el tratamiento de los datos, donde se amplia y detalla las previsiones del Convenio N.º 108, dejando a los Estados Miembros un cierto margen de discrecionalidad para regular y desarrollar de manera interna tales condiciones. En este sentido, la Directiva estableció un periodo de 3 años a los Estados Miembros para su transposición a sus respectivos derechos internos. Pero, dado que los Estados tienen cierta discrecionalidad en la transposición de directivas, supuso una transposición de forma diferente en ellos, lo que dio lugar a que se adoptasen diversas normas en materia de protección de datos en el conjunto de la UE, con textos legales y definiciones interpretadas de manera diferente en las legislaciones nacionales (GIAKOUMOPOULOS, BUTTARELLI y O'FLAHERTY 2018).

Siguiendo la cronología en relación a normativa de carácter regional europeo, en el año 2000 fue aprobada la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE), en la que su artículo 8 reconoce el derecho de toda persona a la protección de datos de carácter personal (art. 8 CDFUE). La aprobación de este texto fue necesaria para reforzar la protección de los derechos fundamentales, recogidos en textos anteriores, a la luz de los cambios sociales y avances científicos y tecnológicos que afrontan los Estados (Preámbulo CDFUE). Con ello se le ofreció a la UE una base jurídica específica para que, en base a la misma, pudieran adoptar actos legislativos destinados a proteger este derecho fundamental (Consejo Europeo, Consejo de Europa, 2022).

Por último, en cuanto a normativa europea se refiere, tras la necesidad de modernizar los textos legales en materia de protección de datos de la UE, la Comisión consideró preciso elaborar una propuesta de Reglamento, dando inicio a un largo proceso legislativo de negociaciones entre el Parlamento Europeo y el Consejo de la UE.

Con la entrada en vigor del Reglamento General de Protección de Datos, se inicia un proceso de modernización y actualización legislativa en materia de protección de datos, adecuándola para proteger los derechos fundamentales en el contexto de los retos económicos y sociales de la era digital, con la pretensión de unificar los principios de protección de datos de la UE. El RGPD conserva y desarrolla los principios y derechos esenciales del interesado, recogidos en la Directiva 95/46/CE sobre protección de datos. Así mismo, introduce nuevas disposiciones obligando a las organizaciones a introducir nuevos cambios en el tratamiento de los datos personales, como son, entre otras obligaciones, la aplicación la protección de datos desde el diseño y por defecto, el nombramiento de un Delegado de Protección de Datos para determinados supuestos tasados, la creación de un nuevo derecho a la portabilidad de los datos y cumplir con el principio de responsabilidad proactiva (GIAKOUMOPOULOS et al. 2018).

El ámbito de aplicación material del RGPD se atribuye al tratamiento total o parcial automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero (art. 2 RGPD). Por el contrario, no es de aplicación fuera del Espacio Económico Europeo (EEE) cuando se desarrollen actividades de tratamiento de datos únicamente en el ejercicio de actividades domésticas o personales, así como el tratamiento de datos por parte de jueces o tribunales.

El Reglamento, al ser de aplicación directa, conlleva la no necesidad de transposición nacional (a diferencia de la Directiva), lo que implica la creación de un único marco normativo para toda la UE, estableciendo un entorno de seguridad jurídica del que pueden beneficiarse tanto los operadores económicos como las personas físicas a las que se pretende proteger. No obstante, aunque el RGPD sea de aplicación directa, los Estados Miembros deben actualizar su legislación nacional en materia de protección de datos para que se ajuste al Reglamento, así como aplicar el margen de discrecionalidad para la adopción de disposiciones específicas que se contempla en su Considerando 10. En este sentido, autores como Artemi Rallo consideran que la aplicabilidad directa del Reglamento impide divergencias nacionales en su

aplicación, pues impone a las autoridades nacionales de los países de la UE un mecanismo de coherencia con el fin de garantizar la efectiva aplicación uniforme del Reglamento (LOMBARTE 2019).

No obstante lo anterior, la incorporación directa del RGPD al derecho nacional y la consiguiente derogación implícita de la normativa interna de protección de datos española anterior, supone un problema en cuanto a la afectación del principio de seguridad jurídica el cual obliga a una depuración del ordenamiento español que debería iniciarse con la derogación explícita de todas las normas nacionales que sean incompatibles con el RGPD (ROLLO 2019). Es por ello que, la actual normativa nacional en materia de protección de datos contiene una disposición derogatoria específica de toda normativa anterior contraria a lo dispuesto en el RGPD y por ende, en la normativa interna de desarrollo del mismo.

Hasta el año 2018 se encontraba operativo el Grupo de Trabajo del Artículo 29 (GT Art.29), tratándose de un ente europeo independiente el cual emitía opiniones vinculantes relacionadas con la protección de la privacidad y de los datos de carácter personal. Con la entrada en vigor del RGPD, fue sustituido por el actual Comité Europeo de Protección de Datos, órgano encargado de velar por el cumplimiento normativo.

Como hemos observado, el respeto a la vida privada y los datos personales son derechos fundamentales que necesitan una protección adecuada. Es por ello que el Parlamento Europeo ha insistido a lo largo de sus regulaciones en la necesidad de conseguir un equilibrio entre reforzar la seguridad y tutela de los derechos humanos, incluyendo la protección de los datos y de la vida privada desencadenando en una regulación europea en materia de protección de datos cuyo objetivo es fortalecer los derechos de los ciudadanos, aportándoles un mayor control de sus datos y tratando de garantizar su privacidad en la era digital (BERROCAL 2019).

Finalizando este apartado, comprobamos que, a lo largo de casi 60 años, ha habido una regulación en materia de protección de datos con tendencia a ampliar la protección de este derecho fundamental. Ello implica, a su vez, como ahora veremos, una amplia regulación y actualización por parte de los legisladores nacionales de los diferentes países, adaptando sus normativas internas a las regulaciones europeas, las cuales dejan un margen de discrecionalidad a los Estados para desarrollar y completar esta regulación interna.

2.1.2. Carencias del derecho nacional español en la regulación del derecho a la protección de datos personales

Una vez realizado el recorrido a través de los distintos instrumentos legislativos en materia de protección de datos a nivel europeo, analizaremos en este apartado los distintos instrumentos legales a nivel nacional que se han ido incorporando en España, desarrollando lo dispuesto en el orden internacional. El objetivo es examinar si han sido suficientes las actualizaciones normativas o, por el contrario, todavía encontramos carencias en la legislación actual.

El primer instrumento legislativo donde se hace mención a la regulación en materia de protección de datos personales es la Constitución Española del año 1978 (CE). Se regula de manera implícita este concepto, concretamente en su artículo 18.4, el cual dispone que la ley será la encargada de establecer los límites al uso de las nuevas tecnologías con el fin de asegurar el honor y la intimidad personal y familiar de los individuos, así como el pleno ejercicio de sus derechos (art. 18.4 CE).

Del precepto constitucional se infiere el derecho a la protección de datos como un derecho relacionado o ligado al derecho a la intimidad, honor y pleno ejercicio de derechos. En este sentido, conviene traer a colación la sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre (STC 292/2000), la cual se pronuncia sobre un recurso de inconstitucionalidad promovido por el Defensor del Pueblo con respecto a dos artículos específicos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD). En este pronunciamiento, se sienta por primera vez la distinción entre el derecho fundamental a la intimidad personal y familiar y el derecho fundamental a la protección de datos personales, ambos regulados en nuestra carta magna (STC 292/2000).

El Tribunal Constitucional viene a establecer el derecho a la protección de datos como "derecho fundamental autónomo" cuyo contenido se encuentra en la propia LOPD. Este derecho pretende garantizar que el ciudadano tenga un poder de control sobre sus datos personales frente al derecho fundamental a la intimidad, que pretende proteger cualquier invasión que pueda hacerse en el ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (STC 114/1999).

La sentencia continúa señalando que el objeto que protege el derecho a la protección de datos personales es más amplio que el del derecho a la intimidad pues extiende su garantía a cualquier tipo de dato personal que permita identificar a una persona, no únicamente a datos íntimos de los ciudadanos (STC 292/2000).

No obstante, la redacción del artículo 18.4 CE ha sido objeto de crítica por algunos autores. Así, por ejemplo, José Ignacio Cubero o Unai Aberasturi consideran que la CE ignora cualquier referencia a la protección de datos personales, siendo el Tribunal Constitucional el que ha tenido que hacer una interpretación de la misma (CUBERO y ABERASTURI 2008). Asimismo, otros autores afirman que tal y como está actualmente redactado el artículo, no está reconociendo un nuevo derecho autónomo (SERRANO 2005).

Sin embargo, esta no parece ser una opinión generalmente aceptada. Autores como Juan Luis Requejo Pagés o Artemi Rallo Lombarte, sostienen la idea de que, si bien la CE en sí misma no es lo suficientemente clara a la hora de hacer frente a la protección del derecho fundamental a la protección de datos personales, confirman que el constitucional sí reconoció este último como derecho fundamental, de manera independiente a los derechos de intimidad y honor (REQUEJO 2020).

En este sentido, el letrado del Tribunal de Justicia de la Unión Europea, Juan Luis Requejo Pagés, contempla la idea de que la CE pudo establecer una posible garantía del ámbito de la privacidad. En su redacción del artículo 18, incluye una cláusula en la que obliga a la ley a limitar el uso de la informática, con el fin de garantizar el honor y la intimidad personal y familiar de los ciudadanos. Así mismo, considera que, en un principio, se trataba de un mandato al legislador a fin de ofrecer una mayor protección de los derechos fundamentales al honor e intimidad. El objetivo era permitir que las personas pudieran acudir a la justicia en caso de ver violados sus derechos con motivo de una regulación deficiente del uso de la informática. Por ello, interpreta que el apartado 4 del artículo 18 CE no reconoce un derecho fundamental autónomo a la protección de datos, sino una garantía normativa a favor de los derechos al honor, intimidad y propia imagen (REQUEJO 2020).

No obstante lo anterior, el autor reconoce que, fue con la sentencia del Tribunal Constitucional STC 292/2000, cuando se pudo afirmar que el constituyente quiso garantizar no sólo un ámbito de protección específico, sino también un marco de protección más

oportuno que el que pudieran abarcar los derechos fundamentales señalados en el propio artículo 18 CE (REQUEJO 2020).

Así mismo, Artemi Rallo Lombarte afirma que, en un principio, el TC en su sentencia 254/1993, señala que "nuestra CE ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la CE llama la informática" (STC 254/1993).

Ello quiere decir que, el TC no restringe el alcance del artículo 18.4 CE al derecho al honor y a la intimidad, sino que lo amplía al otorgarle autonomía como un derecho fundamental frente a posibles agresiones a la dignidad y libertad de la persona, que pudieran surgir del tratamiento mecanizado de datos ilícitos. Ello significa que el artículo tiene un alcance más amplio y protege a los individuos de otras formas de invasión a su privacidad (LOMBARTE 2017).

Sin embargo, el Tribunal advirtió que, ante la falta de un desarrollo legislativo del artículo 18.4 CE, éste no es simplemente una recomendación al legislador y tiene la capacidad de amparar pretensiones individuales por sí solo. Por lo tanto, sin un desarrollo legislativo, el mandato constitucional sería de contenido mínimo, lo que lleva a TC a cuestionar cuál es ese contenido mínimo. No obstante, aunque el TC reconoce que el respeto al honor y privacidad son límites importantes para el contenido mínimo del artículo, advierte que, para garantizar la efectividad del derecho a la privacidad, puede requerirse garantías complementarias (LOMBARTE 2017).

Se amplía, por tanto, el derecho a la privacidad como un derecho a controlar el uso personal que se hace sobre el tratamiento de los datos personales de los individuos y, en caso de que los mismos se utilicen de manera ilegal, puedan recurrir a medidas legales para proteger su privacidad.

De igual forma debemos tener en cuenta que el derecho a la protección de datos personales, al ser un derecho europeizado, debe basarse también en la normativa de ámbito europeo y no exclusivamente en el artículo 18.4 CE. Es por ello que, hoy en día, dado que la normativa

española tiene su origen en la normativa europea, se deja poco margen de discrecionalidad a los Estados, los cuales han de observar, en todo caso, la normativa internacional. Por lo tanto, tal y como describe el autor Andoni Polo, resulta necesaria una ligera reforma constitucional para la redacción del artículo 18.4 CE en aras de adaptarlo a los avances tecnológicos estableciendo una expresa mención a la protección de datos y a los derechos digitales (POLO 2020). De hecho, esto no es una opinión aislada, dado que otros autores se pronuncian también sobre esta cuestión.

De hecho, cabe mencionar que, en el propio Preámbulo de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDGDD) ya se contemplaba la necesidad de reforma constitucional, en lo que respecta a la redacción del artículo 18.4 CE. En este sentido, los responsables de redactar la Carta Magna ya preveían que el impacto de la tecnología en nuestra sociedad y, en particular, en la protección de nuestros derechos fundamentales, sería significativo.

Para asegurar que la CE siga siendo relevante en la era digital en la que nos encontramos, es importante que se incluya una nueva generación de derechos digitales. Sin embargo, hasta que ocurra una futura reforma constitucional, es crucial que los legisladores trabajen en el reconocimiento de un sistema que garantice los derechos digitales, lo que está en línea con el mandato establecido en el apartado cuarto del artículo 18 CE. En algunos casos, la jurisprudencia ordinaria, constitucional e incluso europea, ya han perfilado estos derechos, pero se necesita una mayor claridad y certeza jurídica (Preámbulo LOPDGDD).

En esta misma corriente de pensamiento se encuentra la autora Rosario García Mahamut, afirmando, en consonancia con lo estipulado en la LOPDGDD, que la CE requiere de una reforma inmediata para responder a las necesidades actuales y regular los nuevos derechos digitales existentes. La autora reconoce que, dado que internet se ha vuelto indispensable para el desarrollo de la vida, tanto personal como profesional, es importante identificar los riesgos y oportunidades que el mundo digital ofrece a los ciudadanos. Así mismo, los poderes públicos deben liderar iniciativas que garanticen los derechos de la ciudadanía en internet. Solo de esta manera podremos ejercer nuestros derechos fundamentales plenamente, en una sociedad cada vez más globalizada y digitalizada (GARCÍA 2018).

Igualmente, el mencionado autor Artemi Rallo Lombarte, considera que no es suficiente la redacción actual del artículo 18.4 CE para cubrir las necesidades actuales en cuanto al

establecimiento de un marco de garantías en cuanto a la protección de nuevos derechos digitales de los ciudadanos. Destaca la importancia de reconocer, tanto legal como constitucionalmente, nuevos derechos digitales de nueva creación, surgidos en estos últimos años, con motivo de la incesante globalización tecnológica (LOMBARTE 2017).

Por último, Lombarte comparte una reflexión acerca de las carencias que implica lo dispuesto en el artículo 18.4 CE, para atender a las necesidades actuales para garantizar los derechos en Internet. Así mismo señala que, una posible reforma de la CE debería implicar la inclusión de protección de nuevos derechos surgidos como, por ejemplo, el derecho a la formación digital, el derecho a la neutralidad de la Red garantizando un internet libre o el derecho de los menores a su seguridad en la Red, entre otros (LOMBARTE 2017).

No obstante lo anterior, el artículo 18.4 CE no es la única referencia normativa en el ordenamiento jurídico español en esta materia. Más tarde, con motivo de la transposición de la Directiva 95/46/CE, a nivel nacional, se aprobó la LOPD. Esta norma impuso estrictas restricciones a la captación y utilización de datos personales, así como la exigencia de la creación de una autoridad nacional independiente en cada Estado Miembro de la UE. En el caso de España, esta autoridad es la Agencia Española de Protección de Datos (AEPD), la cual se encarga de supervisar todas las actividades relacionadas con el tratamiento de datos personales. Con la redacción de esta norma, el legislador español pretendió establecer una regulación que responda a los nuevos riesgos surgidos con la generalización de las tecnologías de la información. Entre ellos, la obtención de información personal de un sujeto sin su consentimiento o el uso indebido de esa información (HEREDERO 1994).

Posteriormente, se vio la necesidad de adaptar los textos legales de los Estados Miembros de la UE debido al aumento del intercambio de datos personales entre países y al intenso avance de la tecnología. Como resultado, la LOPD fue derogada tras la entrada en vigor del Reglamento General de Protección de Datos en la UE. Ello supuso la consecuente entrada en vigor de la norma vigente, la LOPDGDD. Con la aprobación de esta norma se adapta el ordenamiento jurídico español al Reglamento aprobado a nivel europeo, desarrollándolo y complementándolo en su contenido.

Como se ha expuesto anteriormente, la nueva normativa surge de la necesidad del legislador de abordar el reconocimiento de un sistema de garantía para los derechos, no solo personales, sino también digitales de los individuos, introduciendo cambios significativos con respecto a

las anteriores normas, creando nuevas obligaciones para los responsables del tratamiento de los datos (Preámbulo LOPDGDD). En primer lugar, el nuevo RGPD ha aumentado el importe de las sanciones por la comisión de infracciones en materia de protección de datos. En segundo lugar, todas las empresas tienen que identificar y realizar un análisis de todas las áreas de riesgo, incluyendo las operaciones de tratamiento realizadas con la creación del denominado «Registro de Actividades de Tratamiento» (que sustituye la obligatoriedad de inscripción de ficheros ante la AEPD). Por otra parte, se determina la necesidad de firmar un contrato de encargado de tratamiento siempre que un proveedor de servicios vaya a tratar datos personales por cuenta de su cliente. Así mismo, se estableció la necesidad de realizar una evaluación de impacto para aquellas organizaciones que realicen tratamientos de datos personales que puedan implicar un alto riesgo para los derechos y libertades de las personas físicas. Por último, se reconoce un amplio y nuevo conjunto de derechos digitales para la ciudadanía, conforme al mandato que se establece en el artículo 18.4 CE (FERNÁNDEZ 2016).

Como se puede observar, actualmente hay una escasa regulación en materia de protección de datos personales a nivel europeo, dado que los primeros textos legales datan entorno a los años 40. No obstante, debido al creciente desarrollo de las sociedades actuales, la gran cantidad de transferencias internacionales de datos que se realizan y el uso de las nuevas tecnologías, en las últimas décadas hemos experimentado una tendencia a la alza en cuanto a creación normativa se refiere, aunque siguen existiendo lagunas legales las cuales deberán abordarse en un futuro, como por ejemplo, las situaciones derivadas del uso de la inteligencia artificial y el impacto que supone en cuanto al conocimiento y tratamiento de los datos.

En definitiva, tras el análisis de la evolución en el tiempo de las diferentes regulaciones sobre protección de datos personales, se analizará la repercusión que ha tenido el virus SARS CoV-2 en los derechos fundamentales de los ciudadanos, concretamente en nuestro derecho fundamental a la protección de datos personales. Para abordar esta cuestión, se debe reflejar qué entiende el legislador como datos de carácter personal y su diferencia con las categorías especiales de datos, con el fin de analizar una serie de tratamientos de datos concretos que se llevan a cabo con motivo de la pandemia.

2.2. LEGITIMACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

2.2.1. Concepto de dato personal y criterios que legitiman su tratamiento

Para poder determinar si, con motivo de la pandemia sufrida por el SARS CoV-2, los derechos de los ciudadanos se vieron afectados o limitados debido a las medidas excepcionales decretadas por los países de todo el mundo, se deben analizar una serie de conceptos jurídicos establecidos en la normativa de protección de datos de carácter personal.

El concepto «dato personal» ha sido establecido en las diferentes normas, tanto a nivel europeo como a nivel nacional, manteniendo todas ellas, una percepción en sentido amplio de la definición (Dict. Grupo de Trabajo del Artículo 29, de 20 de junio de 2007).

En este sentido, el RGPD no establece una lista concreta de lo que son o no datos personales considerando los mismos como cualquier tipo de información sobre un individuo identificado o identificable. Así mismo, establece como persona física identificable aquella cuya identidad pueda determinarse directa o indirectamente, mediante un identificador, como, por ejemplo, un nombre, número de identificación, datos de localización, identificador en línea o uno o varios elementos propios de la identificación física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona, incluso la forma de caminar de una persona puede llegar a considerarse como dato personal (art. 4 RGPD). La normativa en materia de protección de datos entiende el concepto «identificada» a una persona física cuando, dentro de un grupo de personas, se la distingue de todos los demás miembros del grupo. Por consiguiente, la persona física es «identificable» cuando, aunque no se la haya identificado todavía, sea posible hacerlo (Dict. GT Art. 29, de 20 de junio de 2007).

En este mismo sentido se pronunció el Tribunal Supremo en su sentencia STS 5073/2004, de 12 de julio de 2004, en la cual se entiende que la silueta de una persona puede llegar a arrojar suficiente información personal como para poder llegar a identificar a una persona de manera concreta. Curiosamente, en la sentencia no se hace referencia a la protección de datos personales, sino que habla de una vulneración de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. En los hechos enjuiciados, una persona demandó a un fotógrafo por publicar en un periódico, una imagen de su contorno o silueta donde era visible nítidamente. En primera instancia se dio la razón a la persona afectada por la publicación de su imagen condenando tanto al

fotógrafo como al periódico. La sentencia fue recurrida en segunda instancia donde el tribunal revocó la sentencia anterior absolviendo al fotógrafo y al periódico de la condena, entendiendo que el rostro de la persona no era visible y que la silueta no ofrecía signos especiales o singulares que permitirán la identificación de una persona. Por último, se recurrió ante el Tribunal Supremo que sentenció a favor de la persona afectada alegando lo fallado por el tribunal de primera instancia donde varios testigos reconocieron a la persona fotografiada. En conclusión, la silueta de una persona es un dato suficiente para poder identificarla, encajando dentro del concepto de «identificable» establecido en la normativa relativa a la protección de datos personales.

Esta última sentencia es de gran relevancia debido a que aclara el concepto de dato personal, en tanto en cuanto determina qué criterios deben tenerse en cuenta para concretar si un dato tiene consideración de personal o no. Así mismo, es necesaria su aclaración, pues a lo largo del trabajo se determina si ha habido afectación de nuestro derecho fundamental a la protección de datos personales, por lo que hay que establecer cuál es el concepto más aproximado de «dato personal» (STS 5073/2004).

Pues bien, para que el tratamiento de los datos personales sea lícito, los mismos deben ser tratados en base al cumplimiento de una serie de criterios legitimadores establecidos en el artículo 6 RGPD. El primero de los criterios que legitiman el tratamiento de los datos de carácter personal de los interesados es el consentimiento. El propio Reglamento establece cómo debe prestarse el consentimiento, debiendo ser el responsable del tratamiento capaz de demostrar que el interesado consintió el tratamiento de sus datos personales (art. 7 RGPD). Así mismo, el consentimiento debe prestarse mediante un claro acto afirmativo que refleje la manifestación de voluntad libre, específica, informada e inequívoca del interesado al aceptar el tratamiento de sus datos, como, por ejemplo, una declaración escrita, verbal o a través de medios electrónicos (Considerando 32 RGPD).

El segundo supuesto es la necesidad de tratamiento de los datos personales con motivo de la ejecución de un contrato. En este sentido, se presume lícito el tratamiento de los datos personales del interesado cuando sea necesario para la ejecución de un contrato en el que el interesado es parte, o para la aplicación de medidas precontractuales. La existencia de un vínculo de naturaleza contractual o tratamientos preliminares, también son actos justificativos de dicha licitud (art. 6.1 b) RGPD).

Continuando con los supuestos del artículo 6 RGPD, encontramos la necesidad de tratamiento para cumplir con una obligación legal. Para ello, el tratamiento será lícito cuando el mismo sea necesario para cumplir con una obligación estipulada en una norma con rango legal, no siendo necesario el consentimiento del interesado, pues la justificación se encuentra en la propia ley (art. 6.1 c) RGPD). En este aspecto, este apartado cobra gran importancia en el análisis de este trabajo. Este criterio pudo haberse seguido a la hora de tratar de legitimar el tratamiento de nuestros datos de salud con motivo de la pandemia por coronavirus, pues puede entenderse que el decreto del estado de alarma era una habilitación legal para ello.

El cuarto criterio legitimador es la necesidad de proteger intereses vitales. Lo que el legislador europeo ha señalado es que el tratamiento de los datos personales no requerirá consentimiento del interesado cuando el mismo derive de la necesidad de protección de intereses vitales del interesado o de otra persona física, siempre que no prevalezcan otros derechos fundamentales frente al derecho a la protección de datos personales (art. 6.1 d) RGPD).

En penúltimo lugar encontramos la necesidad de tratamiento de los datos personales para para cumplir con una misión realizada en interés público. Para este supuesto es necesario que exista una norma previa habilitante que confiera tanto el interés público de dicha misión, como el ejercicio del poder público de tal función (art. 6.1 e) RGPD).

Los dos criterios anteriores, tanto la necesidad de protección de intereses vitales, como el cumplimiento de una misión realizada en interés público, también pudieron ser habilitaciones para la licitud del tratamiento de los datos sensibles de los ciudadanos. Sobre esta cuestión se ha pronunciado el autor Juan Francisco Rodríguez Ayuso, el cual considera que, en situaciones excepcionales como es una pandemia, el RGPD contiene habilitaciones legales para el tratamiento de datos especialmente protegidos, tanto por parte de organismos públicos como privados, con el fin de evitar la propagación del virus y defender la vida de las personas (RODRÍGUEZ 2021). En esta misma línea de pensamiento, la autora Ana Marzo Portera también llegó a la conclusión de que las normas de protección de datos personales no deberían ser un obstáculo para la protección de la salud de la población, pues nuestro ordenamiento jurídico prevé situaciones de este tipo (MARZO 2020).

Por último, se encuentra la necesidad del tratamiento de los datos para satisfacer intereses legítimos. Se considera lícito el tratamiento de los datos personales cuando sea necesario para

la satisfacción de intereses legítimos del responsable o de una tercera persona, siempre que los mismos no prevalezcan sobre lo intereses o derechos y libertades del interesado, particularmente cuando el interesado sea un niño. En este apartado se debe concretar el concepto de «interés legítimo» pues se trata de un concepto jurídico indeterminado que debe ser completado en cada caso en función de las circunstancias concretas. No obstante, existe una mención expresa en la norma en relación a esta última disposición donde exceptúa su aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de las funciones que legalmente les hayan sido encomendadas (art. 6.1 f) RGPD).

Como hemos observado, el legislador europeo ha señalado una serie de supuestos específicos que habilitan el tratamiento de los datos personales. Se trata de una lista cerrada en la que, en principio, no se admiten otros criterios distintos a los ya establecidos, por lo que podrían llegar a quedar fuera de regulación diversos tratamientos de datos personales cuando el único criterio aplicable fuese el consentimiento del interesado, entendiendo este apartado como un «cajón de sastre».

En el ámbito del empleo del consentimiento como medio de legitimación del tratamiento de datos personales, se pronunció el Grupo de Trabajo del Artículo 29, concretamente en su Dictamen 15/2011, sobre la definición del consentimiento. Destaca la idea de que el consentimiento no siempre es el criterio legitimador más idóneo o adecuado para que un tratamiento de datos personales sea legítimo. Pueden darse circunstancias en las que el consentimiento sea una base de legitimación insuficiente y pierda valor si se adapta a supuestos donde no debería utilizarse, pudiendo derivar en una situación de vulnerabilidad (Dict. Grupo Art. 24, de 13 de julio de 2011).

Dado que uno de los requisitos para que se entienda que el consentimiento se ha prestado de una manera válida, el propio Considerando 32 del RGPD contempla que debe ser un acto de voluntad “libre” (Considerando 32 RGPD). Por lo tanto, no debe mediar ningún tipo de intimidación o engaño hacia el interesado para que preste su consentimiento. Así, por ejemplo, en el ámbito laboral, donde hay un elemento de subordinación del empleado al empleador, o en los servicios de salud que presta la administración, el consentimiento puede verse viciado y por tanto no se consideraría válido.

Visto el concepto de dato personal y las bases de legitimación para el tratamiento de datos personales, conviene analizar en qué supuestos, de manera excepcional, se podrán tratar

categorías especiales de datos. En este sentido, ya no serán válidos los criterios citados sobre estas líneas, pues, con carácter general, se prohíbe uso de los datos sensibles.

2.2.2. Concepto de categorías especiales de datos y criterios que legitiman su tratamiento

En este apartado centraremos el estudio en las bases de licitud para el tratamiento de las categorías especiales de datos personales, con el objetivo de observar las diferencias entre los criterios legitimadores a la hora de tratar datos personales generales y datos personales de carácter sensibles. El RGPD establece en su artículo 9, las categorías especiales de datos que considera como sensibles y que, en consecuencia, requieren una protección especial, bien sea por su naturaleza o bien por la relación o implicación que pudieran tener en relación con los derechos y libertades de las personas, quedando sujetos a determinadas disposiciones cuando su tratamiento implique un alto riesgo para los interesados.

Pues bien, la normativa europea considera datos sensibles aquellos 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 orientaciones sexuales de una persona física (art. 9 RGPD). En el Considerando 51 del RGPD encontramos la categorización de los datos sensibles en relación con los derechos y libertades fundamentales de los interesados y, por tanto, estos datos no deben ser tratados, salvo que se permita su tratamiento en supuestos específicos estipulados en el propio Reglamento (Considerando 51 RGPD).

El propio Reglamento establece, como regla general, la prohibición expresa del tratamiento de los datos de carácter sensible citados anteriormente. Si bien esto es cierto, se permite su tratamiento en algunas situaciones excepcionales. Esto ocurriría cuando el interesado haya prestado su consentimiento de manera expresa; cuando exista la necesidad de cumplir con una obligación legal; cuando el tratamiento sea necesario para la protección de intereses vitales; cuando el tratamiento lo efectúen entidades sin ánimo de lucro con finalidades políticas, filosóficas, religiosas o sindicales (previo consentimiento); cuando los datos tratados se hayan hecho manifiestamente públicos previamente por el interesado; cuando el tratamiento se lleve a cabo por los jueces en el ejercicio de su función judicial; cuando haya

razones de interés público esencial (siempre que se motive y sean de manera proporcionada); cuando se necesite tratar los datos con finalidades médicas preventivas o laborales; cuando el tratamiento sea necesario por razones de interés público en el ámbito de la salud pública como la protección frente a amenazas transfronterizas; y, por último, cuando el tratamiento se requiera con fines de archivo en interés público, científico o estadístico (art. 9 RGPD).

Como puede apreciarse, podría entenderse que el RGPD establece supuestos concretos para poder llevar a cabo un tratamiento de datos especiales. Pues bien, contextualizando el tratamiento de categorías especiales de datos durante la pandemia de COVID-19, autores como Ana Marzo consideran prioritaria la salud de la población frente al derecho a la protección de datos personales. Así mismo, señalan que la norma europea regula este tipo de situaciones excepcionales, por lo que, *a priori*, el tratamiento de los datos personales que pudieran efectuarse por parte de entidades u organismos públicos, se encuentra legitimado, en cuanto a protección de datos se refiere (MARZO 2020).

En contra, el autor Carlos Vidal realiza una crítica al procesamiento de datos personales durante la pandemia, especialmente sobre datos relativos a la salud. Debido a la insuficiencia legislativa que había tras la declaración del estado de alarma, las diferentes Comunidades Autónomas aprobaron diferentes normas específicas, lo que dio lugar a que los diferentes juzgados contencioso-administrativos ratificasen o no las medias que fueron adoptando las diferentes autoridades sanitarias, como, por ejemplo, la implantación del llamado «pasaporte COVID-19» –véase en el epígrafe 2.3.3.2– (PARDO 2021). El autor critica que la mayoría de las medidas adoptadas alegaban tener cobertura legal en materia sanitaria, concretamente basándose en el artículo 3 de la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública (LOMESP), la cual considera que está redactada de manera muy genérica (PARDO 2021). No obstante, algunos autores como Alba Nogueira, entre otros, consideran este precepto suficiente para adoptar medidas que afectasen a toda la población (NOGUEIRA 2020).

De la regulación establecida por el legislador europeo sobre datos de carácter sensible, se desprende que, salvo los supuestos tasados en la normativa y salvo las excepciones previstas, no se podrá tratar bajo ningún concepto datos de categorías especiales. Esta afirmación lo que supone es que, con el desarrollo tecnológico y la constante evolución de la sociedad, los Estados Miembros deberán regular a través de su normativa interna, supuestos de nueva

creación los cuales unos Estados contemplarán y otros no, por lo que se podría volver a producir una desarmonización a nivel comunitaria de conceptos y regulación. El RGPD no deja espacio a la interpretación del precepto regulador de los criterios legitimadores a la hora de tratar datos de carácter sensible, así como la posible inclusión de nuevos supuestos legitimadores que pudieran derivarse de nuevos tratamientos de datos.

Al igual que sucede con los criterios establecidos en el artículo 6 RGPD, los supuestos legitimadores del artículo 9 RGPD, en principio, tampoco admiten más escenarios fuera de los que ya se encuentran previstos en la norma. En este sentido, pueden darse situaciones en las que se generen supuestos nuevos donde se pudiera plantear un conflicto, tanto en relación con los derechos fundamentales afectados, como en relación a la contradicción normativa.

En esos supuestos concretos que devengan de situaciones sociales, políticas o económicas de actualidad, corresponderá al legislador de cada Estado Miembro establecer criterios legitimadores diferentes, lo que implicará que difieran las regulaciones en los diferentes países. Aunque los Estados Miembros cuentan con una normativa comunitaria, como es el Reglamento General de Protección de Datos, la norma de protección se desarrolla y complementa de manera diferente en unos países y otros, lo que da lugar a que juzgados y tribunales puedan generar con el tiempo varios criterios diferentes, pudiendo llegar a ser contradictorios. Ello supone que un mismo precepto contemplado en la normativa europea, sea desarrollado o completado según la interpretación del legislador a la hora de elaborar la normativa interna en cada país.

En este sentido, la normativa europea de protección de datos personales permite establecer excepciones en la regulación interna de cada Estado Miembro, ya que les permite cierto margen maniobra a la hora de desarrollar el RGPD de manera interna. A modo de ejemplo, el consentimiento puede ser un criterio legitimador no válido para el tratamiento de categorías especiales de datos si un Estado lo prohíbe en su legislación interna de desarrollo. El levantamiento de la prohibición general de tratamiento de categorías especiales de datos tomando como base el consentimiento del interesado, por lo tanto, no serviría como criterio legitimador válido.

Uno de los casos que puso de relieve la problemática de la legitimación del tratamiento de estos supuestos, fue el contexto generado a raíz de la pandemia provocada por el COVID-19. La pandemia dio lugar a un conflicto de derechos fundamentales entre los que se encontraba

el derecho a la protección de datos personales, sobre el cual todavía, a día de hoy, no hay suficiente jurisprudencia por parte de tribunales y autoridades competentes, tanto a nivel europeo como a nivel interno en los diferentes Estados Miembros. Sin embargo, esto no quiere decir que la cuestión haya sido pacífica. Desde el año en que surgió la pandemia hasta la actualidad, el TEDH ha recibido numerosas demandas en cuanto a posibles vulneraciones de derechos con motivo de la pandemia – véase, posteriormente, en el epígrafe siguiente 2.3.

Como ya se ha expuesto anteriormente, la regla general es la prohibición del tratamiento de categorías especiales de datos, salvo que se dé alguna de las excepciones mencionadas en el artículo 9 RGPD. Para ello, los responsables de tratar datos de carácter sensible, habrán de cumplir con lo dispuesto en las normas de protección de datos personales, concretamente aplicando el principio de licitud, así como estableciendo medidas especiales de seguridad.

Analizando el concepto de categorías especiales de datos y su tratamiento relacionado con el presente trabajo, encontramos que el RGPD ya contemplaba en su Considerando 46 que la base jurídica de los tratamientos de datos realizado con motivo de una epidemia podría basarse tanto en el interés público como en el interés vital del interesado u otra persona física (Considerando 46 RGPD). Sin embargo, para el tratamiento de datos de carácter sensible, como son los datos relativos a la salud de las personas, no es suficiente con que exista un criterio jurídico establecido en el art. 6 RGPD, sino que, tal y como establece el art. 9 RGPD, exista una circunstancia que levante la prohibición expresa de tratamiento de dicha categoría especial de datos.

Es por ello que, una vez planteada la distinción de las categorías de datos, analizaremos si los siguientes escenarios planteados implican tratamientos de categorías especiales de datos, siendo de aplicación lo dispuesto en el mencionado artículo 9 RGPD. En este sentido veremos que, durante la pandemia de coronavirus, en numerosas situaciones fue necesario el tratamiento de nuestros datos de salud para frenar la propagación del virus, lo que supone una especial atención a las normas reguladoras de nuestro derecho fundamental a la protección de datos personales, ya que, como hemos visto, no siempre será legítimo procesar nuestros datos sensibles, como son los datos relativos a la salud.

2.3. CONTEXTUALIZACIÓN Y ANÁLISIS DE LOS TRATAMIENTOS DE DATOS PERSONALES EFECTUADOS COMO MOTIVO DEL COVID-19

2.3.1. Las medidas decretadas en la pandemia del COVID-19 y el TEDH

La emergencia sanitaria que ha afectado a nuestro país a raíz del COVID-19 y el consecutivo decreto del estado de alarma (RD 463/2020) ha desencadenado numerosos retos en el ámbito económico, social y jurídico. La salvaguarda de los ciudadanos y su colisión con los derechos fundamentales han generado una de las cuestiones más controvertidas en los últimos años, la prevalencia del bienestar social frente a la intromisión o limitación de derechos fundamentales.

A comienzos de marzo de 2020, debido a los efectos que podía provocar la enfermedad en la salud de los ciudadanos de todo el mundo, así como las consecuencias sanitarias derivadas de los mismos, dieron lugar a que las autoridades competentes de los diversos Estados decretasen una serie de medidas sanitarias con objeto de frenar la expansión de la epidemia y proteger a la ciudadanía, afectando consigo a los derechos y libertades de las personas (LA MONCLOA 2020).

En España, el Gobierno decretó el estado de alarma de la nación, suponiendo esto una suspensión temporal de derechos a través del Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19, se determinaron una serie de medidas en aras de prevenir nuevos contagios y controlar la propagación del virus (RD 463/2020). Una de las medidas contenidas en ese decreto fue el confinamiento total de la población en sus hogares, permitiendo la salida únicamente al personal dedicado a sectores de servicios esenciales, para que la población pudiera proveerse de alimentos y medicamentos, afectando al derecho fundamental a la libre circulación de personas. Otra de las medidas decretadas fue el uso obligatorio de la mascarilla, tanto en espacios cerrados como en espacios abiertos. Hay autores que consideran que la declaración del estado de alarma no supone la suspensión del derecho fundamental a la protección de datos, tan solo conlleva la adopción de algunas medidas que implican la limitación en el ejercicio de determinados derechos y libertades (PIÑAR 2020).

Paulatinamente se fueron rebajando las medidas adoptadas a comienzos de la pandemia, teniendo que establecerse nuevas medidas para seguir combatiendo la enfermedad, como

fueron la administración de vacunas a la sociedad de manera escalonada por franjas de edad y personas de riesgo y la creación del llamado «certificado COVID-19».

En este sentido, algunas autoridades de control pertenecientes a los distintos países europeos, debido al aluvión de consultas realizadas, tanto por representantes de personas jurídicas, empleados, asociaciones como interesados afectados, emitieron una serie de opiniones e informes, elaborados por sus gabinetes jurídicos, a cerca de la implicación del tratamiento de los datos personales relacionados con el COVID-19, suponiendo, en su mayoría, una doctrina más restrictiva de las medidas para hacer frente al COVID-19.

Una de ellas fue la autoridad francesa de protección de datos, Commission Nationale Informatique & Libestés (CNIL), determinando que los empleadores no podían violar la privacidad de las personas llevando a cabo tratamientos de datos dotados de protección especial, como son los datos de salud. En este sentido, la misma señaló la imposibilidad de implementar controles de temperatura obligatorios de empleados o visitantes a las instalaciones (CNIL 2022).

En semejante línea se pronunció la autoridad italiana de protección de datos de carácter personal (Garante per la protezione dei dati personali), la cual emitió un comunicado señalando que las entidades no debían recopilar, de manera generalizada y sistemática, información sobre cualquier síntoma de COVID-19. De esta manera, justificaba que, únicamente las entidades encargadas de la prevención de la salud y protección civil, eran los organismos autorizados para recopilar información relacionada con los síntomas de COVID-19 (Garante per la protezione dei dati personali 2020).

Siguiendo un criterio menos restrictivo en cuanto a la aplicación de medidas para evitar la propagación del virus, la Agencia Española de Protección de Datos emitió un informe en el que establecía que la normativa en materia de protección de datos personales, no debería ser utilizada con el objetivo de obstaculizar o limitar la efectividad de las medidas adoptadas por las autoridades sanitarias contra la enfermedad. Argumentaba que el RGPD contempla una regulación para los supuestos en los que se produzca una epidemia, compatibilizando los intereses y derechos de los ciudadanos con la salvaguarda del interés general (Informe AEPD 0017/2020).

Sin embargo, algunos de los intentos de compatibilizar las normativas con la situación de pandemia trajeron como repercusión que los ciudadanos europeos interpusieran demandas ante el Tribunal Europeo de Derechos Humanos, al considerar afectados o limitados sus derechos fundamentales.

Así, por ejemplo, en la sentencia del TEDH Zambrano contra Francia se interpuso demanda ante el tribunal por parte de un profesor universitario, con motivo de la obligatoriedad de portar el certificado COVID-19. Lideró un movimiento popular de protesta en contra del pasaporte COVID-19 e instó a los ciudadanos a que interpusieran demandas ante el TEDH. El Tribunal falló inadmitiendo la demanda, entre otros motivos, por no haber agotado las vías internas, así como por considerarlo un abuso del derecho de demanda individual (STEDH Caso Zambrano contra Francia).

Por su parte, en el caso de Thevenon contra Francia se estudiaba la negativa de un bombero a vacunarse del COVID-19, siendo requisito impuesto a los trabajadores por la Ley núm. 2021-1040, de 5 de agosto de 2021, sobre la gestión de la crisis sanitaria. El reclamante fue suspendido de empleo y sueldo por negarse a que se le administrase una dosis de la vacuna, sin haber expuesto ningún tipo de exención médica conforme a la normativa. Al igual que en el supuesto expuesto anteriormente citado, el Tribunal declaró la inadmisibilidad de la demanda por no haber acudido previamente a los tribunales nacionales antes de acudir directamente al TEDH (STEDH Caso Thevenon contra Francia).

Por otro lado, en el caso Theres contra Rumanía, un diputado del Parlamento Europeo interpuso una demanda contra el confinamiento que se impuso por parte del gobierno rumano, entre el 24 de marzo y el 14 de mayo de 2020, con motivo de frenar la expansión de pandemia. El demandante alegó que ese confinamiento era equivalente a la interposición de un arresto domiciliario como medida privativa de libertad. El TEDH inadmitió la demanda al considerarla incompatible con las disposiciones del CEDH. Así mismo, declaró que el confinamiento no podía ser considerado como un arresto domiciliario, aludiendo al artículo 5 del CEDH, relativo al derecho a la libertad y a la seguridad. Por otra parte, el Tribunal expuso que el demandante no había aclarado el impacto concreto que había tenido la medida decretada sobre su situación personal (STEDH Caso Theres contra Rumanía).

En resumen, se puede observar, en líneas generales, cómo los ciudadanos acuden directamente al TEDH, lo que lleva a concluir que las medidas adoptadas por la pandemia han

generado una preocupación sobre la existencia de potenciales vulneraciones de derechos humanos. Se trata de un tema no carente de debate, pues en un corto espacio de tiempo, se han dado traslado a bastantes casos que han llegado hasta el TEDH. Si bien es cierto, gran parte de ellos, como se ha expuesto, han sido inadmitidos por no haber agotado las vías jurisdiccionales internas antes de trasladar las quejas a tribunales superiores.

A continuación, se expondrán una serie de casos concretos en los cuales se examinará si los criterios de legitimación aplicados fueron efectivamente los adecuados en España. En ello, se analizará la posible vulneración del derecho fundamental a la protección de datos, debido a las medidas adoptadas por las autoridades sanitarias en el contexto de la pandemia, pues el tratamiento de categorías especiales de datos podría suponer un alto riesgo para los derechos y libertades de los interesados. Los escenarios analizados implican un tratamiento de categorías especiales de datos, no obstante, algunos como el teletrabajo no necesariamente conllevan un tratamiento de datos sensibles, como veremos.

2.3.2. Tratamientos de datos personales en el ámbito laboral con motivo de una pandemia

En esta sección centraremos el estudio en un conjunto específico de escenarios en los que, debido al virus SARS CoV-2, se ha podido producir algún tipo de injerencia por parte de las autoridades o entidades privadas en el procesamiento de los datos personales, en particular los datos relacionados con la salud, dando lugar a una posible intromisión en los derechos fundamentales, como la privacidad o la protección de datos personales. En este sentido, se comentarán cuestiones que implican un tratamiento de datos de salud en el ámbito del trabajo, en una época afectada por la pandemia del SARS CoV-2, como son el teletrabajo, el control de temperatura de trabajadores, el acceso al empleo y la obligatoriedad de vacunación, así como la potencial vulneración de derechos de los individuos.

2.3.2.1. El teletrabajo

En primer lugar, se analiza el tratamiento de datos personales que, tanto empresas como organismos públicos llevaron a cabo mediante la implantación del sistema de teletrabajo. En este sentido, la situación excepcional derivada de la pandemia supuso la urgente necesidad de cambio en los modelos de negocios tradicionales, lo que derivó en la adopción de políticas

como el teletrabajo. En un mínimo intervalo de tiempo fue necesario adoptar medidas de carácter urgente y hacer uso de accesos remotos y plataformas online para que las actividades laborales y educativas pudieran seguir desarrollándose con una cierta normalidad.

El contexto del teletrabajo plantea un nuevo escenario de riesgos en materia de protección de datos personales que deben ser gestionados de manera adecuada por el responsable de tratamiento para evitar la comisión de infracciones normativas y posibles brechas de seguridad de la información. Para ello, la AEPD publicó una serie de recomendaciones para que los responsables de tratamiento adaptasen el tratamiento de los datos personales al contexto del teletrabajo cumplimento con la normativa de protección de datos (Recomendación AEPD 2020).

Organismos tales como el Instituto Nacional de Ciberseguridad (INCIBE) establecieron pautas para fomentar un entorno de trabajo ciberseguro. Las distintas guías publicadas por el citado organismo fueron publicadas con la finalidad de que las empresas conocieran las distintas amenazas que pueden derivar de no implantar políticas de seguridad a la hora de teletrabajar (INCIBE 2020). Por su parte, el Gobierno aprobó el Real Decreto-Ley 28/2020, de 22 de septiembre, de trabajo a distancia (RDL 28/2020) que se incorporó al ordenamiento jurídico a través de la Ley 10/2021, de 9 de julio, de trabajo a distancia (Ley 10/2021).

En este sentido, el artículo 32.1 RGPD establece la necesidad de aplicación de medidas de carácter técnico y organizativo en aras de garantizar un nivel de seguridad adecuado a los posibles riesgos para los derechos y libertades de las personas en el tratamiento de sus datos personales (art. 32 RGPD) lo que conlleva, en este caso, la adopción previa de políticas encaminadas a garantizar la seguridad de los datos en el teletrabajo.

En lo que respecta a las categorías especiales de datos, únicamente se podrá amparar el tratamiento de los mismos cuando sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos de la persona responsable de tratamiento o de la persona interesada en el ámbito que establece el derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice la norma o un convenio colectivo con arreglo a derecho que establezca las garantías adecuadas para el respeto de los derechos fundamentales y de los intereses de la persona interesada (art. 9.1 b) RGPD).

No obstante lo anterior, el teletrabajo no necesariamente implica un tratamiento de categorías especiales de datos, pues habrá casos en los que el empleador, por ejemplo, únicamente tratará sus datos de contacto, bien personales o bien corporativos. Por el contrario, pueden darse situaciones en las que sí haya un tratamiento de datos personales sensibles, como podría ser el registro de jornada utilizando datos biométricos.

Así mismo se debe tener una previsión dentro de las empresas con respecto a los derechos relacionados con el uso de dispositivos en el ámbito laboral, tanto propios como proporcionados por la empresa a sus trabajadores. En este sentido, el uso de dispositivos tecnológicos a través de los cuales se traten datos de carácter personal, podrá afectar a derechos como son el derecho a la intimidad del trabajador, así como el derecho a la desconexión digital.

En definitiva, cuando se implanta el teletrabajo en las entidades, hay que tomar decisiones para gestionar el cambio en la naturaleza del tratamiento y la forma en la que se implementa, volver a evaluar los riesgos existentes y tratarlos de manera adecuada con el fin de minimizar su posible impacto, ya que el Dictamen 2/2017 del Grupo de Trabajo del Artículo 29 respecto al tratamiento de datos en el ámbito laboral advierte de que el teletrabajo supone un riesgo adicional para los derechos y libertades, tanto de las personas trabajadores como de los sujetos de los datos que éstas tratan (Dict. Grupo de Trabajo Art. 29, de 8 de junio de 2017).

Por último, señalar que la crisis sanitaria del COVID-19 ha supuesto un antes y un después en la consideración de la población sobre el teletrabajo. En la mayoría de los países europeos, el teletrabajo era una práctica ocasional que experimentó un incremento en el año 2020, llegando a ser el porcentaje total de ocupados que trabaja habitualmente en su domicilio en la Unión Europea en torno a un 21%, frente al 5,4% en el año 2019 (Randstad Research 2021). Dentro de la Unión Europea, encontramos países como Luxemburgo, Holanda o Suiza que superan el 40% de ocupados que teletrabajan, siendo países con gran nivel de desarrollo económico muy por encima de la media europea (21%), en comparación con países como España o Italia, que no llegan al 15% (Randstad Research 2021).

Debemos destacar que España no es una gran potencia mundial en lo que a teletrabajo se refiere, dado que no es un país con una cultura de teletrabajo instaurada, lo que provoca una falta de regulación por parte de las autoridades competentes, así como una falta de conciencia y actuación de los empleadores y trabajadores pues, como podemos comprobar, no

contábamos con una ley reguladora del teletrabajo hasta el año 2021 (Ley 10/2021, de 9 de julio, de trabajo a distancia). La situación sanitaria provocada por el virus derivó en tener que reaccionar rápidamente ante la implantación de medidas para regular el teletrabajo y la forma de tratamiento de los datos personales que conlleva, aumentando exponencialmente el teletrabajo como forma de desarrollo de la prestación laboral.

2.3.2.2. La realización de pruebas para la detección del COVID-19

En segundo lugar, se analiza el tratamiento de datos personales de los empleados relativos al control de temperatura corporal por parte del empleador y la realización de pruebas para la detección del COVID-19 en el ámbito laboral.

Es importante subrayar que, en el entorno laboral, los empleadores tienen obligación de garantizar la seguridad y salud de las personas trabajadoras a su servicio en los aspectos relacionados con el trabajo (art. 19 RD Leg. 2/2015). Esta obligación opera tanto como excepción que permite el tratamiento de los datos de salud como la base jurídica que legitima el tratamiento de los mismos (art. 9.1 b) RGPD).

En aplicación de lo establecido en la normativa sanitaria y laboral y, en particular, en la Ley 31/1995, de 8 de noviembre, de prevención de riesgos laborales (LPRL) (Ley 31/1995), los empleadores podrán tratar, de acuerdo con dicha normativa y con las garantías que establecen, los datos del personal necesarios para garantizar su salud y adoptar las medidas necesarias por las autoridades competentes, lo que incluye igualmente asegurar el derecho a la protección de la salud del resto del personal y evitar los contagios en el seno de la empresa o centros de trabajo. Es por ello que existe habilitación legal como criterio legitimador para controlar la temperatura de los trabajadores en el ámbito laboral, tal y como señaló la AEPD en un comunicado de fecha 30 de abril de 2020 (AEPD 30 de abril de 2020).

No obstante, aun existiendo una base legal para el tratamiento de los datos de salud de los trabajadores en cuanto al control de temperatura, la AEPD señala que deberán tenerse en cuenta los principios de minimización de datos, tratando los datos de manera limitada a lo necesario en relación a los fines para los que se capta, por lo que no deben ser utilizados con una finalidad diferente (AEPD 30 de abril de 2020).

Sobre este punto se ha pronunciado el Tribunal Superior de Justicia de la Comunidad Valenciana (TSJCV). El caso enjuiciado versa sobre el control de temperatura que realizaban los vigilantes de seguridad de una empresa privada contratada en un centro comercial a todos los empleados. La parte demandante, el sindicato representante de los trabajadores, alegó que los vigilantes no estaban cualificados para la realización de esta función, ni era competencia suya llevar a cabo este acto. El TSJCV señaló que la toma de temperatura de los trabajadores, efectivamente, corresponde a los servicios de prevención y salud de la entidad, pero que, debido a la situación excepcional de pandemia, esta cuestión debía abordarse desde esta perspectiva, como medida extraordinaria adoptada por parte de la empresa. Finalmente, los magistrados consideraros que se trataba de una medida necesaria, dada la situación extraordinaria, para poder detectar casos de empleados que sufrieran la enfermedad, pues previene un riesgo laboral específico. Pese a ello, el tribunal sostiene que, a pesar de legitimar a los vigilantes de seguridad para la toma de temperatura de los trabajadores, para poder cumplir con la normativa de protección de datos personales, la información obtenida tenía que ser comunicada y valorada por el personal sanitario habilitado (STSJCV 1018/2020).

Como podemos comprobar, tanto la autoridad de control en materia de protección de datos como este tribunal, siguen el mismo criterio interpretativo en cuanto a la toma de temperatura de los trabajadores, en tanto en cuanto corresponde al empleador establecer un entorno seguro de trabajo y, en este caso, establecer medidas para evitar la propagación del virus.

Caso contrario es la realización de pruebas diagnósticas de la enfermedad como son las Pruebas de Reacción en Cadena de la Polimerasa (PCR), los test de antígenos o los test de anticuerpos. Como bien se señala anteriormente, el empleador tiene el deber de garantizar un entorno seguro y saludable para el desempeño de las labores de sus empleados. En este sentido, las bases jurídicas que podrían fundamentar este tratamiento de datos de salud por parte de la empresa sería por un lado el consentimiento libre del interesado (art. 9.2 a) RGPD) o, por otro lado, que el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable en el ámbito del derecho laboral y de la seguridad y protección social (art. 9.2 b) RGPD).

En cambio, ninguno de los dos preceptos señalados sería de aplicación en el presente caso. Por un lado, el consentimiento no sería válido, pues debe consistir en una manifestación de

voluntad libre, específica e informada del trabajador y el consentimiento prestado por el empleado al empleador en el ámbito laboral no se considera un consentimiento libre, pues se produce un desequilibrio entre ambas partes, tal y como ha apuntado el Comité Europeo de Protección de Datos (Dict. Grupo de Trabajo Art. 29, de 8 de junio de 2017). Por otro lado, no se aplicaría el segundo criterio dado que la empresa no tiene obligación legal de realizar un control de la salud de los trabajadores. La vigilancia de la salud le corresponde a un servicio externo a la empresa tal y como señala el artículo 22.6 de la Ley 31/1995, de 8 de noviembre (art. 22.6 Ley 31/1995). En consecuencia, la opción de realizar las pruebas detectoras de la enfermedad iría más allá de los derechos y obligaciones que tendría la empresa en materia de seguridad y protección social.

2.3.2.3. El tratamiento de datos de salud para el acceso al empleo

En tercer lugar, corresponde analizar el tratamiento de datos personales de salud en el contexto de acceso al empleo.

Tras la pandemia, se han puesto de manifiesto ciertas prácticas relacionadas con la contratación laboral consistentes en requerir a los candidatos a un puesto de trabajo información relativa a si han superado la enfermedad, así como si han desarrollado anticuerpos como requisito previo para acceder a los puestos de trabajo ofertados. En este sentido, la AEPD se ha pronunciado que la práctica de estas actuaciones constituye una clara vulneración de la normativa en materia de protección de datos (AEPD 18 de junio de 2020).

El hecho de comunicar a un empleador la información de haber superado la enfermedad y tener anticuerpos constituye un tratamiento de categorías especiales de datos, el cual requiere que se de algún supuesto de excepción para el tratamiento de datos sensibles contemplado en el art. 9.2 RGPD.

Podemos entender que el consentimiento podría ser un criterio válido para poder tratar los datos de salud del interesado. Sin embargo, como hemos señalado anteriormente, el consentimiento se entenderá que no se ha prestado de manera libre cuando no se dispone de libre elección o no se puede retirar o denegar el consentimiento sin que se sufra algún tipo de perjuicio o en el caso de que existiera un desequilibrio entre las partes (Considerando 42 RGPD). Sobre esta última cuestión se pronunció el Comité Europeo de Protección de Datos el

cual consideró que en el contexto del trabajo se produce un desequilibrio de poder entre empleado y empleador, pues no es probable que la persona candidata al puesto de trabajo pueda negar a la empresa el consentimiento para el tratamiento de datos sin temor o riesgo de que su negativa produzca efectos perjudiciales y, por tanto, surge la posibilidad de que la empresa realice el tratamiento de datos personales de empleados y empleadas actuales o futuros sobre la base del consentimiento, ya que no es probable que éste se otorgue libremente (Directrices 5/2020 Comité Europeo de Protección de Datos, de 4 de mayo 2020).

Por otra parte, analizando las excepciones contenidas en el art. 9.2 RGPD, solicitar este tipo de información al candidato supondría extralimitarse en cuanto a las obligaciones y derechos específicos que la legislación laboral impone al empleador, concretamente el deber de proteger a los trabajadores frente a los riesgos laborales. Por un lado, en tanto en cuanto la persona interesada todavía no es empleada y en consecuencia, la empresa no tiene obligación de velar por la seguridad de los trabajadores. Por otro lado, solicitar información de haber pasado la enfermedad o tener anticuerpos supondría el tener que aplicarlo a cualquier otra enfermedad que implique un riesgo de infección.

2.3.2.4. La obligatoriedad de administrar la vacuna contra el COVID-19

Por último, relacionado con el tratamiento de categorías especiales de datos relacionadas con los empleados corresponde el análisis de la licitud de interponer por parte del empleador, la obligatoriedad de que sus trabajadores reciban la vacuna contra el SARS CoV-2.

En este punto entran en conflicto varios derechos y normativas. En primer lugar, de acuerdo con lo establecido en la CE, los empleadores no podrían exigir la vacunación contra el COVID-19 a sus trabajadores, pues se estaría limitando o coartando sus derechos fundamentales a la integridad física y a la intimidad (artículo 15 y 18 CE respectivamente).

Por otro lado, la normativa sanitaria aplicable a pacientes señala como principio que todo paciente tiene derecho a negarse a la administración de un tratamiento bajo el principio del consentimiento informado (Ley 41/2022).

Ambas normas podrían colisionar con lo dispuesto en la normativa sobre prevención de riesgos laborales, la cual únicamente señala la obligación del empleador de realizar, a través de una entidad externa, la vigilancia de la salud de sus trabajadores, en aras de establecer un

espacio de trabajo saludable, a través de la realización de estudios médicos lo que no implica la obligatoriedad de suministrar tratamientos sanitarios de carácter preventivo como es una vacuna. En consecuencia, lo único que podrían hacer las empresas es recomendar a sus trabajadores la vacunación, pero nunca establecerla como una obligación y mucho menos tomar algún tipo de represalia contra el trabajador, incluido el despido.

De este epígrafe se extrae la conclusión de que la normativa es restrictiva en cuanto al tratamiento de datos personales de los trabajadores, no pudiendo el empleador basar el tratamiento de datos de salud de los mismos en el consentimiento. Con motivo de frenar los contagios por el SARS CoV-2, la normativa sí que establece otros supuestos habilitantes para poder llevar a cabo un tratamiento de los datos de salud de los empleados, como es la existencia de una obligación impuesta por una ley. Así mismo, destaca la importancia de la creación de mecanismos que garanticen la seguridad en cuanto a la captación y el uso de los datos sanitarios de los trabajadores, limitando el conocimiento de este tipo de datos a las entidades encargadas de los servicios de prevención.

Una vez analizados una serie de tratamientos de datos personales en el entorno laboral derivados de la pandemia, se pasa a examinar dos casos concretos acerca del tratamiento de datos personales fuera de este ámbito, cuya legitimación sigue discutiéndose ante los tribunales.

2.3.3. Tratamiento de datos fuera del ámbito laboral con motivo de una pandemia

En este punto se analiza la legitimación para el tratamiento de categorías especiales de datos fuera del ámbito laboral, es decir, en aquellas situaciones cotidianas que impliquen un tratamiento de datos de salud en relación a la prevención y detección del virus SARS CoV-2. Se expondrá la posible vulneración de derechos fundamentales de los ciudadanos, como la libertad de circulación o la protección de datos personales, derivada de la imposición de algunas medidas por parte de las autoridades para intentar frenar la propagación del virus. En particular, se atiende al control de temperatura para acceder al interior de algunos establecimientos y la imposición del certificado COVID-19.

2.3.3.1. El control de temperatura para acceder al interior de instalaciones

Una de las primeras medidas adoptadas con el proceso de desescalada para controlar el acceso a centros de trabajo, comercios, centros educativos u otro tipo de establecimientos fue la toma de temperatura para el acceso a las instalaciones (RDL 8/2021). Este tipo de actuaciones implica un tratamiento de datos personales relativo a la salud de los ciudadanos, lo que conlleva una injerencia elevada en los derechos de las personas afectadas. En este sentido, constituye un tratamiento de datos personales, no solo 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 determinada enfermedad, como es el caso de la infección por COVID-19.

En relación a la toma de temperatura en establecimientos a toda persona ajena a la entidad, como puede ser la toma de temperatura a clientes o proveedores con la finalidad de permitir el acceso a las instalaciones del responsable de tratamiento, la AEPD determina que deben ser las propias autoridades sanitarias quienes tomen la decisión sobre la necesidad y adecuación de esta medida para la prevención de contagios. En definitiva, corresponde a la autoridad sanitaria valorar si la medida es idónea, necesaria o proporcional para la prevención en cuanto a la propagación de la enfermedad (AEPD, 30 de abril de 2020). Como vemos, las autoridades en materia de protección de datos españolas no se pronuncian más allá sobre el tratamiento de los datos es lícito o no, simplemente remiten su articulación a las autoridades sanitarias competentes.

Para autores como J. Raúl Fernández, se requiere un análisis específico sobre los medios utilizados para la toma de temperatura, pues no es lo mismo el empleo de un termómetro, que no registra ni conserva los resultados, que la utilización de un dispositivo que permita registrar los parámetros de temperatura en una base de datos e incluso atribuirlos a una persona. En este último supuesto, el tratamiento de los datos relativos a la salud de las personas puede afectar a sus derechos de privacidad y protección de datos (FERNÁNDEZ 2020).

Así mismo, la AEPD considera que no se puede captar un dato personal de salud de una persona, como es la temperatura y tratarlo espontáneamente por cualquier persona de un lugar público simplemente por el hecho de creer que es lo mejor para sus clientes, sin tener la formación adecuada o los conocimientos necesarios en cuanto a la captación, tratamiento

y posterior conservación de esos datos (AEPD, 30 de abril de 2020). En estos casos se corre el riesgo de discriminar, estigmatizar o difundir de manera pública los datos de salud relativos a una persona, agravando el riesgo de que se produzca una violación de seguridad de la información de carácter sensible entrando en conflicto con la agresión a los derechos de los afectados.

Sobre esta cuestión se pronunció la Conselleria de Igualdad y Políticas inclusivas de la Comunidad Valenciana en una resolución donde autorizaba la toma de temperatura a todo aquel que pretendiera el acceso a las instalaciones de hogares, residencias y servicios de atención a la infancia y adolescencia. En la misma no se prevé qué se hará con esos datos de salud, si se efectuará un registro de los mismos y el plazo de conservación de la información o incluso si se comunicarán a las autoridades sanitarias a efectos de su conocimiento y seguimiento de cualquier sospecha de infección (Resolución 2020/3460). En consecuencia, deja la puerta abierta al tratamiento de datos relativos a la salud de los interesados que accedan a las instalaciones determinadas provocando un vacío normativo en cuanto a los límites del tratamiento de los datos que van a solicitar.

En idéntica línea, las autoridades competentes han autorizado la toma de temperatura en lugares como centros educativos, antes de acceder al interior, como medida de prevención en la detección de la COVID-19. Así mismo, el Ministerio de Sanidad ha publicado una Guía para escuelas y centros educativos frente a casos de COVID-19 en la que aboga por que sean los propios tutores legales de los menores los que tomen la temperatura previamente en el domicilio antes de llevarlos a las aulas (Ministerio de Sanidad, 7 de septiembre de 2021).

El artículo 9 del Real Decreto-ley 21/2020, de 9 de junio, de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por el COVID-19 menciona expresamente el caso de los centros docentes, afirmando que las administraciones educativas son las encargadas de asegurar el cumplimiento por los directores de los centros docentes, públicos o privados, que impartan enseñanzas regladas, de las normas de desinfección, prevención y acondicionamiento de los centros que aquellas establezcan. En el artículo no se hace mención alguna a la toma de temperatura lo que deriva en que, en este supuesto concreto, no existe legitimación suficiente para tomar la temperatura de las personas que accedan al centro (art. 9 RD 21/2020).

2.3.3.2. La imposición del certificado COVID-19

Como último punto a analizar relativo a la incidencia del COVID-19 en los derechos fundamentales de los ciudadanos, se destaca una de las medidas adoptadas por las autoridades sanitarias más polémicas en cuanto a su posible afectación de derechos fundamentales.

Tras el fin del estado de alarma y una vez iniciado el proceso de desescalada, España entró en una etapa de nueva normalidad durante la cual los poderes públicos y autoridades sanitarias continuaron tomando medidas enfocadas a controlar los brotes y frenar los contagios por COVID-19, como la sucesiva aprobación de reales decretos-leyes enfocados a paliar las consecuencias y efectos negativos que en el ámbito socioeconómico supone una pandemia. Entre estas medidas se encuentra la aprobación del Real Decreto-ley 21/2020, de 9 de junio, de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por el COVID-19 (RD 21/2020), el Plan de respuesta temprana en un escenario de control de la pandemia o las diferentes disposiciones y actos adoptados por las autoridades competentes de las Comunidades Autónomas.

En este sentido, la UE reguló la creación de un certificado COVID-19 como instrumento de medida de control de la propagación del virus con la aprobación del Reglamento (UE) 2021/953 del Parlamento Europeo y del Consejo de 14 de junio de 2021 relativo a un marco para la expedición, verificación y aceptación de certificados COVID-19 interoperables de vacunación, de prueba diagnóstica y de recuperación (Certificado COVID-19 digital de la UE) a fin de facilitar la libre circulación durante la pandemia de COVID-19 (R (UE) 2021/953).

En su primer considerando, establece el derecho fundamental de los ciudadanos de la Unión a circular y residir libremente en el territorio de los Estados Miembros, con las limitaciones contempladas en la propia normativa vigente (Considerando 1 R (UE) 21/953). No obstante, debido a la situación mundial de pandemia, el Consejo restringió la libre circulación de los ciudadanos utilizando una serie de criterios y umbrales, salvo necesidades esenciales de trabajo, familia o atenciones médicas.

Así mismo, el considerando 6 de la citada Directiva establece que, los Estados Miembros pueden limitar el derecho fundamental a la libre circulación por motivos de salud pública aplicándose los principios de proporcionalidad y no discriminación. Además, allí se establece

que las medidas adoptadas deberán ser limitadas tanto en su aplicación como en el tiempo de duración con el fin de un restablecimiento de la libre circulación de personas en la UE y la salvaguarda de la salud pública (Considerando 6 R (UE) 2021/953).

El certificado COVID-19 o pasaporte COVID-19, se crea por parte de la UE con la finalidad de facilitar la libre circulación de personas dentro del espacio comunitario. Con ello, en un principio no se pretendía el control o geolocalización de la población. Sin embargo, los usos o finalidades que se le han dado han sido cuestionados tanto por algunos sectores de la población como por algunos organismos o entidades de carácter público. Para autoras como Sara Antúnez o Luisa Cardona, *a priori* el certificado no debería ser incompatible con nuestro derecho a la intimidad o protección de datos personales, no obstante, señalan la posibilidad de que surjan ciertos problemas a la hora de su aplicación. Algunos de ellos pueden ser el uso o finalidad de los datos obtenidos, debiendo cumplir con los principios de eficacia, necesidad y proporcionalidad, teniendo en cuenta la existencia de otras medidas de protección que pudieran resultar menos invasivas. Otro problema que surge es la conservación de los datos obrantes en el certificado a la hora de ser comprobado en cada Estado. Por último, puede surgir el problema de usurpación de identidad o falsificación de certificados (ANTÚNEZ y CARDONA 2021). En definitiva, toda esta problemática debe ser abordada por los Estados antes de la instauración de este tipo de medidas de control para frenar la expansión del virus y contemplar la posibilidad de establecer otro tipo de medidas menos lesivas de derechos fundamentales.

Pues bien, posteriormente a su implantación algunos gobiernos decidieron utilizar el certificado COVID-19 con la finalidad de controlar el acceso a determinados establecimientos, permitiendo el mismo a las personas vacunadas o que hayan obtenido un resultado negativo en una prueba reciente de COVID-19, así como a las personas que se hayan recuperado de la enfermedad en los últimos seis meses desde su contagio.

De entrada, podría cuestionarse este uso, pues se plantea la posibilidad de que se esté produciendo una discriminación a un sector de la población por el simple hecho de no administrarse una vacuna contra la enfermedad, pues la implantación de la vacuna no es obligatoria.

En teoría, la normativa establece que la verificación de los certificados que conforman el certificado COVID-19 digital de la UE no debe dar lugar a nuevas restricciones a la libertad de

circulación dentro de la Unión ni a restricciones de viaje en el interior del espacio Schengen, por lo que se deben aplicar las exenciones a las restricciones de la libre circulación en respuesta a la pandemia de COVID-19 a que se refiere la Recomendación (UE) 2020/1475 y debe tenerse en cuenta la situación específica de las comunidades transfronterizas, que se vieran particularmente afectadas por esas restricciones.

El propio Reglamento hace una referencia a la protección de los datos personales que se deriven del tratamiento efectuado por la utilización del certificado COVID-19. Así en su artículo 10 señala que los datos personales que se contengan en los certificados COVID-19, únicamente deben ser tratados con la finalidad de acceso a la información que incluyen en los mismos y su verificación para facilitar el ejercicio del derecho a la libre circulación dentro de la Unión, estableciendo así mismo que no se producirá ningún tratamiento ulterior o con otros fines (art. 10 R (UE) 2021/953).

Pues bien, existen opiniones en contra de la utilización del pasaporte COVID-19 como medida de control de la propagación del virus, pues una corriente de pensamiento considera una intromisión ilegítima en diversos derechos fundamentales, como son el derecho a la protección de datos personales, libertad de circulación o el derecho de reunión, entre otros y otros lo consideran un argumento lícito y necesario para frenar los contagios.

En este sentido, el autor Guillermo A. Morales, considera que, previa implantación de una medida intromisiva o limitativa de derechos fundamentales, como ha sido el uso del certificado COVID-19, es conveniente analizar, en primer lugar, la habilitación legal de la medida, y, en segundo lugar, realizar un juicio de proporcionalidad (SANCHO 2022).

En cuanto a la primera cuestión, el autor comenta que la exigencia de información sanitaria relativa al COVID-19 supone una restricción de la intimidad personal, tratándose de un dato íntimo perteneciente a la esfera privada de una persona. Así mismo, cualquier limitación impuesta sobre un derecho fundamental requiere una regulación mediante ley orgánica. Por otro lado, señala que el ordenamiento constitucional español no permite adoptar cualquier medida que las autoridades públicas consideren necesaria para hacer frente a una crisis sanitaria, a través del uso de cualquier instrumento jurídico (SANCHO 2022).

En cuanto a la segunda cuestión, para determinar si la medida ha sido proporcional, habría que determinar los derechos fundamentales afectados. En este sentido, la imposición del

certificado COVID-19 ha afectado a los derechos a la igualdad, a la integridad física, a la intimidad, a la protección de datos personales, a la libertad de circulación, así como al derecho de reunión (SANCHO 2022).

Sobre la finalidad de esta medida también se ha pronunciado el TS en su sentencia 1112/2021 –comentada posteriormente en este epígrafe. En la misma, el tribunal señala que la implantación del pasaporte COVID-19 pretende limitar o evitar la transmisión del virus, mediante la simple exhibición del documento para acceder a determinados establecimientos (STS 1112/2021). A pesar de ello, el análisis sobre la proporcionalidad cambiaría si la finalidad del pasaporte COVID-19 pretendiera fomentar la vacunación masiva de la población, castigando a aquellos que decidan no vacunarse, con el fin de descargar de trabajo al sistema sanitario. Esta misma apreciación es compartida por el autor Vicente Álvarez. Éste apunta que la exigencia del certificado es una medida que obliga indirectamente a la vacunación de la población, pues su ausencia impide el acceso de los ciudadanos a diferentes tipos de establecimientos (ÁLVAREZ 2022).

En este sentido, el Tribunal Superior de Justicia de Andalucía (TSJA) se pronunció sobre la afectación de los derechos fundamentales con motivo de la solicitud del certificado COVID-19 para el acceso a locales de ocio nocturno. Los magistrados no dieron el visto bueno a la implantación del certificado para permitir el acceso al interior de los establecimientos, pues afecta a la intimidad de las personas el hecho de tener que facilitar sus datos de salud para que sean tratados por entidades que no ofrecen garantías suficientes sobre el tratamiento de los mismos y su posible conservación (STSJA 1543/2021).

En España, fueron las diferentes comunidades autónomas, con apoyo del Sistema Nacional de Salud, las encargadas de emitir los certificados COVID-19, las cuales deciden sobre su implantación para el acceso a determinados establecimientos (LA MONCLOA 2021).

Llegados a este punto, son destacables dos sentencias del Tribunal Supremo (TS) relativas a la implantación del certificado COVID-19 para acceder al interior de una serie de establecimientos en las Comunidades Autónomas de Andalucía y Galicia.

La primera de ellas, fue la Sentencia del Tribunal Supremo 3260/2021, de 18 de agosto (STS 3260/2021), resolviendo un recurso de casación interpuesto por la Junta de Andalucía contra un Auto de la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia de

Andalucía en el cual se denegaba la ratificación del uso el certificado COVID-19 para acceder al interior de establecimientos de ocio con música. El Tribunal Supremo desestimó el recurso de casación denegando la ratificación de la medida de solicita del pasaporte COVID-19 para acceder a los establecimientos de ocio nocturno, estableciendo que la exigencia del certificado COVID-19 no se trata de una limitación puntual que afecte a un número determinado de personas, sino que se trata de una medida restrictiva del derecho fundamental a la intimidad personal incidiendo en el principio de no discriminación. Así mismo establece que la medida no supera el juicio de proporcionalidad por considerar la falta de justificación de la misma, no estableciendo una medida menos lesiva para los derechos fundamentales (STS 3260/2021).

Por otro lado, señala que no se encuentra justificación en cuanto a solicitar el certificado únicamente en locales de ocio con música, no exigiéndolo en locales de prestaciones similares o que conlleven la misma problemática en cuanto a la propagación del virus. Por último, considera que la medida se impone a todo el territorio de la comunidad autónoma, con independencia de la tasa de incidencia de cada municipio. En definitiva, el Supremo no observó justificación suficiente para ratificar la decisión de implantar el certificado COVID-19 pues las alegaciones expuestas por la Junta de Andalucía para su aprobación no las consideraron válidas o suficientes como justificación para la adopción de la medida (STS 3260/2021).

La segunda, es la Sentencia del Tribunal Supremo 1112/2021, de 14 de septiembre, en la cual se pretende la impugnación del Auto de 20 de agosto de 2021, dictado por la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia de Galicia (TJS Galicia) en el que se acordó denegar la presentación del certificado COVID-19 en ciertos establecimientos. En la sentencia se analiza el supuesto de exhibición del pasaporte COVID-19 para el acceso a establecimientos de ocio nocturno en la Comunidad de Galicia. En ella se considera la necesidad de solicitar la autorización judicial previa para instaurar la medida, pues afecta a derechos fundamentales como la igualdad, intimidad y protección de datos personales.

El motivo principal del recurso de casación contra la sentencia dictada por el TSJ de Galicia es la determinación de la afectación a los derechos fundamentales de la medida administrativa, pues para su implementación se requiere autorización judicial previa. El Tribunal entiende que sí afecta (por muy leve que sea afección) a los derechos fundamentales de igualdad, pues ciertos ciudadanos se van a ver privados del acceso a los establecimientos por no disponer o

no querer mostrar el documento; al derecho a la intimidad, pues la exhibición del documento revela datos de carácter íntimo y al derecho a la protección de datos, dado que se tratan datos de salud considerados sensibles y que requieren una protección más amplia (STS 1112/2021).

Por otro lado, el Tribunal Constitucional afirma que los derechos fundamentales no son absolutos ni ilimitados (STC 11/1981), por lo que se requiere una ponderación de los mismos en un juicio de proporcionalidad para cada caso concreto. Pues bien, el TSJ de Galicia justifica la proporcionalidad en la voluntariedad de entrada a los locales de ocio, donde no se realizan actividades consideradas esenciales, esto es, señala que las personas pueden disfrutar su ocio de maneras muy diversas, acudiendo a los locales o no, entrando al interior o quedándose en la terraza (STS 1112/2021).

Analizando las palabras del Tribunal Supremo, parece un argumento destacable pues, en otro contexto de actividad esencial o no voluntariedad (como por ejemplo acudir al puesto de trabajo), el juicio de proporcionalidad en las circunstancias del supuesto concreto podría ser totalmente contrario.

En definitiva, en el juicio de proporcionalidad en cuanto a la afectación de los derechos fundamentales afectados, el TS establece la prevalencia de la vida y protección de la salud frente a los derechos de igualdad, intimidad y protección de datos personales, por lo que estima el recurso de casación y da luz verde a la exigencia del pasaporte COVID-19 para acceder a los establecimientos de hostelería y restauración, juego y ocio nocturno.

Cabe destacar el voto particular efectuado por el magistrado del Tribunal Antonio Jesús Fonseca-Herrero, partidario de desestimar el recurso del Gobierno Vasco en el que argumenta que la Administración vasca no justifica suficientemente las razones por las que considera que se debe exhibir el certificado COVID-19 como única medida para controlar la expansión del virus, no siendo proporcionada a la situación descrita para justificar la lesión e intromisión en los derechos fundamentales aducidos.

Como corolario de este último apartado, en cuanto al tratamiento de datos personales de los ciudadanos efectuado por la pandemia del coronavirus, se puede apreciar la preocupación social que han generado las medidas impuestas por el gobierno.

Destaca la diferente interpretación de algunos tribunales españoles en cuanto a la licitud de medidas como la obligatoriedad de exhibir el certificado COVID-19 para poder acceder al

interior de algunos establecimientos, llegando a elevar esta cuestión hasta el Tribunal Supremo.

3. Conclusiones

Uno. - La protección de los datos personales es una materia relativamente nueva en la mayoría de ordenamientos jurídicos. Ello supone que existe una escasa regulación por parte de los legisladores de los distintos Estados, así como por parte de las autoridades de control competentes, motivo por el cual, actualmente no contemplan todos los supuestos de tratamiento que van surgiendo en la sociedad, así como lo son los escasos pronunciamientos por nuestros jueces, tribunales y autoridades de control.

Dos. - La constante globalización y el desarrollo de nuevas tecnologías implica la posibilidad de que terceros pudieran tener acceso a nuestros datos personales, con o sin nuestro consentimiento. Es por ello que se torna necesaria la creación de medidas para preservar el derecho fundamental a la protección de datos personales. En el caso de la UE, estas medidas deberían ser consensuadas por parte de todos sus Estados Miembros de la UE, con el ánimo de armonizar las legislaciones en materia de protección de datos en todo el ámbito de aplicación de las mismas.

Tres. - La normativa vigente europea en materia de protección de datos personales, cuando establece las bases jurídicas para que el tratamiento de los datos personales sea lícito, lo hace a través de una serie de supuestos taxativos que, en principio, no admiten la inclusión de otros supuestos nuevos. El problema surge cuando se plantea un supuesto de tratamiento novedoso, donde serán las autoridades competentes de cada Estado Miembro las encargadas de legislar sobre esa materia. Ello supondrá que se den soluciones diferentes en los distintos Estados que conforman el ámbito de aplicación de la normativa europea en materia de protección de datos, o al menos, diferentes interpretaciones. Este escenario podría enturbiar el deseo europeo de contar con una normativa común en materia de protección de datos personales que siente unas bases generales de regulación.

Cuatro. - El RGPD dispone que, en el ámbito de la situación derivada de la expansión del COVID-19, en situaciones excepcionales como una pandemia, el criterio legitimador para el tratamiento de los datos personales puede ser de carácter múltiple, sustentándose tanto en el interés público como en el interés vital del afectado. Sin embargo, para el tratamiento de datos de salud, la regla general es la prohibición, sin ningún tipo de excepción, del tratamiento salvo que exista una circunstancia que levante esa prohibición general para el tratamiento de

categorías especiales de datos (donde se encuentran los datos de salud) como la necesidad del tratamiento para proteger intereses vitales de los interesados.

La base jurídica, por lo tanto, en la mayoría de los escenarios analizados, no podía ser el consentimiento del interesado, pues no cumple los requisitos recogidos en la normativa vigente en materia de protección de datos, es decir, el tratamiento debe basarse en un consentimiento libre e informado. A este respecto, no sería libre si se derivase del mismo alguna consecuencia negativa, como pudiera ser en los supuestos analizados en el presente trabajo, es decir, si no presento el certificado COVID-19 para entrar a un determinado establecimiento, me negarán la entrada.

Cinco. - Se observa una falta de organización común a la hora de afrontar la disposición de medidas para evitar la propagación del virus, pues no ha habido un criterio común y unificado para todas las Comunidades Autónomas, lo que supone una afectación a la igualdad de los ciudadanos.

Seis. - Por último, en lo que respecta a la exigencia del pasaporte COVID-19, ha implicado un alto nivel de afectación a los derechos fundamentales de protección de datos, intimidad y libertad de circulación de las personas, pues se ha accedido a información personal de carácter sensible de la población, como son los datos de salud. Así mismo, la exhibición del pasaporte COVID-19 a través de un código QR, que se puede escanear con cualquier *smartphone*, no comportaba seguridad ninguna acerca de qué se hace con nuestros datos, si se han conservado o si terceros no autorizados han podido acceder a ellos.

En base a lo anterior, se puede considerar que la implantación del certificado COVID-19 ha sido un instrumento de los Estados tendente al control de la población, de sus movimientos y de sus datos de salud, no encontrando justificación alguna de su uso. Se trata de una medida que, teóricamente, era opcional, como lo era la administración de la vacuna, lo que implica que si un individuo no contaba con una serie de dosis administradas, no podía circular libremente, afectando a su derecho fundamental a la libre circulación, así como al tratamiento de sus datos personales. Es más, la administración de la pauta completa de vacunación que se ha requerido para la expedición del certificado, no ha eximido a la población de poder volver a infectarse del virus.

La exhibición del certificado y su comprobación a través de dispositivos electrónicos no ha garantizado en ningún momento la seguridad de la información, pues no sabemos si al comprobar el código QR, nuestros datos se han estado guardando o enviando a personal no autorizado. En definitiva, el tratamiento de datos personales de salud no debería realizarse de manera genérica y sin ofrecer garantías de seguridad.

4. Referencias bibliográficas

Bibliografía básica

ÁLVAREZ GARCÍA, V. «La evolución de la jurisprudencia del Tribunal Supremo sobre el pasaporte covid en un país carente de una legislación antipandemias». *Diario del Derecho, Iustel*. 5 enero 2022. [Última consulta 15 mayo 2023]. Disponible en: https://www.iustel.com/diario_del_derecho/noticia.asp?ref_iustel=1218492

ALZÍBAR CUELLO, J.M. «La pandemia de la COVID-19 como debate público: el caso español». *Anuario Electrónico de Estudios en Comunicación Social "Disertaciones".* 2021. vol. 14, núm. 2. [Última consulta 15 mayo 2023]. ISSN 1856-9536. Disponible en: https://revistas.urosario.edu.co/index.php/disertaciones/article/view/10334

ANTÚNEZ, S.G. y CARDONA, L. «Certificado COVID e intimidad ¿Compatible?». El Derecho. 2021. [Última consulta 15 mayo 2023]. Disponible en: https://elderecho.com/certificado-covid-e-intimidad-compatible

BERROCAL LANZAROT, A.I. *Estudio jurídico-crítico sobre la ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales*. 1ª ed. Madrid: Reus S.A., 2019.

«Ciberseguridad en el teletrabajo. Una guía de aproximación para el empresario». *INCIBE.* 2020. [Última consulta 15 mayo 2023]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberseguridad_en_el_teletrabajo.pdf

«Comunicado de la AEPD en relación con la toma de temperatura por parte de comercios, centros de trabajo y otros establecimientos». *Agencia Española de Protección de Datos*. 30 abril 2020. [Última consulta 15 mayo 2023]. Disponible en: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-aepd-temperatura-establecimientos

«Comunicado de la AEPD sobre la información acerca de tener anticuerpos de la COVID-19 para la oferta y búsqueda de empleo». *Agencia Española de Protección de Datos*. 18 junio 2020. [Última consulta 15 mayo 2023]. Disponible en: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-AEPD-covid-19-oferta-busqueda-empleo

«Coronavirus: Garante de privacidad, no a las iniciativas de "hágalo usted mismo" en la recopilación de datos. los sujetos públicos y privados deberán cumplir con las indicaciones del Ministerio de Salud y las instrucciones competentes». *Garante Privacy*. 2 marzo 2020. [Última consulta 15 mayo 2023]. Disponible en: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9282117#1

CORRAL TALCIANI, H. F., «Configuración jurídica del derecho a la privacidad, I: origen, desarrollo y fundamentos». *Revista chilena de derecho*. 2000, vol.27, núm. 1, pp. 51-79. [Última consulta 15 mayo 2023]. ISSN 0716-0747. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=2650211

«Covid-19: Las medidas de emergencia no deben servir de pretexto para abusos y vulneraciones de derechos humanos, dice Bachelet». *Oficina del Alto Comisionado de las Naciones unidas para los Derechos Humanos*. 27 abril 2020. [Última consulta 15 mayo 2023]. Disponible en: https://www.ohchr.org/es/2020/04/covid-19-exceptional-measures-should-not-be-cover-human-rights-abuses-and-violations

«COVID-19: preguntas y respuestas sobre la recogida de datos personales en el lugar de trabajo». *CNIL*. 14 febrero 2022. [Última consulta 15 mayo 2023]. Disponible en: https://www.cnil.fr/fr/covid-19-questions-reponses-sur-la-collecte-de-donnees-personnelles-sur-le-lieu-de-travail

«Cronología de la respuesta de la OMS a la COVID-19». *Organización Mundial de la Salud*. 29 enero 2021. [Última consulta 15 mayo 2023]. Disponible en: https://www.who.int/es/news/item/29-06-2020-covidtimeline

CUBERO MARCOS, J.I., y ABERASTURI GORRIÑO, U., «Protección de datos personales en las comunicaciones electrónicas: especial referencia a la Ley 25/2007, sobre conservación de datos». *REDC (Revista Española de Derecho Constitucional)*. 2008, núm. 28, núm. 83, pp. 175-197. [Última consulta 15 mayo 2023]. ISSN 0211-5743. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=2702916

«El Gobierno declarará mañana el estado de alarma por el coronavirus». *La Moncloa*. 13 marzo 2020. [Última consulta 15 mayo 2023]. Disponible en:

https://www.lamoncloa.gob.es/presidente/actividades/Paginas/2020/130320-sanchez-declaracio.aspx

«España comienza a emitir el Certificado COVID digital adelantándose 20 días al momento en el que será obligatorio». *La Moncloa*. 7 junio 2021. [Última consulta 15 mayo 2023]. Disponible en: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/sanidad14/Paginas/2021/070621-certificado-covid.aspx#:~:text=As%C3%AD%2C%20se%20adelanta%20m%C3%A1s%20de,la%20obligaci%C3%B3n%20de%20los%20Estados

FERNÁNDEZ QUINTANILLA, J. R. «Toma de temperatura, desescalada y lucha contra el COVID-19». Jraulfernandez. 11 junio 2020. [Última consulta 15 mayo 2023]. Disponible en: https://www.jraulfernandez.es/toma-de-temperatura-desescalada-y-lucha-contra-el-covid-19/

FERNÁNDEZ VILLAZÓN, L. A. «El nuevo Reglamento Europeo de Protección de Datos». FORO. Revista de Ciencias Jurídicas y Sociales, Nueva Época. 2016, vol.19, núm.1, pp. 395-411. [Última consulta 15 mayo 2023]. ISSN: 1698-5583. Disponible en: https://revistas.ucm.es/index.php/FORO/article/view/53399/48985

GARCÍA MAHAMUT, R. «El derecho fundamental a la protección de datos: El Reglamento (UE) 2016/679 como elemento definidor del contenido esencial del artículo 18.4 de la Constitución». *Anuario de derecho parlamentario de las Cortes Valencianas*. 2018, núm. Extra 31, pp. 59-80. [Última consulta 15 mayo 2023]. ISSN: 1136-3339. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6762711

«Guía de actuación ante la aparición de casos de COVID-19 en centros educativos». Ministerio de Sanidad. 7 septiembre 2021. [Última consulta 15 mayo 2023]. Disponible en: https://www.sanidad.gob.es/profesionales/saludPublica/ccayes/alertasActual/nCov/documentos/Guia_actuacion_centros_educativos.pdf

GIAKOUMOPOULOS, C., BUTTARELLI, G. Y O'FLAHERTY, M. *Manual de legislación europea en materia de protección de datos.* Edición de 2018. Luxemburgo: *Oficina de Publicaciones de la Unión Europea*, 2019. [Última consulta 15 mayo 2023]. Disponible en:

https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_es.pdf

HEREDERO HUIGUERAS, M. «La protección de los datos de carácter personal registrados en soporte informatizado con fines estadísticos en el derecho español». *Revista Iberoamericana de derecho informático*. 1994, núm. 4, pp.299-312. [Última consulta 15 mayo 2023]. ISSN 299-312. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=250530

HERNÁNDEZ, A. «La historia oculta de IBM: vendió 700.000 tarjetas a Franco para ganar la Guerra Civil». *El confidencial*. 2018. [Última consulta 15 mayo 2023]. Disponible en: https://www.elconfidencial.com/tecnologia/2018-04-21/otra-historia-de-ibm-tarjetas-franquismo-guerra-civil_1552819/

«Informe N/REF 0017/2020 del Gabinete Jurídico de la Agencia Española de Protección de Datos». *Agencia Española de Protección de Datos*. 2020. [Última consulta 15 mayo 2023]. Disponible en: https://www.aepd.es/es/documento/2020-0017.pdf

«Informe teletrabajo en España». *Randstad Research*. 2021. [Última consulta 15 mayo 2023]. Disponible en: https://www-randstadresearch-es.s3.amazonaws.com/wp-content/uploads/2021/07/RANDSTAD-Informe-Research-Teletrabajo.pdf

LOMBARTE, A. R. « De la «libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018)». *Revista de Derecho Político*. 2017, núm. 100, pp. 639-669. [Última consulta 15 mayo 2023]. ISSN 0211979X. Disponible en: https://www.proquest.com/docview/2076931332/fulltextPDF/CBFA31818C45BDPQ/1?accountid=142712

LOMBARTE, A. R. «El nuevo derecho de protección de datos». *Revista Española de Derecho Constitucional.* 2019, núm. 116, pp. 45-74. [Última consulta 15 mayo 2023]. Disponible en: https://recyt.fecyt.es/index.php/REDCons/article/view/73736

MARZO PORTERA, A. «La inoportuna doctrina de las autoridades europeas de protección de datos frente al COVID-19». *Hay Derecho*. 17 marzo 2020. [Última consulta 15 mayo 2023]. Disponible en: https://www.hayderecho.com/portfolio-item/la-inoportuna-doctrina-de-las-autoridades-europeas-de-proteccion-de-datos-frente-al-covid-19/

NISA ÁVILA, J. A., «Origen jurídico histórico de la protección de datos: evolución de las diferentes teorías jurídicas que la han protegido». *El derecho*. 8 octubre 2020. [Última consulta

15 mayo 2023]. Disponible en: https://elderecho.com/origen-juridico-historico-la-proteccion-datos-evolucion-las-diferentes-teorias-juridicas-la-protegido

NOGUEIRA LÓPEZ, A. «Confinar el coronavirus. Entre el viejo Derecho sectorial y el Derecho de excepción». *El Cronista del Estado Social y Democrático de Derecho*. 2020. Núm. 86-87, pp. 22-31. [Última consulta 15 mayo 2023]. Disponible en: http://www.elcronista.es/El-Cronista-n%C3%BAmero-86-87-Coronavirus.pdf

PARDO, C. V. «Herramientas jurídicas frente a situaciones de emergencia sanitaria ¿Hasta dónde se pueden limitar derechos sin recurrir a la excepcionalidad constitucional?». *Teoría y Realidad Constitucional.* 2021. Núm. 48, pp. 265-296. [Última consulta 15 mayo 2023]. ISSN 11395583. Disponible en: https://www.proquest.com/docview/2607336627?parentSessionId=%2Fi1hYs65pjbNN24CLSEbW8ab8x7AE6sdjMz37VZykkI%3D&pq-origsite=summon&accountid=142712

PIÑAR MAÑAS, J.L. «La protección de datos durante la crisis del coronavirus». *Consejo General de la Abogacía Española*. 20 marzo 2020. [Última consulta 15 mayo 2023]. Disponible en: https://www.abogacia.es/actualidad/opinion-y-analisis/la-proteccion-de-datos-durante-la-crisis-del-coronavirus/

«Protección de datos en la UE». *Consejo Europeo. Consejo de Europa*. 1 septiembre 2022. [Última consulta 15 mayo 2023]. Disponible en: https://www.consilium.europa.eu/es/policies/data-protection/

«¿Por fin un RGPD en Estados Unidos?». *Hosteltur*. 15 septiembre 2022. [Última consulta 15 mayo 2023]. Disponible en: https://www.hosteltur.com/comunidad/005159_por-fin-un-rgpd-en-estados-unidos.html

POLO ROCA, A. «El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado». *Revista de Derecho Político*. 2020, núm. 108, pp. 165-193. [Última consulta 15 mayo 2023]. Disponible en: https://revistas.uned.es/index.php/derechopolitico/article/view/27998/21775

«Preguntas y respuestas sobre el nuevo coronavirus (COVID-19)». *Ministerio de sanidad*. 12 marzo 2021. [Última consulta 15 mayo 2023]. Disponible en: https://www.sanidad.gob.es/profesionales/saludPublica/ccayes/alertasActual/nCov/documentos/Preguntas_respuestas_2019-nCoV2.pdf

«Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo». *Agencia Española de Protección de Datos*. 2020. [Última consulta 15 mayo 2023]. Disponible en: https://www.aepd.es/es/documento/nota-tecnica-proteger-datos-teletrabajo.pdf

REQUEJO PAGÉS, J. L. «La protección de datos, en la encrucijada entre el Derecho de la Unión y la Constitución Española», 21-38. En CASAS BAAMONDE, M. E. (coord.). *El derecho a la protección de datos personales en la sociedad digital.* 1ª ed. Madrid: Editorial Centro de Estudios Ramón Areces S. A., 2020. [Última consulta 15 mayo 2023]. Disponible en: https://www.fundacionareces.es/recursos/doc/portal/2018/03/20/el-derecho-a-la-proteccion-de-datos-personales.pdf

RODRIGUEZ AYUSO, J.F. «Estado de alarma y protección de la privacidad en tiempos de pandemia: licitud del tratamiento de categorías especiales de datos». *Revista de Derecho Político*. 2021, núm. 110, pp. 299-318. [Última consulta 15 mayo 2023]. Disponible en: https://revistas.uned.es/index.php/derechopolitico/article/view/30337.

SANCHO, G. A. M. «Pasaporte COVID a examen. Nudging y derechos fundamentales». *Revista de Derecho Político.* 2022, núm. 115, pp. 171-204. ISSN 0211979X. Disponible en: https://www.proquest.com/docview/2760071596?parentSessionId=5Xx0pgJUVZzXMOKIqqtwQndkMeo%2F6w1W62UYbodXY4o%3D&pq-origsite=summon&accountid=142712

SERRANO PÉREZ, M.M., «El derecho fundamental a la Protección de Datos. Su contenido esencial». *Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas*. 2005, núm. 1, pp. 245-265. [Última consulta 15 mayo 2023]. ISSN 1699-7026. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=1396395

«Teletrabajo y protección de datos en el ámbito digital». *Agencia Española de Protección de Datos*. 19 julio 2021. [Última consulta 15 mayo 2023]. Disponible en: https://www.aepd.es/es/prensa-y-comunicacion/blog/teletrabajo-y-pd-en-el-ambito-digital

WARREN, S. D., y BRANDEIS, L. D. «The Right to Privacy». *Harvard Law Review*. 1890, vol. IX, núm. 5, pp. 193 y sigs. [Última consulta 15 mayo 2023]. Disponible en http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

Legislación citada

Carta de los Derechos Fundamentales de la Unión Europea. *Diario Oficial de las Comunidades Europeas,* 11 de diciembre de 2000. [Última consulta 15 mayo 2023]. Disponible en: https://www.europarl.europa.eu/charter/pdf/text_es.pdf

Constitución Española. *Boletín Oficial del Estado*, 29 de diciembre de 1978, núm. 311, pp. 29313 a 29424. [Última consulta 15 mayo 2023]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229

Convenio (núm. 108) relativo a la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, adoptado en Estrasburgo el 28 de enero de 1981. *Boletín Oficial del Estado,* núm. 274, de 15 de noviembre, pp. 36000-36004. [Última consulta 15 mayo 2023]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447

Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950. Ratificado por España el 26 de septiembre de 1979. *Boletín Oficial del Estado* núm. 243/1979, de 10 de octubre, pp.23564-23570. [Última consulta 15 mayo 2023]. Disponible en: https://www.boe.es/boe/dias/1979/10/10/pdfs/A23564-23570.pdf

Declaración Universal de los Derechos Humanos. Adoptada y proclamada por la Asamblea General de la ONU en su resolución 217 A (III), de 10 de diciembre de 1948. [Última consulta 15 mayo 2023]. Disponible en: https://www.un.org/es/about-us/universal-declaration-of-human-rights

Dictamen 2/2017 del Grupo de Trabajo del Artículo 29, de 8 de junio de 2017, sobre el tratamiento de datos en el ámbito laboral (17/ES). [Última consulta 15 mayo 2023]. Disponible en: https://adenda.net/wp-content/uploads/2021/05/2.WP249_2017_RELACIONES-LABORALES_Opinion22017ondataprocessingatwork-wp249_es.pdf

Dictamen 4/2007 del Grupo de Trabajo del Artículo 29, de 20 de junio de 2007, sobre el concepto de datos personales (01248/07/ES). [Última consulta 15 mayo 2023]. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

Dictamen 15/2011 del Grupo de Trabajo del Artículo 29, de 13 de julio de 2011, sobre la definición del consentimiento (01197/11/ES). [Última consulta 15 mayo 2023]. Disponible en:

https://www.incliva.es/wp-content/uploads/2021/02/Dictamen-15.2011-sobre-la-definicion-del-consentimiento-Grupo-de-Trabajo....pdf

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. *Boletín Oficial del Estado*, núm. 281, de 23 de noviembre, pp. 31-50. [Última consulta 15 mayo 2023]. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678

Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, adoptadas el 4 de mayo de 2020. Versión 1.1. *Comité Europeo de Protección de Datos*. [Última consulta 15 mayo 2023]. Disponible en: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_es.pdf

Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales. *Boletín Oficial del Estado*, 10 de noviembre de 1995, núm. 269, pp. 32590-32611. [Última consulta 15 mayo 2023]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1995-24292

Ley 41/2022, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. Boletín Oficial del Estado, 15 de noviembre de 2002, núm. 274, pp. 40126-40132. [Última consulta 15 mayo 2023]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2002-22188

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *Boletín Oficial del Estado*, 14 de diciembre de 1999, núm. 298, pp. 43088-43099. [Última consulta 15 mayo 2023]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado*, 6 de diciembre de 2018, núm. 294, pp. 119788-119857. [Última consulta 15 mayo 2023]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19. *Boletín Oficial del*

Estado, 14 de marzo de 2020, núm. 67. [Última consulta 15 mayo 2023]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2020-3692

Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Lay del Estatuto de los Trabajadores. *Boletín Oficial del Estado*, 24 de octubre de 2015, núm. 255. [Última consulta 15 mayo 2023]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2015-11430

Real Decreto-ley 8/2021, de 4 de mayo, por el que se adoptan medidas urgentes en el orden sanitario, social y jurisdiccional, a aplicar tras la finalización de la vigencia del estado de alarma declarado por el Real Decreto 926/2020, de 35 de octubre, por el que se declara el estado de alarma para contener la propagación de infecciones causadas por el SARS CoV-2. Boletín Oficial del Estado, 5 de mayo de 2021, núm. 107. [Última consulta 15 mayo 2023]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2021-7351

Real Decreto-ley 21/2020, de 9 de junio, de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por el COVID-19. *Boletín Oficial del Estado*, 10 de junio de 2020, núm. 163. [Última consulta 15 mayo 2023]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2020-5895

Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia. Boletín Oficial del Estado, 23 de septiembre de 2020, núm. 253. [Última consulta 15 mayo 2023]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2020-11043

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. *Diario Oficial de las Comunidades Europeas*, 4 de mayo de 2016, núm. 119. [Última consulta 15 mayo 2023]. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

Reglamento (UE) 2021/953 del Parlamento Europeo y del Consejo de 14 de junio de 2021 relativo a un marco para la expedición, verificación y aceptación de certificados COVID-19 interoperables de vacunación, de prueba diagnóstica y de recuperación (certificado COVID digital de la UE) a fin de facilitar la libre circulación durante la pandemia de COVID-19. *Diario Oficial de las Comunidades Europeas,* 15 de junio de 2021, núm. 211. [Última consulta 15 mayo

2023]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32021R0953

Resolución 2020/3460, de 14 de mayo de 2020, de la Vicepresidencia y Conselleria de Igualdad y Políticas Inclusivas, por la que se establece el plan de transición a la nueva normalidad, en el contexto de crisis sanitaria ocasionada por la COVID-19, de los hogares, residencias y servicios de atención a la infancia y adolescencia comprendidos en su ámbito de competencias. *Boletín Oficial de la Generalitat Valenciana*, núm. 8812, de 15 de mayo. [Última consulta 15 mayo 2023]. Disponible en: https://dogv.gva.es/datos/2020/05/15/pdf/2020_3460.pdf

Tratado de Funcionamiento de la Unión Europea, firmado en Roma en 1957. *Diario oficial de las Comunidades Europeas*, 26 de octubre de 2012, núm. 326, pp. 1-390. [Última consulta 15 mayo 2023]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex%3A12012E%2FTXT

Jurisprudencia referenciada

Affaire Halford c. Royaume-Uni, 25/06/1997, Recueil 1997-III. TEDH. [Última consulta 15 mayo 2023]. Disponible en: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-62600%22]}

Sentencia Tribunal Constitucional 11/1981, de 8 de abril de 1981. *Boletín Oficial del Estado*, núm. 99, de 25 de abril de 1981. ECLI:ES:TC:1981:11. [Última consulta 15 mayo 2023]. Disponible en: https://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/11

Sentencia Tribunal Constitucional 144/1999, de 22 de julio de 1999. *Boletín Oficial del Estado*, núm. 204, 22 de agosto 1999. ECLI:ES:TC:1999:144. [Última consulta 15 mayo 2023]. Disponible en: https://hj.tribunalconstitucional.es/es/Resolucion/Show/3886

Sentencia Tribunal Constitucional 254/1993, de 20 de julio de 1993. *Boletín Oficial del Estado*, núm. 197, 18 de agosto 1993. ECLI:ES:TC:1993:254. [Última consulta 15 mayo 2023]. Disponible en: http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/2383

Sentencia Tribunal Constitucional 292/2000, de 30 de noviembre. *Boletín Oficial del Estado*, núm. 4, 4 de enero de 2001. ECLI:ES:TC:2000:292. [Última consulta 15 mayo 2023]. Disponible en: https://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4276

Sentencia del Tribunal Superior de Justicia de Andalucía 1543/2021, de 6 de agosto. N.I.G.:1808733320211001618. [Última consulta 15 mayo 2023]. Disponible en: file:///C:/Users/USER/Downloads/20210806%20El%20TSJA%20deniega%20la%20ratificaci%C3%B3n%20judicial%20del%20pasaporte%20covid.pdf

Sentencia del Tribunal Superior de Justicia de la Comunidad Valenciana 1018/2020, de 22 de junio de 2020. *Centro de Documentación Judicial*. ECLI:ES:TSJCV:2020:1018. [Última consulta 15 mayo 2023]. Disponible en: https://www.poderjudicial.es/search/AN/openDocument/1b029547188eea9d/20200702

Sentencia Tribunal Supremo 1112/2021, de 14 de septiembre. ECLI:ES:TS:2021:3298. [Última consulta 15 mayo 2023]. Disponible en: https://www.poderjudicial.es/search/TS/openDocument/308a9176fc4b9502/20210920

Sentencia Tribunal Supremo 3260/2021, de 18 de agosto de 2021. ECLI:ES:TS:2021:3260. [Última consulta 15 mayo 2023]. Disponible en: https://www.poderjudicial.es/search/AN/openCDocument/47c54a4d73e1a196eb9f320e282b0b42094a1ef10f1fb978

Sentencia Tribunal Supremo 5073/2004, de 12 de julio de 2004. ECLI:ES:TS:2004:5073. [Última consulta 15 mayo 2023]. Disponible en: https://www.poderjudicial.es/search/indexAN.jsp

Theres c. Roumanie, n.º 49933/20, TEDH. [Última consulta 15 mayo 2023]. Disponible en: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22TERHE%C5%9E%22],%22itemid%22:[%22001-210026%22]}

Thevenon c. France (dec.), n.º 46061/22, TEDH. [Última consulta 15 mayo 2023]. Disponible en: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22\%22THEVENON%20c.%20FRANCE\%22%22],%22itemid%22:[%22002-13813%22]}

Zambrano c. France, n.º 41994/21, TEDH. [Última consulta 15 mayo 2023]. Disponible en: https://ojs.uc.cl/index.php/bjur/article/view/43465/35197

Listado de abreviaturas

AEPD	Agencia de Protección de Datos
Art.	Artículo
CDFUE	Carta de derechos Fundamentales de la Unión Europea
CE	Constitución Española
CEDH	Convenio Europeo de Derechos Humanos
CNIL	Commission Nationale Informatique & Libestés
DUDH	Declaración Universal de los Derechos Humanos
EEE	Espacio Económico Europeo
GT Art.29	Grupo de Trabajo del Artículo 29
IBM	International Business Machines
INCIBE	Instituto Nacional de Ciberseguridad
LOMESP	Ley de Medidas Especiales en Materia de Salud Pública
LOPD	Ley Orgánica de Protección de Datos
LOPDGDD	Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales
LPRL	Ley de Prevención de Riesgos Laborales
OMS	Organización Mundial de la Salud
RD	Real Decreto
RD Leg.	Real Decreto Legislativo
RDL	Real Decreto Ley
RGPD	Reglamento General de Protección de Datos
PCR	Pruebas de Reacción en Cadena de la Polimerasa
STC	Sentencia del Tribunal Constitucional
STSJCV	Sentencia del Tribunal Superior de Justicia de la Comunidad Valenciana
STSJA	Sentencia del Tribunal Superior de Justicia de Andalucía
TEDH	Tribunal Europeo de Derechos Humanos
TFUE	Tratado de Funcionamiento de la Unión Europea
TS	Tribunal Supremo
TSJ	Tribunal Superior de Justicia
TSJA	Tribunal Superior de Justicia de Andalucía
UE	Unión Europea