Universidad Internacional de La Rioja
Facultad de Derecho

Máster Universitario en Propiedad Intelectual
y Derecho de las Nuevas Tecnologías

La resiliencia de la normativa reguladora de la protección de datos en el contexto de pandemia causada por la COVID-19.

Trabajo fin de estudio presentado por:	María Victoria Moreno Muñoz
Tipo de trabajo:	TFM de investigación
Director/a:	Susana Checa Prieto
Fecha:	14 de julio de 2021

Resumen

La declaración de pandemia ocasionada por la COVID-19 a nivel mundial trajo consigo numerosas medidas restrictivas de derechos fundamentales y la necesidad de adaptarse a las nuevas tecnologías. Para combatir la transmisión de la enfermedad se han utilizado medios tradicionales y nuevas soluciones tecnológicas que han avivado el debate sobre la injerencia en el derecho de la protección de datos y su compatibilidad con otros derechos fundamentales. Estas soluciones tecnológicas han sido acogidas con distintos resultados, en parte por el desconocimiento de las posibilidades y garantías que ofrece la normativa reguladora vigente, así como la falta de confianza en sus principios. Actualmente, las autoridades europeas están realizando grandes esfuerzos de divulgación sobre los beneficios de la última solución tecnológica ideada para frenar los contagios de la COVID-19, el Certificado COVID Digital de la UE, con el fin de que sea empleado por el mayor número posible de ciudadanos de la Unión Europea y países terceros.

Palabras clave: (De 3 a 5 palabras)

COVID-19, derechos fundamentales, nuevas tecnologías, Certificado COVID Digital de la UE

Abstract

The declaration of a global pandemic due to the COVID-19 involved numerous restrictive measures of fundamental rights and the need to adapt to the new technologies. To fight against the transmission of the disease, it has been used conventional and new technological tools that have sharpened the debate on the interferences with data protection right and its compatibility with other fundamental rights. These technological tools have been embraced with a wide range of outcomes, due to the lack of knowledge on the possibilities and the guaranties that the current regulations provide and the lack of trust on its principles. Currently, European authorities are making great efforts to disclose the benefits of the last technological tool designed to reduce the number of infections from COVID-19, the EU Digital COVID Certificate, which is intended to ensure that it is used by as many people from the European Union and third contries as possible.

Keywords:

COVID-19, fundamental rigths, new technologies, EU Digital COVID Certificate

Índice de contenidos

Listado de abreviaturas

AEPD	Agencia Española de Protección de Datos.
CEPD	Comité Europeo de Protección de Datos.
COVID-19	enfermedad infecciosa provocada por el virus SARS-CoV-2.
DOUE	Diario Oficial de la Unión Europea
Ley Orgánica 3/2018	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
Ley Orgánica 15/1999	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
Ley Orgánica 3/1986	Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública.
OMS	Organización Mundial de la Salud.
Propuesta de Reglamento	Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a un marco para la expedición, verificación y aceptación de certificados interoperables de vacunación, de test y de recuperación para facilitar la libre circulación durante la pandemia de COVID-19 (certificado verde digital).
Reglamento 2021/953	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
RGPD	Reglamento General de Protección de Datos.
STC 186/2000	Sentencia de la Sala Primera del Tribunal Constitucional, número 186/2000, de 10 de julio.

1. Introducción

1.1. Justificación del tema elegido

Huelga extenderse en lo que resulta ser una evidencia: la irrupción de la COVID-19 ha sido, y continua siendo a día de hoy, un reto a nivel mundial que ha puesto a prueba la fortaleza de los estados, sus representantes e instituciones y, claro está, a la sociedad en general.

La pérdida de forma indiscriminada de millones de vidas humanas, las restricciones sobre derechos fundamentales, el descalabro de las economías de los estados, la incertidumbre política, el cuestionamiento de valores y fundamentos democráticos, etc., se han inmiscuido en la vida cotidiana de los ciudadanos a través de los boletines oficiales y los medios de comunicación desde hace más de un año. Ahora, parece intuirse débilmente una salida a largo plazo de la presente crisis sanitaria y económica, al menos, en los países desarrollados. Así y sin querer caer en el derrotismo, tal y como veremos a lo largo del presente trabajo, se encuentran en marcha algunas iniciativas pendientes de implantación que, junto con la vacuna contra la COVID-19, hacen palpable la recuperación y la posibilidad, al menos, de convivir con el virus y volver a retomar nuestra forma de vida.

En este contexto, la COMISIÓN EUROPEA (2020) oportunamente ha calificado como "*hastío por la pandemi*a" el sentimiento generalizado de los ciudadanos y de los entes públicos y privados, quienes se encuentran agotados por los esfuerzos realizados para contener la propagación del virus, el exceso de información, en ocasiones no debidamente contrastada, y la necesidad de adaptación a los nuevos medios digitales de forma inmediata y sin tiempo para la reflexión.

Así las cosas, la pandemia ha puesto de manifiesto que la globalización es una realidad y que las nuevas tecnologías se han revelado como un instrumento imprescindible en nuestras comunicaciones y estilo de vida. En este sentido, su uso se ha incrementado de forma exponencial a la hora de atajar la actual crisis sanitaria no sólo de cara al control de la transmisión de la enfermedad, sino también con fines informativos, como medio paliativo para evitar una catástrofe económica en determinados sectores profesionales, etc.

Mas aún si cabe, las personas físicas han sido realmente conscientes de la magnitud del flujo e intercambio de datos personales y la capacidad de tratamiento y utilización de dichos datos por parte de las empresas y organismos oficiales. Esta inquietud se ha visto negativamente influenciada por debates en torno a la colisión del derecho fundamental a la protección de datos personales frente a otros derechos fundamentales tales como el derecho a la salud o a la libre circulación y movilidad.

Si bien el Considerando 4 del RGPD estipula tajantemente que el tratamiento de datos personales debe estar concebido para servir a la humanidad, en las actuales circunstancias se ha expandido el sentimiento generalizado de que es un obstáculo y un impedimento que nos obliga a dirimir entre salvar vidas humanas y preservar la intimidad de otras.

A la vista del escenario expuesto, se examinarán los pronunciamientos de los organismos europeos sobre esta cuestión y las dificultades que se han encontrado en la aplicación de las nuevas tecnologías para contener y prevenir la enfermedad de la COVID-19.

1.2. Problema y finalidad del trabajo

El presente trabajo analiza la vigencia del RGPD en el contexto de la pandemia causada por la COVID-19 y la aplicabilidad de sus principios en el marco de las restricciones adoptadas en los Estados miembros de la Unión Europea.

Como sabemos, el RGPD, que entró en vigor en el año 2016 -si bien no fue de aplicación hasta el 25 de mayo de 2018-, prevé el tratamiento de datos personales en contextos tales como el control de epidemias y su propagación, situaciones de emergencia humanitaria y catástrofes naturales o de origen humano.

Las excepcionales circunstancias actuales han requerido que dichas previsiones teóricas sean debidamente interpretadas y puestas en práctica. A este fin, se analizará si efectivamente el marco legislativo regulador del derecho fundamental a la protección de datos personales ha estado a la altura de las circunstancias y la manera en que, en su caso, este se ha visto limitado o supeditado para salvaguardar otros derechos fundamentales como el derecho a la salud o a la libre circulación y movilidad.

A mayor abundamiento, se estudiará una de las medidas que, junto con la vacunación contra la COVID-19, infunde una vía esperanzadora para la reapertura y recuperación de los estados como es el pasaporte inmunológico. En este sentido, se tratarán aspectos tales como su regulación e implantación así como las cautelas necesarias para preservar el derecho a la protección de datos personales de sus portadores.

1.3. Objetivos

Este trabajo tiene como objetivo realizar un análisis crítico de la interpretación del derecho fundamental a la protección de los datos personales, llevada a cabo por los distintos agentes, operadores y autoridades, en el contexto de la pandemia en Europa. A este fin, se cuestionará si una exégesis excesivamente prudente de su normativa reguladora ha limitado la capacidad de las nuevas tecnologías de combatir de manera eficaz la pandemia.

La normativa reguladora del derecho fundamental a la protección de datos se ha tornado en ocasiones vacua e ineficaz, toda vez que las autoridades no han sido capaces de infundir la suficiente confianza en los ciudadanos ni han aplicado debidamente sus preceptos.

Como consecuencia de lo anterior, se pondrá en valor la necesidad de una política y comunicación transparente alrededor del marco normativo de la protección de datos personales que ha de trasladarse a los ciudadanos. En otras palabras, se pondrá de manifiesto la importancia de transmitir de forma efectiva y clara a los beneficiarios últimos de dicha normativa la existencia de un "*marco más sólido y coherente*", tal y como expone el Considerando 7 del propio RGPD, que les proporciona el control de sus propios datos personales.

Por todo ello, dicha confianza en la normativa vigente y en las instituciones es imprescindible para que, tal y como indica el reseñado Considerando 7 del RGPD, la economía digital pueda desarrollarse en todo el mercado interior y contribuir, en consecuencia, al desarrollo económico, social y cultural a todos los niveles.

2. Marco teórico y desarrollo

2.1. EL CONTEXTO DE CRISIS SOCIO-SANITARIO ACTUAL COMO DESAFÍO A LA NORMATIVA DE PROTECCIÓN DE DATOS PERSONALES VIGENTE

2.1.1. El desarrollo tecnológico como causa del origen del derecho fundamental a la protección de datos personales.

De cara al análisis de la resiliencia del derecho fundamental a la protección de datos personales en las circunstancias actuales, fuertemente marcadas por la situación de crisis socio-sanitaria causada por la COVID-19, cabe realizar una breve contextualización histórica del precitado derecho cuyo origen se encuentra fuertemente vinculado al desarrollo tecnológico.

En este sentido, CAZURRO (2020) se remonta a finales del siglo XIX, tras la publicación del artículo "The Right To Privacy" de los norteamericanos Samuel Warren y Louis Brandeis, para señalar el germen del derecho a la intimidad, entendido en sus inicios como defensa a la vida privada, que evolucionaría, como consecuencia principal de los avances tecnológicos (referidos, fundamentalmente, al desarrollo de aparatos de captación de imagen y sonido), en la noción legal de protección de datos personales, con los principios y garantías que conocemos en la actualidad.

En este contexto, el temor a los incipientes avances tecnológicos, los cuales procuraban grandes ventajas a la sociedad y a su vez revelaban parcelas de la intimidad de las personas físicas, condujo a realizar una reflexión acerca de la protección de los individuos frente a las nuevas técnicas de recogida y tratamiento de información y proporcionar herramientas legales que permitieran controlar o al menos conocer dicha información.

En consecuencia, CAZURRO (2020) señala que, de forma paulatina, el derecho a la protección de datos personales se fue configurando como una solución que permitía el tratamiento de información personal garantizando un uso debido de la misma a sus titulares.

En definitiva, el reseñado autor concluye que el derecho a la protección de datos personales es relativamente moderno cuyo nacimiento está íntimamente ligado al desarrollo tecnológico.

Bajo esta premisa, analizaremos la repercusión de las soluciones tecnológicas diseñadas para luchar contra la pandemia causada por la COVID-19, en relación, principalmente, con los derechos fundamentales recogidos en la Carta de los Derechos Fundamentales de la Unión Europea, consagrados en el artículo 7, sobre el respeto de la vida privada, y el artículo 8, sobre el derecho a la protección de datos personales.

En particular, cabe precisar que, en lo que se refiere al tratamiento de datos personales, es de aplicación el RGPD a nivel europeo y en España la Ley Orgánica 3/2018, las cuales, tras un breve periodo de evolución, estipulan los principios y garantías que deben regir la totalidad de los tratamientos de datos personales de las personas físicas.

2.1.2. La irrupción de la COVID-19 en el panorama internacional

El pasado 22 y 23 de enero de 2020, el Comité de Emergencia convocado por el Director General de la OMS se reunió para tratar sobre un brote de un nuevo coronavirus, hasta la fecha desconocido. Sin ser posible determinar la fecha ni la causa exacta de su aparición, las primeras noticias relativas a los estragos causados por su infección sitúan su origen en la ciudad china de Wuhan, en diciembre de 2019. No obstante su alto índice de contagio y de transmisión sin precedentes, el Comité de Emergencia no acordó la declaración la de "emergencia de salud pública de importancia internacional" (ESPII), de conformidad con lo establecido en el Reglamento Sanitario Internacional (2005) sin perjuicio de que, habida cuenta de la urgencia de la situación, sus miembros serían convocados nuevamente en unos días para proseguir su examen.

Dicha declaración fue acordada al término de la segunda reunión, celebrada el 30 de enero de 2020. Consecuentemente y, tomando como referencia a China quien ya venía sufriendo las consecuencias de la enfermedad, el Comité de Emergencia de la OMS publicó algunas recomendaciones temporales con el fin de conseguir la detección de forma temprana de la enfermedad, tales como, promover la vigilancia activa, el aislamiento de casos, el seguimiento de contactos y la promoción medidas de distanciamiento físico de acuerdo con el nivel de riesgo al que pudieran verse sometidas las personas.

Con carácter adicional, sin perjuicio de que el Comité de Emergencia advirtió de la necesidad de evitar la propagación del virus a escala internacional, dada la información disponible en

aquel momento, cabe destacar a estos efectos que el Comité de Emergencia no recomendó la aplicación de medidas restrictivas sobre viajes o el comercio.

En fecha 11 de marzo de 2020, la OMS determinó en su evaluación que la COVID-19 podía ser calificada como una pandemia y alentó a los dirigentes de todos los países a detectar, realizar pruebas, tratar, aislar, rastrear, y activar sus mecanismos de respuesta para hacer frente a una emergencia de dimensión mundial. En ese momento, se había detectado que en las dos semanas anteriores a la declaración de pandemia el número de casos de COVID-19 fuera de China se había multiplicado por 13 y el número de países afectados se había triplicado, como consecuencia de los alarmantes niveles de propagación y gravedad de la enfermedad, como por los alarmantes niveles de inacción de las autoridades.

A raíz de lo anterior, a nivel jurídico se sucedieron las declaraciones de estados excepcionales en los distintos países y comenzó una inflación normativa, fruto en muchos casos de la improvisación y falta de medios y recursos para afrontar la situación[1].

Transcurrido más de un año desde la citada declaración de emergencia AMNISTÍA INTERNACIONAL (2021) ha denunciado que la pandemia y algunas de las medidas adoptadas para abordarla han tenido un efecto devastador en la vida de millones de personas. Dichas medidas asimismo han revelado y en ocasiones agravado patrones ya existentes de abusos contra los derechos humanos y de desigualdad. Así, el precitado informe advierte que la pandemia ha puesto claramente de manifiesto los efectos que habían tenido en los derechos humanos los años de crisis económicas y políticas y las deficiencias de los sistemas mundiales de gobernanza y cooperación, que algunos Estados agravaron eludiendo sus responsabilidades.

2.1.3. La necesidad de adoptar medidas excepcionales para afrontar la crisis sanitaria provocada por la COVID-19

A raíz de la irrupción de la pandemia y de la consecuente necesidad de imponer graves medidas restrictivas para conocer su evolución y evitar su propagación, las instituciones y

[1] Sin ir más lejos, en la misma fecha de depósito del presente trabajo, los medios de comunicación han publicado que el Pleno del Tribunal Constitucional español ha declarado inconstitucional el artículo referido al confinamiento domiciliario de la población impuesto durante el estado de alarma.

ordenamientos jurídicos de los estados de derecho se han visto sometidos a duras pruebas de resiliencia, a través de la utilización de herramientas jurídicas extraordinarias previstas para circunstancias de grave alteración de la normalidad y estabilidad institucional y la puesta en peligro de la seguridad de las naciones.

DOMÍNGUEZ (2021) afirma que la gravedad y excepcionalidad de esta circunstancia nos permitiría afirmar que la crisis de la COVID-19 nos enfrenta a multitud de escenarios desconocidos hasta la fecha, y propicia la necesidad de que el conjunto de la ciudadanía aporte, en la medida de sus posibilidades, su (*sic*) cuota alícuota de responsabilidad para superar esta difícil situación. En este sentido, no únicamente los organismos oficiales han tenido un papel irremplazable para reconducir la situación a través de la imposición de medidas restrictivas, sino que ha sido necesario el esfuerzo y disposición de la totalidad de los ciudadanos para mitigar las consecuencias de la pandemia.

A título enunciativo, todas estas medidas han conllevado la introducción de nuevos hábitos de higiene, imposición de normas de distanciamiento social, confinamiento, etc. En definitiva, las reseñadas medidas han supuesto una grave intrusión en los derechos fundamentales de los ciudadanos y un serio perjuicio para las economías de los países. Asimismo, en el contexto incierto en el que nos encontramos, las autoridades están buscando medidas alternativas que de forma escalonada y coordinada, permitan nuevamente el ejercicio libre y seguro de los derechos fundamentales hasta ahora restringidos y favorezcan la recuperación económica.

No obstante, como veremos, las incógnitas relacionadas con las medidas propuestas de cara al futuro (tales como la posibilidad de imponer la vacunación obligatoria a toda la población, el pasaporte inmunológico, etc.) interferirían reiteradamente en la esfera de los derechos fundamentales de los ciudadanos.

La utilización de dichos instrumentos jurídicos se ha visto propulsada en gran parte por el avance tecnológico actual que ha permitido, entre otros, el acceso a información permanentemente actualizada y a publicaciones oficiales a gran parte de la población (creando en consecuencia una gran incertidumbre jurídica al publicarse con periodicidad prácticamente diaria nueva normativa y dando por sentado que todos disponen de medios

humanos y tecnológicos para hacer el seguimiento), la trazabilidad masiva de contagios y la obtención a marchas forzadas de una vacuna contra la COVID-19.

La revolución tecnológica que veníamos observando con anterioridad a la pandemia ha permitido que la información, las medidas de seguimiento, alerta, intercambio de datos, etc. pudieran ser aplicadas de manera *cuasi* inmediata y masiva y que sus resultados hayan sido más eficaces que a través de la utilización de recursos no tecnológicos o tradicionales.

Desde un primer momento, las autoridades competentes y las entidades privadas han reconocido el valor de los medios tecnológicos para optimizar la efectividad de los recursos empleados para preservar la salud de las personas y mantener, en la medida de lo posible, la actividad y productividad de la economía.

Así, la tecnología ha amortiguado la caída de la economía, si bien de forma discriminatoria por sectores y/o segmentos de población, permitiendo, entre otros, la adopción inmediata del teletrabajo, el auge del comercio electrónico y propiciando cambios en los comportamientos y estilos de vida de los ciudadanos que previsiblemente perdurarán tras la contención de la pandemia.

En palabras de ARENAS (2020), existiría un consenso generalizado en que la tecnología y el uso masivo de dispositivos móviles, así como el tratamiento de datos personales, han constituido una herramienta clave en la lucha contra la pandemia.

La presente crisis sanitaria se ha afrontado desde nuevas perspectivas a través del diseño al efecto de nuevos instrumentos y cauces que han colisionado, o al menos, han generado tensión con otros derechos fundamentales como la libre circulación y movilidad o el derecho a la protección de datos personales.

Así, son numerosas voces las que en la situación actual han reiterado que los derechos fundamentales no son absolutos y que, por tanto, la aplicación de medidas que pudieran ser intrusivas y limitadoras de otros derechos fundamentales deben ser cautelosamente analizadas desde un punto de vista jurídico, requiriendo un cuidadoso examen de ponderación.

De este modo, la utilización de herramientas tecnológicas y medidas digitales han despertado la conciencia social sobre la necesidad de proteger un bien jurídico que, si bien

ya se encontraba previsto y protegido en la legislación vigente, hasta la fecha no había sido una prioridad para los ciudadanos.

En este sentido los titulares de datos personales han sido conscientes de que el flujo y el tratamiento de datos se ha incrementado exponencialmente, alertando a la sociedad a este respecto y aumentando la preocupación sobre cuestiones tales como el tratamiento automatizado de datos, el control de las instituciones y empresas responsables del tratamiento, la necesidad del consentimiento para proporcionar datos personales, los fines y usos que se darán a los datos personales, etc.

Ya el CEPD (2020b) advirtió que los datos y la tecnología empleados para contribuir a la lucha contra la COVID-19 deben utilizarse para empoderar, más que para controlar, estigmatizar o reprimir a los ciudadanos. Continúa afirmando que aunque los datos y la tecnología puedan ser herramientas importantes, tienen limitaciones intrínsecas y tan solo pueden potenciar la eficacia de otras medidas de salud pública. En este sentido, el CEPD completa argumentando que los principios generales de eficacia, necesidad y proporcionalidad deben dirigir cualquier medida adoptada por los Estados miembros o las instituciones de la UE que implique el tratamiento de datos personales para combatir la COVID-19.

Como se verá a continuación, pese a la intensificación del debate sobre la privacidad y la protección de datos en la pandemia, ha de precisarse que no existe una dicotomía entre seguridad y privacidad, y no sería necesario tener que renunciar a uno para beneficiarse de otro. Es pernicioso entrar en este debate. Tal y como se encuentra regulado el derecho a la protección de datos no es incompatible con la seguridad, el derecho a la movilidad y circulación o a la salud.

Bajo este prisma y a los efectos del presente trabajo, centraremos el análisis en el estudio de la injerencia de las restricciones adoptadas sobre los derechos fundamentales y, en particular, sobre el derecho a la protección de datos personales así como su influencia en la modulación de otros derechos fundamentales.

2.1.4. Las premisas adoptadas por las autoridades competentes en materia de protección de datos personales frente a los tratamientos efectuados en la lucha contra la COVID-19.

Resulta preciso partir de la premisa anunciada por las autoridades competentes en materia de protección de datos, por la cual afirman que los principios consagrados en el artículo 5 del RGPD siguen plenamente vigentes y la regulación es lo suficientemente amplia como para ser aplicada en circunstancias extraordinarias de crisis sanitaria como la actual.

Así, el CEPD (2020a) desde los inicios de la pandemia ha reiterado que las normas de protección de datos, como serían el RGPD y en el caso español la Ley 3/2018, no entorpecerían las medidas adoptadas para luchar contra la pandemia de COVID-19. Más específicamente el CEPD (2020b) ha insistido en que no debe entenderse que la normativa impide el tratamiento de datos personales sino que previene un uso indebido de los mismos. En otras palabras, el CEPD señala que nadie debería verse obligado a elegir entre una respuesta eficaz a la crisis actual y la protección de nuestros derechos fundamentales, puesto que es posible la consecución de ambos objetivos. A mayor abundancia, defiende los principios consagrados en la normativa vigente de protección de datos y su importancia primordial en la lucha contra el virus.

Así, concreta que la legislación europea en materia de protección de datos personales no solo prevé sino que permite el uso responsable de datos personales para fines de gestión sanitaria, al tiempo que garantiza que en ese proceso no se erosionen los derechos y libertades individuales.

La conclusión del CEPD va más allá, advirtiendo que la protección de datos no solo no sería un obstáculo para la lucha contra la pandemia sino que constituiría un generador de confianza para la aceptación social, tan necesaria como veremos en epígrafes posteriores, de soluciones que garanticen la eficacia de las medidas propuestas para la erradicación de la pandemia.

Paralelamente, cabe traer a colación los pronunciamientos de la AEPD en España, quien en similares términos ha aclarado que la normativa en protección de datos es aplicable en su

integridad a la situación epidemiológica actual sin que se puedan encontrar motivos que pudieran justificar la suspensión de los principios del derecho a la protección de datos.

Así, la AEPD (2020b) ha declarado que el RGPD contendría las salvaguardas y reglas necesarias para permitir legítimamente los tratamientos de datos personales en situaciones, como la presente crisis sanitaria.

De forma análoga al CEPD, la AEPD (2020b) ha defendido que la debida aplicación de los preceptos consagrados en el RGPD, en consonancia con la normativa sectorial aplicable en el ámbito de la salud pública, no deberían utilizarse para obstaculizar o limitar la efectividad de las medidas que adopten las autoridades, especialmente las sanitarias, en la lucha contra la epidemia, por cuanto ya la normativa de protección de datos personales contiene una regulación para dichos casos que compatibiliza y pondera los intereses y derechos en liza para el bien común.

Las antedichas declaraciones responden a la necesidad de frenar el debate sobre la colisión entre el derecho fundamental a la salud y el derecho fundamental a la privacidad y a la protección de datos. Tal y como expone ARENAS (2020) este debate nos sitúa en la aparente necesidad de tener que decidir entre seguridad o salud pública y privacidad. Afirma que la respuesta no es tan sencilla, ya que se trata de una decisión compleja que, dadas las actuales circunstancias, hay que tomar sin tiempo para la reflexión, lo cual es peligroso, pues nos estamos enfrentando a decisiones importantes para nuestra sociedad, que marcarán el tipo de sociedad que pretendemos ser.

Por su parte DOMÍNGUEZ (2021), ensalza el valioso papel que desempeñan las tecnologías y los datos digitales en la lucha contra la crisis de la COVID-19. Estas tecnologías y datos ofrecerían en muchos casos una herramienta importante para informar al conjunto de la ciudadanía y ayudar a las autoridades públicas pertinentes en sus esfuerzos por contener la propagación del virus o para permitir que las organizaciones sanitarias intercambien datos sobre la salud.

Sin embargo, como ha puesto de relieve la COMISIÓN EUROPEA (2020) un enfoque fragmentado y descoordinado del empleo de nuevas tecnologías basadas en el tratamiento de datos personales pondría en peligro la eficacia de las medidas destinadas a combatir la

crisis de la COVID-19, dañando gravemente tanto al mercado único como a los derechos y libertades fundamentales.

En este sentido, desde el principio de la pandemia, se ha venido extendiendo un enfoque contraproducente, causado quizás por una incorrecta interpretación y entendimiento de la normativa reguladora de la protección de datos personales, por el cual se ha infundido el temor a la pérdida progresiva de intimidad y control sobre la información personal en aras del beneficio común.

A este respecto, COTINO (2020) es tajante en este asunto manifestando que plantear este tipo de debates en términos binarios sería peligroso e incluso demagógico. En similares palabras, dicho autor cita a PEDREÑO (2020) quien señala que anteponer el derecho a la privacidad al derecho a la vida o al de libertad de movimientos no tendría sentido y constituiría un dislate.

COTINO (2020) defiende que el propio sistema constitucional estaría configurado, política y jurídicamente, para deliberar, ponderar y armonizar derechos fundamentales entre sí con otros bienes constitucionales. Por su parte, y tal y como se verá posteriormente en pronunciamientos del Tribunal Constitucional Español, ningún derecho fundamental y, en consecuencia, el derecho a la protección de datos personales, es un derecho absoluto.

En este contexto, resulta preciso analizar cómo el propio ordenamiento configura las herramientas jurídicas idóneas para sopesar la injerencia de un derecho fundamental sobre otro. Así, en circunstancias excepcionales como la actual crisis sanitaria, no se haría necesario prescindir ni limitar el derecho a la protección de datos personales puesto que ya la propia normativa dispone de sus propios mecanismos para asegurar su vigencia, siendo íntegramente aplicable a los tratamientos de datos realizados en el contexto de la pandemia.

2.1.5. Análisis de las bases legitimadoras del tratamiento de los datos personales en el contexto actual de crisis sanitaria ocasionada por la COVID-19

De cara al estudio de la aplicación práctica del derecho fundamental a la protección de datos en el marco de la crisis sanitaria actual, resulta preciso conocer primeramente cuáles serían las bases legitimadoras que permitirían el tratamiento de datos personales. En este sentido,

la vigente normativa reguladora de la protección de datos personales recoge el principio de la ya derogada Directiva 95/46 por el cual se establecía que todo tratamiento de datos debe estar fundamentado en una base legal que lo legitime.

Así, el Considerando 40 del RGDP establece que "*[p]ara que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho, ya sea en el presente Reglamento o en virtud de otro Derecho de la Unión o de los Estados miembros a que se refiera el presente Reglamento, incluida la necesidad de cumplir la obligación legal aplicable al responsable del tratamiento o la necesidad de ejecutar un contrato en el que sea parte el interesado o con objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato.*"

A la vista de lo anterior, se advierte, entre otros, la facultad legislativa proporcionada a los Estados miembros quienes podrán establecer condiciones necesarias para que pueda considerarse lícito un tratamiento de datos.

En este punto cabe avanzar una reflexión que se tratará en epígrafes posteriores relativa la vacilación de las autoridades para hacer uso de la señalada facultad de establecer una base legítima para el tratamiento de datos. Así, llama cuanto menos la atención la carencia de iniciativa legislativa para promulgar normas que facilitaran el tratamiento de datos de salud, salvaguardando debidamente los principios y garantías ya establecidos por la normativa vigente en materia de protección de datos.

En este contexto, se produjo de facto, y se siguen produciendo en algunos casos, tratamientos realizados por responsables que no se encuentran amparados por ninguna norma. A título ilustrativo, cabría señalar la recogida de datos de contactos en determinados establecimientos cerrados, toma de temperatura a la entrada de establecimientos públicos, etc.

Si bien la AEPD se apresuró a comunicar el difícil encaje de algunas de estas medidas en la normativa vigente de protección de datos, las autoridades competentes no habrían actuado con la suficiente rapidez para regular estos tratamientos o, al menos, establecer alternativas seguras y proporcionar indicaciones fiables a los responsables (aclarando por ejemplo

cuándo un tratamiento podría fundarse en la base legítima del interés vital del interesado o de terceros), creando un clima de incertidumbre y desconfianza entre la población. Para estas circunstancias, hubiera sido procedente considerar la modulación, que no constricción, del derecho fundamental a la protección de datos, en beneficio del interés vital tanto del propio interesado como de terceros y, en definitiva, la salud pública o, al menos el establecimiento de líneas claras de actuación para los responsables del tratamiento.

Así, la AEPD (2020b) reconoce que en una situación de emergencia sanitaria la normativa vigente de protección de datos permite a los responsables del tratamiento, adoptar decisiones necesarias para salvaguardar los intereses vitales de las personas físicas, el cumplimiento de obligaciones legales o la salvaguardia de intereses esenciales en el tratamiento de la salud pública. No obstante, muchos responsables, aun cumpliendo con alguna de las bases legítimas precitadas, se aventuraron a realizar tratamientos sin respetar las garantías preceptivas e incluso, en algunos casos, sin ser conscientes de que realmente estaban llevando a cabo un tratamiento de datos personales, calificados estos últimos además como categoría especial de datos personales. El ejemplo más claro, sería el de la toma de temperatura a la entrada de establecimientos, como ya se ha señalado. Masivamente, los responsables del tratamiento comenzaron a tomar la temperatura de los interesados que trataban de acceder a sus establecimientos sin tener en cuenta obligaciones tales como el deber de informar, la implantación de medios técnicos de seguridad, etc. dispuestos en la normativa vigente y sin pautas de actuación dictadas por las autoridades competentes.

En esta línea, la AEPD (2020b) recuerda que el sistema legislativo español dispone de instrumentos legales suficientes tales como la Ley Orgánica 3/1986 que legitima a la autoridad sanitaria a adoptar las medidas oportunas, entre otros, para controlar enfermedades transmisibles, cuando así lo exigieran razones sanitarias de urgencia o necesidad.

Sentada la facultad legislativa de los Estados miembros, cabe precisar que el Considerando 41 del RGPD expresamente indica que la referencia a una base jurídica o a una medida legislativa dependerá del ordenamiento jurídico de cada uno de los estados, si bien no se requiere expresamente un acto parlamentario. Ahora bien, la reseñada base jurídica o

medida legislativa deberá "*ser clara y precisa y su aplicación previsible para sus destinatarios, de conformidad con la jurisprudencia del Tribunal de Justicia de la Unión Europea*".

En este contexto, el artículo 6 del RGPD establece que el tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

El apartado a) del artículo 6 del RGPD fundamenta el tratamiento en el consentimiento del interesado, que deberá cumplir los requisitos estipulados en el propio RGPD para que sea válido. Sin perjuicio de que el responsable del tratamiento haya recabado el consentimiento del interesado conforme a lo establecido en el RGPD, cabe señalar que el consentimiento no suprime la obligatoriedad de garantizar los principios del tratamiento. En otras palabras, cualquier tratamiento de datos, incluso aquellos que cuenten con el propio consentimiento

informado del interesado, deberán garantizar el cumplimiento de los principios consagrados en el artículo 5 del RGPD.

Con carácter adicional, resulta preciso indicar que, tal y como recuerda el CEPD (2020b), el consentimiento ha de ser libre, esto es, que el interesado tenga facultad real de denegar su consentimiento sin que ello conlleve consecuencias perjudiciales para el mismo. Por otro lado, el CEPD (2020a) también ha advertido recientemente que en aquellos tratamientos cuya base legítima esté fundamentada en el consentimiento deberán prever el mecanismo o posibilidad de que los interesados retiren el consentimiento otorgado en cualquier momento, de manera que cualquier tratamiento realizado con posterioridad quedaría proscrito.

Las anteriores premisas serán importantes a la hora de diseñar herramientas que conlleven tratamientos de datos para hacer frente a la actual crisis sanitaria, toda vez que la retirada del consentimiento por parte del interesado debería suponer la paralización de inmediata de cualquier tratamiento que se estuviera realizando hasta ese momento, con independencia de la conveniencia o necesidad del mismo.

Sentado lo anterior, cabe recordar que la derogada Ley Orgánica 15/1999 establecía como base de legitimación básica el consentimiento del interesado. En consecuencia, el resto de bases legitimadoras ostentaban una suerte de carácter subsidiario e incluso excepcional.

No obstante, ya el Grupo de Trabajo sobre protección de datos del artículo 29 concluyó que las bases legitimadoras habrían de fundamentar el tratamiento de datos personales en circunstancias en las que, independientemente del consentimiento, resulte apropiado y necesario.

En esta línea, tanto el RGPD como la Ley Orgánica 3/2018 no establecen una regla de prelación de las bases de legitimación, siendo todas ellas objeto de análisis de idoneidad a la hora de diseñar herramientas para el tratamiento de datos.

A estos efectos, tal y como hemos señalado con anterioridad, las autoridades competentes en materia de protección de datos se han pronunciado sobre la capacidad de la normativa vigente de regular una situación de emergencia sanitaria como la actual así como las bases legitimadoras de las que disponen los responsables, tanto públicos como privados, para

realizar los tratamientos de datos personales pertinentes en circunstancias excepcionales. En este sentido, la AEPD (2020b) aclaró cuáles serían, en particular, las bases del tratamiento en una situación de epidemia.

A continuación, analizaremos las bases jurídicas que legitiman el tratamiento para proteger los intereses vitales del interesado o de otra persona física y el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, establecidas en el artículo 6 apartados d) y f), respectivamente, y el tratamiento de categorías especiales de datos personales.

2.1.6. Artículo 6.1.d) del RGPD: Los intereses vitales del interesado u otras personas físicas como base legitimadora del tratamiento.

El artículo 6.1.d) del RGPD establece como base de legitimación para el tratamiento el interés vital del interesado, del siguiente tenor literal: "*1. El tratamiento solo será lícito si (…) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física*".

Primeramente, resulta preciso traer a colación el Considerando 46 del RGPD que establece que *"[e]l tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano*".

Cabe señalar que el interés vital como base de legitimación para el tratamiento ya venía siendo reconocido en la Directiva/95/46/CE. El RGPD vino a esclarecer su carácter suplementario frente a otras bases legitimadoras, esto es, el RGPD estableció la licitud de la presente base legítima del tratamiento cuando no pudiera basarse manifiestamente en una base jurídica diferente.

Por otro lado, el RGPD ejemplifica las circunstancias en las que pudiera ser de aplicación el interés vital del propio interesado y de otros terceros personas físicas cuando el tratamiento fuera necesario para "*fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano*".

A este respecto, la AEPD (2020b), en relación con los tratamientos de datos analizados para hacer frente a la actual crisis sanitaria ocasionada por la COVID-19, ha concretado lo siguiente:

- La base jurídica del tratamiento para proteger intereses vitales del interesado es aplicable tanto para el tratamiento de datos del propio interesado como de terceras personas físicas no identificadas o identificables, de conformidad con la redacción del apartado c) del artículo 6.1 del RGPD, que pudieran estar expuestas a riesgo de contagio.
- El artículo 6.3 del RGPD no determina la necesidad de que la presente base del tratamiento haya de ser establecida por el Derecho de la Unión o el Derecho de los Estados miembros aplicables al responsable del tratamiento.

Sin perjuicio de lo anterior, la AEPD (2020b) recalca que la base legítima establecida en el apartado d) del artículo 6.1 del RGPD no sería suficiente para el tratamiento de datos de salud. En este sentido, dicho artículo no eximiría de la prohibición del tratamiento de categorías especiales de datos, entre los que se encontrarían los datos de salud, consignada en el artículo 9.1 del RGPD.

A estos efectos, resulta preciso indicar que el RGPD otorga una especial protección a aquellos datos que se encuentran estrechamente vinculados a los derechos y las libertades fundamentales de los interesados. Así, las categorías de datos que merecen una protección reforzada serían las estipuladas en el artículo 9.1 del RGPD, a saber: los datos que revelen (i) el origen étnico o racial, (ii) las opiniones políticas, (iii) las convicciones religiosas o filosóficas, (iv) la afiliación sindical, (v) datos genéticos, (vi) datos biométricos, (vii) datos relativos a la salud o (viii) datos relativos a la vida sexual o las orientación sexual de una persona física.

El tratamiento de dichos datos estaría sometido a una prohibición general que únicamente habría de levantarse cuando el responsable obtenga el consentimiento válido del interesado o el tratamiento se realice en situaciones específicas reguladas en el propio RGPD.

Por lo tanto, para el tratamiento de categorías especiales de datos, como son los datos relativos a la salud de los interesados, deberán concurrir determinadas circunstancias que levanten la prohibición del artículo 9.1 RGPD.

En este sentido, la AEPD (2020b) ha esclarecido que para el tratamiento de datos de salud sobre la base de la protección de los intereses vitales del interesado, sería de aplicación la letra c) del artículo 9.2 RGPD que legitimaría el tratamiento del propio interesado o de otra persona física, no identificada o identificable, cuando concurran las circunstancias recogidas en el propio artículo, esto es, en el supuesto de que el interesado no estuviera capacitado, física o jurídicamente, para dar su consentimiento.

Ya el Grupo de Trabajo sobre protección de datos del artículo 29, consideraba que la base legítima que hoy constituye el apartado d) del artículo 6.2 del RGPD, había de interpretarse de forma restrictiva para proteger un interés esencial para la vida del interesado, refiriéndose en particular a cuestiones de vida o muerte o a amenazas que pudieran suponer un riesgo de lesiones u otro daño para la salud del interesado.

Así, diferenciaba la aplicación de esta base legitimadora, contenida en el apartado d) del artículo 7 de la Directiva 95/46/CE -hoy apartado d) del artículo 6 del RGPD-, de la excepción estipulada en el apartado c) del artículo 8 de la misma norma referido al tratamiento de categorías especiales de datos, que se circunscribía a aquellos tratamientos necesarios para proteger intereses vitales del interesados en los que este último no pudiera dar su consentimiento por falta de capacidad, física o jurídica.

No obstante, dada la amplitud de la redacción del apartado d) del artículo 7 de la Directiva 95/46/CE, ya derogada, el Grupo de Trabajo sobre protección de datos del artículo 29 concluía que en los casos en que fuera posible la obtención del consentimiento del interesado, prevalecería este sobre la base legítima del interés vital para llevar a cabo el tratamiento de datos. Asimismo, declinaba la utilización de la base legítima del interés vital para la recopilación o tratamiento masivo de datos personales.

2.1.7. Artículo 6.1.e) del RGDP: Misión realizada en interés público como base legitimadora del tratamiento.

El artículo 6.1.e) del RGPD establece la licitud del tratamiento si "*es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento*".

A estos efectos, resulta preciso tener en cuenta que el artículo 6.3 del RGPD dispone la necesidad de que dicha base de tratamiento se encuentre establecida por el Derecho de la Unión o el Derecho de los Estados miembros que se aplique al responsable del tratamiento.

Específicamente, el Considerando 45 del RGPD explicita que no será necesario que cada tratamiento individual legitimado por la realización de una misión en interés público se encuentre regulado por una norma específica. Sin perjuicio de lo anterior, la norma reguladora a estos efectos deberá concretar la finalidad del tratamiento o tratamientos de datos personales y podrá, de manera adicional, regular aspectos tales como las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, etc. A estos efectos, el derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

El poder oficial o misión de interés público, sobre el que se fundamente el tratamiento, deberá conferirse o atribuirse normalmente mediante leyes ordinarias u otra normativa jurídica. Si el tratamiento conllevara una invasión de la privacidad o si este se exige de otro modo en virtud de la legislación nacional para garantizar la protección de las personas afectadas, la base jurídica deberá ser lo suficientemente específica y precisa a la hora de definir el tipo de tratamiento de datos que puede permitirse.

De acuerdo con las conclusiones alcanzadas por el Grupo de Trabajo sobre protección de datos del artículo 29 en relación con el ya derogado apartado e) del artículo 7 de la Directiva 95/46/CE (correlativo al apartado e) del artículo 6 del RGPD), la base legitimadora del

tratamiento en virtud de una misión de interés público, contemplaba los tratamientos realizados en interés público de la Unión Europea o de un Estado miembro. Asimismo, especificaba que habría de entenderse por "poder público" a una autoridad conferida por la Unión Europea o un Estado miembro.

Sentado lo anterior, la indicada base de legitimación sería aplicable para los tratamientos realizados por un responsable del tratamiento que ostentase una potestad pública o tuviera encomendada una misión de interés público (aunque no necesariamente tuviera obligación de tratar los datos) y el tratamiento fuera necesario para el ejercicio de dicha potestad o realización de una misión en interés público.

Adicionalmente, la base de legitimación analizada serviría de soporte para los tratamientos en los que el responsable del tratamiento no tuviera una potestad oficial, pero una tercera parte con dicha potestad le requiriera para revelar los datos. Asimismo, la referida base legítima cubriría las situaciones en las que el responsable del tratamiento, sin potestad oficial, comunicase de forma proactiva los datos a una tercera parte que si ostentara potestad oficial.

Por otro lado, advertía el Grupo de Trabajo del Artículo 29 que para alegar la concurrencia de dicha base de legitimación, no se exigiría que el responsable del tratamiento actuara en virtud de una obligación jurídica. Sin perjuicio de lo anterior, esclarecía que de forma alternativa, el tratamiento debía ser en todo caso necesario para el cumplimiento de una misión en interés público, o el responsable o la tercera parte a la que se comunican los datos debe estar debidamente embestida de un poder oficial y el tratamiento debe ser necesario para el ejercicio de dicha potestad.

A efectos de los tratamientos de datos personales realizados en el marco de la pandemia ocasionada por la COVID-19, la AEPD (2020b), encuadra los tratamientos de datos de salud realizados en virtud de interés público en los apartados g) e i) del artículo 9.2 del RGPD, refiriéndose el primero de ellos a un interés público calificado de "esencial" y el segundo en el ámbito de la salud pública, siempre y cuando fuera acorde al Derecho de la Unión Europea o de los Estados miembros y se establezcan medidas adecuadas y específicas para proteger los derechos y libertades de los interesados.

2.2. Aplicaciones tecnológicas en la lucha contra la pandemia

En el presente epígrafe se tratará la aplicación práctica de los preceptos de la normativa reguladora del derecho fundamental a la protección de datos personales y, en particular, algunas aplicaciones y herramientas tecnológicas creadas para frenar su avance y propagación. En este sentido, a lo largo de la existente emergencia sanitaria se han venido desarrollando diferentes soluciones tecnológicas con el fin de interrumpir las cadenas de transmisión de la COVID-19, cuyo diseño ha sido supeditado al cumplimiento del RGPD y, en España, a la Ley 3/2018.

Con carácter general, destacan las aplicaciones de rastreo de contactos que se han desarrollado en numerosos países, cuyos resultados en la lucha contra la expansión de la COVID-19 han sido absolutamente desiguales en los territorios implantados. Cabe reseñar el siguiente análisis global de ARENAS (2020) al respecto:

> "De entre las 80 *apps* de rastreo existentes, a julio de 2020, debemos mencionar, por ser de las primeras, la de Singapur (*TraceTogether*), o China (*Alipay Health Code*), así como la alemana *CoronaWarm*, por ser una de las que se han demostrado más eficaces y respetuosas con la privacidad de los ciudadanos, hasta aplicaciones que se pusieron en marcha y tuvieron que dar marcha atrás como la de Noruega, o las que han seguido modelos o protocolos diferentes como la francesa con *StopCovid*, o la de Letonia con *ApturiCovid*, [j]unto a Letonia, segundo país en introducir una *app* basada en la API de Google y Apple (el primero fue Suiza, con *SwissCovid*., país donde se desarrolló el protocolo que ha servido de base e inspiración a Google y Apple), en Italia se desarrolló *Immuni*, que se lanzó el 2 de junio de 2020, siguiendo un modelo centralizado.
>
> Entre los intentos fallidos de *apps*, pode[m]os citar el caso de Noruega, que tras meses con su *app* por GPS, *Smittestopp*, la tuvo que retirar, esencialmente por permitir por recopilar grandes cantidades de información personal sobre aquellos que usan la aplicación, incluidos datos de ubicación continua e información sobre el contacto de los usuarios con otros. En un estado de bypass se encuentra también la *app* del Reino Unido, que tienen el antecedente de la *app FluPhone*. Y un caso

> peculiar es la *app* polaca. En Polonia (*Home Quarantining*), curiosamente, junto a los datos de localización solicita como obligatorio mandar fotografías o *selfies* que podrán ser controlados por la policía para controlar la ubicación."

A las numerosas iniciativas desarrolladas en todos los países, cabe añadir el caso español, en el que la acogida de este tipo de aplicaciones ha sido un rotundo fracaso desde sus inicios.

Brevemente, antes de la aprobación del Plan para la Transición a una nueva normalidad, por Acuerdo del Consejo de Ministros de 28 de abril de 2020, por el cual encomendó a la Secretaría de Estado de Digitalización e Inteligencia Artificial el desarrollo de "*soluciones tecnológicas y aplicaciones móviles para la recopilación de datos con el fin de mejorar la eficiencia operativa de los servicios sanitarios, así como la mejor atención y accesibilidad por parte de los ciudadanos*", en España ya se habían desarrollado numerosas aplicaciones, de carácter informativo, preventivo y de rastreo, a nivel autonómico. Así, cabe destacar, entre otras, CoronaMadrid, Stop COVID-19 CAT en Cataluña, Salud Responde en Andalucía, Test COVID-19 en Castilla y León, CoronaTest en Navarra, COVID-19.EUS en Euskadi, etc.

En este contexto, cuando el Consejo de Ministros aprobó la creación a nivel estatal de la aplicación RadarCovid, su acogida entre los usuarios fue cuanto menos escasa. El caos informativo y tecnológico que se había instalado entre los ciudadanos españoles ante la aparición de multitud de aplicaciones y, según apunta ARENAS (2020), la falta de confianza del propio Ministerio de Sanidad en la aplicación como herramienta de contención del virus, resultó en un total desperdicio de recursos económicos que no lograron reducir la congestión del sistema sanitario y de los sistemas de rastreo manuales.

A la vista de la experiencia anterior, la COMISIÓN EUROPEA (2021) publicó sus recomendaciones al respecto, a través de las cuales trató de infundir cierto empoderamiento de los interesados sobre sus datos. A grandes rasgos, estableció con carácter general los siguientes requisitos para el desarrollo de dichas aplicaciones informativas y de rastreo de contactos:

- Su instalación debía ser voluntaria.
- No debían mezclarse distintas funcionalidades (estas serían, función informativa, función de comprobación y telemedicina y función de rastreo).

- Los datos debían almacenarse, en su caso, en el dispositivo del usuario.
- El respeto por los principios y obligaciones establecidos en la normativa vigente en materia de protección de datos personales.
- Las aplicaciones habrían de desactivarse una vez que se hubiera controlado la pandemia, sin que dependiera de la desinstalación por parte del usuario.

Actualmente, una de las soluciones tecnológicas en la lucha contra la propagación contra la COVID-19 que está siendo objeto de desarrollo legislativo e implementación, es la creación de un pasaporte inmunológico, conocido coloquialmente como "Pasaporte COVID".

Dicha medida ideada desde el inicio de la pandemia ha sido sometida a graves cuestionamientos acerca de su eficacia y, sobre todo, acerca de su injerencia en el derecho a la privacidad de las personas. No obstante, hoy día es presentada por las autoridades europeas como una vía beneficiosa para facilitar la movilidad y circulación de ciudadanos europeos y para preservar la economía de los Estados miembros de cara a impulsar la temporada estival.

En este sentido, bajo la premisa de la interoperabilidad entre estados, con la implantación de esta medida, las autoridades pretenden contribuir a la reapertura segura y levantamiento coordinado de las restricciones así como recuperación de la economía de los países, facilitando la movilidad, tanto por motivos justificados como por mero ocio, de forma segura.

La COMISIÓN EUROPEA (2020) señala la urgencia de adoptar esta medida con el fin de proteger sectores muy perjudicados por la actual pandemia como son el turismo, la cultura y el deporte, sectores que constituyen pilares de la sociedad y idiosincrasia europeas. En particular, advierte que el sector turístico europeo:

> "(…) [S]e ha visto gravemente perturbado. En doce Estados miembros, el turismo genera entre el 25% y el 10% del PIB nacional, y cuatro Estados miembros de la UE figuraban en 2019 entre los diez destinos turísticos principales del mundo en términos de llegadas internacionales e ingresos. Como un desplome del 70% de los ingresos durante 2020 y hasta once millones de puestos de trabajo en peligro, los servicios turísticos se encuentran en la zona inferior del índice de confianza

> empresarial. En 2020, las pernoctaciones en la UE disminuyeron un 52% y las estancias turísticas internacionales cayeron un 68%. Las economías de algunos Estados miembros también dependen en enorme medida del turismo internacional y no pueden compensar la pérdida de viajeros extranjeros con el turismo nacional. La reanudación de los viajes y el turismo devolverá a millones de europeos a sus puestos de trabajo y podrá impulsar la recuperación más rápidamente en muchas regiones de la UE."

Los datos arrojados no hacen sino urgir a la búsqueda de propuestas para evitar una catástrofe económica mayor.

2.2.1. El Certificado COVID Digital de la UE.

El 17 de marzo de 2021, la Comisión Europea presentó la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a un marco para la expedición, verificación y aceptación de certificados interoperables de vacunación, de test y de recuperación para facilitar la libre circulación durante la pandemia de COVID-19 (certificado verde digital) con el fin de que, con anterioridad al inicio de la estación del verano, los Estados miembros adaptaran sus infraestructuras logísticas para garantizar su interoperabilidad y consiguiente eficacia, no solo a nivel europeo sino también a nivel internacional.

Dicha Propuesta de Reglamento nació principalmente como respuesta a la preocupación de las autoridades europeas por salvaguardar el derecho fundamental a circular y residir libremente en el territorio de los Estados miembros de la Unión Europea. En este sentido, el citado derecho fundamental constituye uno de los derechos básicos y primordiales para la economía de la Unión, que se ha visto gravemente afectado por las restricciones adoptadas por las autoridades competentes para limitar la propagación del coronavirus y, en particular, por la aplicación desigual de cada uno de los Estados miembros de criterios y umbrales cuyas consecuencias han recaído en última instancia en los ciudadanos.

Si bien las diferentes restricciones dentro de la Unión habían estado enmarcadas en los pronunciamientos de los organismos europeos, que fundamentalmente abogaban por la necesidad de que dichas medidas estuvieran basadas en "*motivos de interés público específicos y limitados*" (CONSEJO EUROPEO, 2021), se había venido detectando que la falta

de documentos normalizados, la imposición de diferentes requisitos por parte de los Estados miembros, habría implicado serias dificultades para la libre circulación de los ciudadanos. Con carácter adicional, la infraestructura digital planteada para acreditación de los certificados, está asimismo diseñada para poner fin a la circulación de documentos falsificados, que ponían en grave riesgo la salud pública.

El Reglamento 2021/953 fue publicado en el DOUE el pasado 15 de junio y entró en vigor posteriormente, el 1 de julio, con un período de introducción progresiva de seis semanas para la expedición de certificados en aquellos Estados miembros que necesitaren más tiempo.

2.2.2. La postura de los organismos europeos con respecto al Certificado COVID Digital de la UE

Las distintas implicaciones de las soluciones digitales en la lucha contra la pandemia han sido objeto de estudio por parte de las autoridades competentes en materia de protección de datos. En particular, el concepto de la creación de un pasaporte inmunológico, no es reciente. Los avances en los estudios sobre las posibles consecuencias de la implantación de esta medida, así como las implicaciones jurídicas, especialmente en lo relativo a su injerencia en derechos tales como la vida privada y la protección de datos personales, han sido objeto de pronunciamiento por parte de las autoridades competentes.

A título de ejemplo, la COMISIÓN EUROPEA (2021) ponía especial énfasis en el valioso papel que podrían desempeñar las tecnologías en la lucha contra la expansión de la COVID-19, enfocando su utilidad a fines informativos y orientativos, de seguimiento y vigilancia epidemiológica, y sensibilización de la ciudadanía. La repercusión y eficacia de los medios digitales estaría supeditada a un enfoque paneuropeo y coordinado poniendo al alcance de todos los ciudadanos de la Unión metodología interoperable y coordinada entre los Estados miembros.

Por su parte, la AEPD (2020a) ya puso de relieve en mayo de 2020 sus reparos a esta clase de soluciones tecnológicas a las que denominaba “pasaportes de inmunidad”. Cabe señalar que en el último año, los avances en investigación sobre la COVID-19 han sido considerables dada la urgencia y la necesidad de combatir la enfermedad, por lo que el escenario actual

dista radicalmente del contexto en el que fue publicado el análisis de costes y beneficios de la AEPD.

En dicho informe, la AEPD (2020a) revelaba cierta reticencia a la consignación de datos de carácter sensible en un documento portado en un dispositivo móvil y ponía de manifiesto la vulnerabilidad de dicho sistema a brechas de seguridad causadas por ciberdelincuentes, así como que pudiera ser utilizado como objeto de cruce con otros datos excediendo así de la finalidad para la que se habrían recabado los datos. Como veremos posteriormente, algunas de las prevenciones advertidas por la AEPD han sido superadas de acuerdo con la redacción actual de la Propuesta de Reglamento.

A los efectos del presente estudio del Certificado COVID Digital de la UE, la AEPD (2020a) recalcaba que dicha solución tecnológica únicamente podría ser beneficiosa en la medida en que el "pasaporte de inmunidad" pudiera ser actualizado con inmediatez, como no podía ser de otra manera, de conformidad con el principio de exactitud de los datos personales consagrado en el RGPD, y accesible a personal vinculado al cumplimiento de las finalidades relacionadas con políticas públicas para el control de la pandemia. Asimismo, destacaba como impedimento la necesidad de utilizar dispositivos móviles de clase *smartphone*, lo cual podría suponer la discriminación de un extenso grupo de población que no tendría acceso a estos, lo que adicionalmente limitaría la eficacia de dicha medida.

2.2.3. Características y funcionalidades del Certificado COVID Digital de la UE

El conocido como "Certificado COVID Digital de la UE" constituye uno de los proyectos más ambiciosos de la Unión Europea en la lucha contra la pandemia de la COVID-19, toda vez que establece especificaciones que sean aplicables no solo en los Estados miembros sino con la vista puesta en la interoperabilidad con sistemas tecnológicos a nivel mundial. En este sentido, un ciudadano portador del Certificado COVID Digital de la UE, en las modalidades reseñadas a continuación, quedaría exento de las restricciones a la libre circulación, equiparándose a un ciudadano del Estado miembro visitado.

Sentado lo anterior, a continuación se exponen brevemente las principales características del Certificado COVID Digital de la UE.

De acuerdo con el artículo 1 de la Propuesta de Reglamento, la implantación del marco común para certificado verde digital contemplaría la expedición, verificación y aceptación transfronterizas de (i) certificados de vacunación; (ii) certificados de test -o de diagnóstico conforme a la redacción final del Reglamento 2021/953-; (iii) certificados de recuperación tras el padecimiento de la COVID-19.

En este marco, los certificados contendrían un código QR con firma digital y se expedirían en formato electrónico o papel, garantizando así el acceso a los certificados a la mayor parte posible de la población y a la neutralidad tecnológica, con las especificaciones técnicas recogidas en la Propuesta de Reglamento y, como mínimo, en la lengua o lenguas oficiales del Estado emisor del certificado y en inglés.

Ante todo, la Comisión Europea advierte de que el presente certificado no puede constituir un requisito para la movilidad sino que se trataría de un salvoconducto o prueba suficiente para dispensar a sus portadores de medidas tales como cuarentena o pruebas diagnósticas.

Lo realmente interesante de la propuesta del Certificado COVID Digital de la UE sería el esfuerzo de coordinación entre estados, es decir, la clave del éxito residiría en el enfoque paneuropeo desde su diseño para poner a disposición de todos los ciudadanos de la Unión, e incluso de países terceros, metodología interoperable que permita la movilidad.

Asimismo, tal y como estaría delineada la infraestructura del Certificado COVID Digital de la UE, se habrían superado las prevenciones ya señaladas por la AEPD. Por un lado, el carácter gratuito y la incorporación del formato papel permitiría la obtención del certificado a la totalidad de los interesados, sin necesidad de estar en posesión de un *smartphone* o tecnología similar. Por otro lado, entre los tratamientos amparados por la normativa europea no se encontraría el almacenamiento de datos de salud, esto es, no estaría contemplada la creación de una base de datos europea sobre vacunación, test o recuperación de la COVID-19. En este sentido, los datos residirían en el dispositivo del portador que estaría protegido contra la falsificación y manipulación a través de la verificación de la firma digital.

A estos efectos, los datos personales contenidos en el certificado no serían objeto de comprobación por las autoridades legitimadas, sino que sería verificada la firma del centro

emisor, mediante la participación en una infraestructura de clave pública o intercambio bilateral de claves públicas, almacenada en una base de datos segura en cada país, para autenticar el certificado por parte de las autoridades competentes del Estado miembro de destino, o por los operadores transfronterizos de servicios de transporte de viajeros obligados por la legislación nacional a aplicar determinadas medidas de salud pública durante la pandemia de COVID-19.

Expuesto lo anterior, no caben dudas acerca de la intrusión del Certificado COVID Digital de la UE en los datos personales de los ciudadanos y, en particular, en la intromisión de datos de categoría especial como son los datos de salud, en beneficio de otro derecho fundamental como es la movilidad entre estados miembros.

En este sentido, la Propuesta de Reglamento reconoce la existencia de posibles repercusiones en los derechos fundamentales de las personas, entre otros, el respeto a la vida privada, consagrado en el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea, y el derecho a la protección de datos personales, recogido en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea. No obstante, de acuerdo con la precitada evolución de impacto de la Propuesta de Reglamento, no se prevería ninguna excepción a la regulación vigente en materia de protección de datos personales, en la medida en que los Estados miembros habrán de aplicar normas claras, condiciones y garantías sólidas para salvaguardar dichos derechos.

En consecuencia, resulta de interés abordar, bajo el prisma de los principios de la protección de datos personales, la adecuación del Certificado COVID Digital de la UE a la normativa vigente a través de un examen de legitimidad y proporcionalidad, para conocer la repercusión de dicha medida en el derecho fundamental a la protección de datos personales y su respeto al contenido esencial de derecho, tal y como disponía la STC 186/2000, citada por la AEPD en informes en los que analiza la colisión de derechos fundamentales con el derecho a la protección de datos personales.

Brevemente, la reseñada sentencia resuelve que ningún derecho fundamental es absoluto "*pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto,*

proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho", para más adelante proporcionar los criterios que debe cumplir cualquier medida restrictiva de un derecho fundamental.

En este sentido, establece la superación del principio de proporcionalidad que tendrá lugar cuando "*cumple los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)*".

Sentado lo anterior, en los siguientes epígrafes, se analizará si el Certificado Digital de la UE, como medida diseñada para promover la libertad de circulación dentro de la UE, cumple con los citados requisitos de legitimidad y proporcionalidad.

2.2.4. Legitimación del tratamiento de datos personales en el Certificado COVID Digital de la UE.

De acuerdo con la Propuesta de Reglamento, una vez aprobada y publicada en el Boletín Oficial de la Unión Europea, constituiría una base legítima para el tratamiento de datos personales en la expedición de los certificados y de la información necesaria para confirmar y verificar la autenticidad y validez de estos. De este modo, sería aplicable la base jurídica recogida en el artículo 6, apartado 1, letra c), esto es, el cumplimiento de una obligación legal aplicable al responsable del tratamiento, junto con el artículo 9, apartado 2, letra g), interés público esencial, del RGPD.

No obstante, tal y como recoge el Considerando 40 de la Propuesta de Reglamento, en ningún caso constituiría base suficiente para la conservación de los datos personales obtenidos del certificado. En este sentido, el Certificado COVID Digital de la UE no conllevaría la creación de una base de datos central, en la medida en que los datos obtenidos no deben ser conservados por las autoridades emisoras sino que estos se mantienen en poder del portador del certificado limitándose los Estados miembros receptores u operadores transfronterizos a verificar la autenticidad del certificado aportado.

En similares términos el Considerando 48 del Reglamento 2021/953 establece la misma base de legitimación y, a mayor abundancia, faculta a los Estados miembros para determinar nuevos tratamientos con otros fines en virtud de regulación nacional.

Llama la atención que las consideraciones realizadas hasta la fecha acerca de otras soluciones tecnológicas contra la COVID-19, entre otras las Directrices emitidas por el Comité Europeo de Protección de Datos, establecían como base de legitimación del tratamiento el consentimiento del interesado, a través de la descarga voluntaria de aplicaciones informativas, seguimiento y rastreo en los dispositivos móviles.

No obstante lo anterior, la base legitimadora del Certificado Digital de la UE no se encuentra en el consentimiento del interesado, ni entendemos, podría residir en el mismo, en la medida en que sería discutible que este fuera otorgado con libertad suficiente para invocar la base legitimadora del artículo 6, apartado 1, letra a) del RGPD.

Sobre esta cuestión, podemos extrapolar algunas de las conclusiones ya publicadas por la AEPD, en relación con la toma de temperatura en espacios públicos, en las que advertía el tratamiento de datos relativos a la salud de las personas "supone una injerencia particularmente intensa en los derechos de las personas afectadas" que podría ser discriminatorio, toda vez que al realizarse generalmente en un espacio público, una eventual denegación de acceso desvelaría a terceros que la persona podría padecer o no una enfermedad como consecuencia de su temperatura corporal.

Admitiendo, tal y como señala la AEPD que el tratamiento de datos de salud en un acceso a un bien, establecimiento o servicio no puede ser libre ante la percepción por parte del usuario de que su negativa pudiera ser un riesgo para la pérdida de derechos tales como la libre circulación por la Unión, concluimos que la base legítima no puede residir en el consentimiento del interesado, siendo dicha libertad uno de los requisitos necesarios alegar dicha base legitimadora.

Inicialmente, el artículo 9 de la Propuesta de Reglamento disponía que las personas legitimadas para acceder al certificado y verificar la información únicamente serían "*las autoridades competentes del Estado miembro de destino, o por los operadores transfronterizos de servicios de transporte de viajeros obligados por la legislación nacional a*

aplicar determinadas medidas de salud pública durante la pandemia de COVID-19", no podrán acceder a los datos personales del Certificado Digital de la UE personas o entidades distintas de las reseñadas, aun contando con el consentimiento del titular, pues estarían infringiendo la normativa vigente en materia de protección de datos personales.

Actualmente, el apartado 3 del artículo 10 del Reglamento 2021/953 establece que los datos personales serán tratados por "*las autoridades competentes del Estado miembro de destino o tránsito, o por los operadores de servicios de transporte transfronterizo de viajeros obligados por la legislación nacional a aplicar determinadas medidas de salud pública durante la pandemia de COVID-19, únicamente a fin de verificar y confirmar la vacunación, el resultado de la prueba o la recuperación del titular. A tal fin, los datos personales se limitarán a lo estrictamente necesario*".

En consecuencia, ante la falta de previsión legislativa al respecto, se podría entender que un establecimiento hotelero no podría solicitar a sus huéspedes la exhibición del Certificado Digital de la UE (que anteriormente habrían mostrado en el aeropuerto) para crear un entorno seguro.

En otras palabras, lo anterior conduce a concluir que no sería posible la extensión del Certificado COVID Digital de la UE a otros ámbitos que no estén expresamente previstos en la Propuesta de Reglamento.

Si bien hemos señalado que el presente proyecto se caracteriza por su ambición y sus bondades han sido extensamente divulgadas por las autoridades correspondientes, llama la atención que no se haya ampliado a otras esferas o actividades -o no se consideren otras propuestas paralelas- que bien propulsarían las economías de los estados de la Unión Europea, tales como a establecimientos hoteleros, eventos multitudinarios, etc., con el fin de regenerar la economía creando entornos seguros.

Tampoco se habría previsto el regreso a la actividad presencial en el entorno laboral o el relajamiento de medidas de los centros escolares o universitarios, algunos de los cuales siguen imponiendo medidas dispares (tales como el mantenimiento de los llamados "grupos burbuja" cuyo coste en recursos económicos y materiales es inconmensurable) y algunas de ellas desaconsejadas por las autoridades en materia de protección de datos.

En consecuencia, cabría valorar la reticencia de las autoridades, no solo a nivel Europeo sino también estatal, de no haber promovido iniciativas legislativas adecuadas para extender el uso del Certificado COVID Digital de la UE o medidas similares a otros ámbitos, si realmente sus beneficios son superiores a las injerencias en el derecho a la protección de datos personales. De cara a futuro, habrá de estarse a las legislaciones nacionales, quienes facultadas por la redacción actual del Reglamento 2021/953, podrán extender los fines del tratamiento incluso a fines no médicos.

A título recordatorio, ya la AEPD se pronunció acerca de la posibilidad de modular el derecho a la protección de datos personales y el establecimiento del interés público como base legitimadora para el tratamiento de categorías especiales de datos como son las opiniones políticas, a través de su regulación mediante ley orgánica. En este contexto, cabría haber planteado, el establecimiento de bases legitimadoras a través de normas *ad hoc* para facilitar el tratamiento de datos personales, principalmente en datos de salud relativos a una enfermedad cuya transmisión es prácticamente indiscriminada y pone en riesgo peligro la salud pública y el sistema sanitario en conjunto.

2.2.5. Necesidad del tratamiento de datos personales en el Certificado COVID Digital de la UE.

Como señalamos anteriormente, el juicio de necesidad considera la inexistencia de otra medida más moderada para la consecución de un propósito con igual eficacia.

Para examinar la necesidad del tratamiento en materia de protección de datos, ha de tenerse en cuenta el principio de minimización de datos, desarrollado en el Considerando 39 del RGPD, por el cual los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

De acuerdo con la Exposición de Motivos de la Propuesta de Reglamento, el tratamiento de datos en el marco del Certificado Digital de la UE estaría limitado a los datos mínimos necesarios, "*incluyendo únicamente un conjunto limitado de datos personales en los certificados que deben expedirse, disponiendo que no deben conservarse los datos obtenidos al verificar los certificados y estableciendo un marco que no requiere la creación y el mantenimiento de una base de datos central*".

El conjunto limitado de datos incluido en el Certificado Digital de la UE vendría listado en el Anexo de la Propuesta de Reglamento, que asumimos, son los imprescindibles para el fin del tratamiento, que no es otro que facilitar el ejercicio por parte de los titulares de su derecho a la libre circulación durante la pandemia de COVID-19.

Si bien no se indicaría en la propuesta, se entiende que el Certificado Digital de la UE habrá de acompañarse de un documento nacional o pasaporte con fotografía, toda vez que un dispositivo electrónico no está vinculado a una persona. En este sentido, será necesario verificar que la identidad del portador del dispositivo se corresponde con la identidad de la persona que figura en el certificado digital. En definitiva, entendemos que la imagen, como dato de carácter personal, sería tratada de forma incidental, en el marco de este tratamiento.

Finalmente, en cuanto a la limitación del tratamiento conforme al principio de minimización establecido en el RGPD, cabe detenerse en el plazo de conservación de los datos recogido en el artículo 9 de la Propuesta de Reglamento, actualmente regulado en el artículo 10 del RGPD 2021/953. Así, el citado artículo de la Propuesta de Reglamento establece que no se conservarán los datos personales más tiempo del necesario para su finalidad y, en ningún caso, más allá del periodo durante el cual los certificados podrán utilizarse para ejercer el derecho a libre circulación.

Si lo anterior pudiera considerarse poco preciso, ya que no fijaría un plazo o siquiera declaración de un organismo oficial por la cual se declarara el fin o al menos el control de la actual pandemia de COVID-19, la Exposición de Motivos de la Propuesta de Reglamento incrementaba la incertidumbre en relación con el plazo de conservación de los datos personales.

En este caso, no hacía referencia siquiera a la cancelación de los datos personales recabados sino a la suspensión de sus disposiciones una vez que se haya superado la pandemia de COVID-19. Adicionalmente, preveía la reanudación del tratamiento si la OMS declarara otra pandemia del SARS-CoV-2, una variante o enfermedades infeccionas similares con potencial epidémico.

A la vista de lo anterior, cabría plantearse seriamente la alineación de los anteriores preceptos con los principios de la normativa vigente en materia de protección de datos personales y si el Certificado Digital de la UE hubiera superado el juicio de necesidad o sería necesario otra medida más moderada, o al menos, más delimitada para facilitar la libre circulación dentro de la Unión Europea durante la pandemia de COVID-19 .

Cabe advertir que en la redacción final del artículo 10 del Reglamento 2021/953 si se ha establecido finalmente un plazo límite para el tratamiento de los datos personales contenidos en los certificados, a saber, el periodo de aplicación del Reglamento 2021/953 que será el 30 de junio de 2022 constituyendo este periodo marco coherente con la normativa vigente de protección de datos.

2.2.6. Idoneidad y proporcionalidad del tratamiento de datos personales en el Certificado COVID Digital de la UE.

Al enjuiciar la idoneidad de una medida restrictiva de un derecho, ha de analizarse si dicha medida puede conseguir el objetivo propuesto. Por su parte, será necesario adicionalmente examinar, tal y como se ha señalado, si resulta ser ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto.

El Certificado COVID Digital de la UE tiene como fin promover un enfoque coordinado, predecible y transparente para el establecimiento de “vías verdes” que permitan circular libremente por la Unión de forma segura sin riesgo de transmisión de la COVID-19.

Si bien dicho fin es deseable y anhelado por todos los ciudadanos de la Unión, a saber, recobrar paulatinamente nuestros hábitos y actividades profesionales y de ocio arrebatados por la pandemia, cabría considerar si el Certificado COVID Digital de la UE contribuye a conseguir dicho objetivo o, al menos, resulta una medida útil y proporcionada, con la suficiente entidad para inferir en el derecho a la protección de datos personales.

Desde luego, el Certificado COVID Digital de la UE no es una medida activa o de lucha contra la COVID-19, que tenga capacidad suficiente para erradicar o disminuir la incidencia de infección, como puedan ser medidas de carácter sanitario tales como la vacunación. No obstante, como medida auxiliar favorecería la eficacia de esta última, aliviaría la adopción de

restricciones a la entrada de viajeros transfronterizos tales como la cuarentena o los test de detección de la COVID-19, y devolvería la confianza a sus usuarios para la reapertura de sectores económicos altamente perjudicados por la presente crisis sanitaria.

No obstante, algunas voces autorizadas, entre ellas la OMS, se han mostrado frontalmente opuestas a la utilización de pasaportes inmunológicos, toda vez que no existiría evidencia científica suficiente para asegurar que las vacunas tienen capacidad suficiente para reducir la transmisión del virus y tampoco habría suficientes estudios que corroboren la inmunidad frente al virus una vez una persona se haya recuperado de la infección.

A la vista de lo anterior, los reparos de la OMS frente a la falta de evidencia científica de la capacidad de las vacunas para frenar las contagios irían más allá de la mera declaración ya que sus efectos podrían tener, entre otros, la determinación de que el Certificado COVID Digital de la UE carece de la nota de la necesidad, en la medida que no sería actualmente lo suficientemente eficaz, para constituir una medida que interfiera en el derecho a la protección de datos personales.

De forma velada, podría entenderse que la Comisión Europea es consciente de esta realidad, en la medida en que ha reconocido que la Propuesta de Reglamento sería un instrumento suficientemente flexible como para que se incorporen nuevas pruebas y directrices científicas conforme se vayan obteniendo más datos sobre el efecto de la vacunación, las consecuencias de la aparición de nuevas variantes de la COVID-19 y el grado de protección inmunológico de las personas que hayan padecido la citada enfermedad.

A la vista de lo anterior, cabría considerar si la incertidumbre científica existente tiene suficiente entidad como para hacer decaer el juicio de idoneidad y proporcionalidad de una medida restrictiva de derechos fundamentales.

En esta tesitura, ARENAS (2020) advierte del hecho de que si una medida no es eficaz porque no contribuye a frenar la pandemia, dejaría de ser necesaria. Así, indica que la doctrina reiterada del Tribunal Europeo de Derechos Humanos señala que los Estados son los responsables de proporcionar justificaciones “pertinentes y suficientes” para limitar un derecho, por lo que serán los propios Estados quienes tendrán que demostrar que no existen medios menos restrictivos para alcanzar el fin propuesto, esto es, impedir la

propagación de la COVID-19. No obstante, si extrapolamos su análisis sobre las aplicaciones de rastreo de las que cuestiona su efectividad debido a la necesidad de concurran multitud de factores tanto tecnológicos como no tecnológicos, ARENAS (2020) concluye que estas soluciones serían necesarias en tanto no existiría otra medida más eficaz, por lo que serían proporcionales al fin perseguido, siempre y cuando cumplan los requisitos y principios propios de todo tratamiento de datos personales.

Con carácter adicional a la falta de evidencia científica, no podemos dejar de señalar la dependencia del Certificado COVID Digital de la UE a la evolución favorable de los programas de vacunación no solo de los Estados miembros, sino también de terceros países. La OMS ya había puesto de manifiesto que los pasaportes inmunológicos podrían aumentar las desigualdades y limitar la circulación de las personas no vacunadas que procederían, fundamentalmente, de países en los que los programas de vacunación estuvieran menos extendidos. Si bien este resulta ser un argumento que no pertenecería al ámbito de la protección de datos personales, llama la atención que en la Exposición de Motivos de la Propuesta de Reglamento, la Comisión Europea, entre los argumentos justificativos para promover la utilización del Certificado COVID Digital de la UE, traiga a colación el enfoque "Equipo Europa", por el cual ha proporcionado apoyo financiero, de emergencia y en especie a países de todo el mundo para contribuir en la lucha contra la COVID-19, en concreto a través del Mecanismo COVAX por el que trata de garantizar el acceso equitativo a las vacunas. Asimismo, esta dependencia de otros programas colaterales, como la vacunación o la realización de test de diagnóstico, ha quedado reflejado en el Considerando 21 del Reglamento 2021/953.

2.2.7. Necesidad de una estrategia de comunicación eficaz para optimizar los beneficios del Certificado COVID Digital de la UE

Partiendo de la premisa señalada en el Considerando 4 del RGPD por la cual el tratamiento de datos personales debe estar concebido para servir a la humanidad y que lejos de se considerado un derecho absoluto, el respeto a su normativa reguladora es compatible en circunstancias tales como la actual crisis sanitaria ocasionada por la COVID-19, no puede dejar de señalarse la necesidad de impulsar campañas divulgativas para asociar la utilización

del Certificado COVID Digital de la UE como un medio seguro tanto para viajar como para proteger la propia intimidad.

De conformidad con el principio de transparencia y el artículo 12 del RGPD, el responsable del tratamiento ha de tomar las medidas oportunas para facilitar a los interesados la información establecida en la normativa vigente, "*en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo*". Siguiendo estos preceptos, otras medidas tecnológicas diseñadas para contener la transmisión de la COVID-19, ponían a disposición de los interesados la información pertinente a efectos de dar cumplimiento al citado artículo. Cabría discernir caso por caso, si la información proporcionada en cada una de las aplicaciones era lo suficiente clara y entendible para los usuarios, de modo que quedara desde un inicio meridianamente claro los fines para los cuales serían tratados sus datos así como los efectos de la prestación o retirada del consentimiento .

No obstante lo anterior, la falta de confianza en las instituciones y la carencia de una adecuada estrategia comunicativa han abocado al fracaso a algunas de dichas soluciones toda vez que su verdadera eficacia y beneficio radicaba en su utilización por el mayor número de usuarios. En esta línea, la AEPD advirtió que las soluciones técnicas no podían considerarse de forma aislada, sino que había de tenerse en cuenta otros muchos factores que no dependen únicamente de la tecnología.

Baste señalar, a título de ejemplo, el derroche de recursos económicos que ha supuesto en España la aplicación RadarCovid cuyo desarrollo, en base al contrato suscrito con la empresa Indra Soluciones Tecnológicas de la Información, S.L.U., supuso para las arcas públicas una inversión de aproximadamente 330.537 €, cayó, en un periodo irrisorio, de tiempo en el olvido sin lograr desahogar a los servicios sanitarios.

A este respecto, no puede dejar de señalarse que los esfuerzos realizados por la Unión Europea y cada uno de los Estados miembros para establecer un marco de confianza podrían quebrar ante la falta de campañas divulgativas eficientes acerca de las medidas de seguridad adoptadas por los responsables del tratamiento y los beneficios que aportará a la libre circulación, el Certificado COVID Digital de la UE.

Así, de cara a su implementación y eficacia en los próximos meses, las comunicaciones y publicaciones de las autoridades europeas denotan cierta euforia y optimismo en dicha medida como forma de prevención y supresión coordinada de las restricciones en vigor. En este sentido, procuran transmitir a sus potenciales usuarios la necesidad y bondades de esta herramienta tecnológica para garantizar la libre circulación de forma segura.

La COMISIÓN EUROPEA (2021), consciente de esta necesidad ha subrayado que "[e]*l uso del certificado verde digital debe ir acompañado de una comunicación diáfana y transparente para explicar a los ciudadanos su alcance y su utilización, aclararles las salvaguardias de protección de los datos personales y tranquilizarlos, especificándose que se trata de una herramienta para ayudarles a disfrutar plenamente de sus derechos de libre circulación*."

Asimismo, ha quedado reflejada la exigencia de una comunicación eficaz para garantizar la seguridad jurídica en el Considerando 56 del Reglamento 953/2021 de acuerdo con el siguiente tenor literal: "[u]*na comunicación clara, completa y oportuna al público, incluidos los titulares, sobre la finalidad, la expedición y la aceptación de cada tipo de los certificados que conforman el certificado COVID digital de la UE es crucial para garantizar la previsibilidad de los viajes y la seguridad jurídica. La Comisión debe apoyar los esfuerzos de los Estados miembros a este respecto, por ejemplo, facilitando la información que proporcionen los Estados miembros en la plataforma web «Re-open EU*".

Sentado lo anterior, no es posible negar la necesidad de transmitir al principal beneficiario de la normativa de protección de datos personales, esto es, las personas físicas, los beneficios de utilizar esta solución tecnológica para sus desplazamientos que, además, conllevarán de forma incidental la adopción de otras medidas que si tienen efectos directos para la contención de la pandemia, como es la vacunación o la realización de pruebas diagnósticas con carácter previo a los desplazamientos.

3. Conclusiones

El derecho fundamental a la protección de datos no es un derecho de reciente reconocimiento. Al contrario, algunos autores advierten su aparición a partir del siglo XIX, como resultado de la disgregación del derecho a la intimidad a raíz del desarrollo tecnológico que evoluciona de forma natural hasta ser un derecho independiente que protege un bien jurídico distinto.

No obstante lo anterior, en Europa, la conciencia social de las personas a las que el reseñado derecho protege ha despertado principalmente a raíz de la promulgación del RGPD. Si bien la aparición de tecnologías y medios de comunicación a través de los cuales los ciudadanos compartían datos personales, unas veces de forma deliberada y otras de manera inconsciente, son anteriores, podría decirse que a nivel social el RGPD supuso la puesta de manifiesto de que el potencial de las nuevas tecnologías para analizar y cruzar datos es inmensa y que requiere de control, no solo por parte de las autoridades competentes sino por los propios titulares del derecho, en quienes reside la última palabra.

Sin perjuicio de los esfuerzos realizados por parte de las agencias europeas en materia de protección de datos por divulgar y difundir las herramientas que se encuentran a disposición de los ciudadanos, es un derecho de compleja interpretación cuya necesidad y beneficios no han sido debidamente transmitidos a sus destinatarios. En ocasiones, no sólo las personas físicas desconocen el marco jurídico del que disponen para hacer valer sus derechos sino que los operadores económicos, tanto públicos como privados, desconocen también sus obligaciones como responsables y encargados del tratamiento.

En este contexto, la única certeza es que cualquier materialización de una infracción en el cumplimiento de las obligaciones establecidas en la legislación reguladora del derecho a la protección de datos personales, puede dar lugar a consecuencias devastadoras, como por ejemplo, la revelación de datos bancarios de miles de clientes, la creación de perfiles individualizados y su puesta a disposición para llevar a cabo técnicas comerciales o propagandísticas agresivas, etc.

Adicionalmente, cabe señalar que es un derecho que depende en gran medida de la confianza de los titulares en que las instituciones y las entidades privadas tratarán sus datos conforme a la legislación aplicable.

La actual situación de pandemia ha forzado a la utilización de las nuevas tecnologías en diferentes ámbitos de la vida privada (teletrabajo, etc.) lo que irremediablemente ha avivado el debate, a todos los niveles, sobre la capacidad y oportunidad de la normativa vigente en regular este derecho fundamental. Asimismo, dicho debate se ha producido erróneamente desde una perspectiva dicotómica, es decir, bajo la premisa de que el ejercicio del derecho a la protección de datos excluye el completo ejercicio de otros derechos fundamentales tales como la salud, o la libre circulación, teniendo que elegir uno de ellos.

Esto es así, en la medida en que para prevenir y evitar la propagación de la COVID-19 se han venido analizando y, en ocasiones, implantando, soluciones tecnológicas con mayor o menor fortuna, que aparentemente obligan al usuario a sacrificar el legítimo tratamiento de sus datos personales para preservar otro derecho fundamental.

Como se ha analizado en el presente trabajo, la propia normativa reguladora del derecho a la protección de datos reconoce que no es un derecho absoluto y que puede quedar supeditado al ejercicio de otros derechos. No obstante, en un escenario de crisis como el actual, la totalidad de sus principios son aplicables y necesarios y los responsables y encargados del tratamiento, en mayor medida, deben dar cumplimiento a sus preceptos para salvaguardar los derechos de las personas físicas.

Sentado lo anterior, cabe indicar que la velocidad en la toma de decisiones junto con la falta de reflexión, las rectificaciones de las autoridades competentes en la lucha contra la pandemia, etc. han minado en ocasiones la confianza en las instituciones, quienes en última instancia son responsables del tratamiento de datos de especial protección o, en su caso, vigilantes de su cumplimiento por parte de los operadores económicos.

Esta incapacidad para transmitir confianza en los titulares de los datos, quienes no tienen la garantía de que sus datos personales estarán siendo debidamente tratados conforme a los fines previamente informados o debidamente protegidos frente a potenciales amenazas, ha provocado, entre otras, la falta de adhesión a las medidas tecnológicas diseñadas para la

lucha contra la COVID-19. En este sentido, la efectividad de dichas medidas tecnológicas dependía en gran parte de que un porcentaje mayoritario de la población otorgara su consentimiento para el tratamiento de sus datos personales. Sin embargo, la falta de confianza ha provocado que grandes inversiones económicas en el desarrollo de aplicaciones o *apps* y otras soluciones tecnológicas hayan quedado difuminadas por la falta de penetración entre los potenciales usuarios.

Asimismo, cabe reseñar la falta de coordinación entre Estados y, en particular en España, entre autonomías. Resulta especialmente llamativa la falta de unificación de medidas en nuestro país, baste así recordar las numerosas aplicaciones de rastreo aparecidas en España y su nimia eficacia.

Tal y como hemos visto a lo largo del presente trabajo, se han puesto en marcha nuevas soluciones tecnológicas que refuercen la efectividad de la vacuna contra la COVID-19, tales como el Certificado COVID Digital de la UE que si bien ha sido diseñado muy meticulosamente, genera ciertas dudas acerca de su respeto a los principios establecidos en el RGPD.

A este respecto, la experiencia generada a lo largo del año 2020 ha enseñado a las autoridades que tan importante es el diseño de dichas soluciones tecnológicas como la necesidad de infundir confianza en los usuarios combatiendo la desinformación y realizando campañas de publicidad transparentes para, tal y como indica la Comisión Europea, “tranquilizarlos” y empoderar a los ciudadanos para que puedan disfrutar plenamente de todos sus derechos en la Unión Europea.

Referencias bibliográficas

Bibliografía básica

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *El uso de las tecnologías en la lucha contra el COVID19. Un análisis de costes y beneficios*. 2020. Disponible en:

https://www.aepd.es/sites/default/files/2020-05/analisis-tecnologias-COVID19.pdf

AGENCIA ESPAÑOLA DE AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Informe (N/REF: 0017/2020), en el que analiza cuestiones relativas a la actual situación derivada de la extensión del virus COVID-19*. 2020. Disponible en:

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

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Informe (N/REF: 0036/2020), en el que analiza cuestiones relativas al uso de técnicas de reconocimiento facial para realizar pruebas de evaluación online ante la situación de crisis sanitaria ocasionada por el COVID-19*. 2020. Disponible en:

https://www.aepd.es/es/documento/2020-0036.pdf

AMNISTÍA INTERNACIONAL. Informe 2020/21, *Análisis global y perspectivas regionales. Amnistía Internacional*, 2021. Disponible en:

https://www.amnesty.org/download/Documents/POL1032022021SPANISH.PDF

ANDRÉS RICART, G. La vacuna contra la COVID-19 y la Protección de Datos. *Aranzadi Digital.* 2021, núm. 1. [consulta: mayo de 2021]. Disponible en:

https://insignis.aranzadidigital.es/maf/app/document?srguid=i0ad82d9b0000017a5888a421b029b2b4&marginal=BIB\2021\1008&docguid=I6aa31940662c11ebb737837ae918d438&ds=ARZ_LEGIS_CS&infotype=arz_biblos;&spos=1&epos=1&td=0&predefinedRelationshipsType=documentRetrieval&global-result-list=global&fromTemplate=&suggestScreen=&&selectedNodeName=&selec_mod=false&displayName=

ARENAS RAMIRO, M. ¿Rastrear o no rastrear? He ahí la cuestión. Las apps de rastreo de contactos y la protección de datos personales. *La Ley Privacidad*. 2020, núm. 5. [consulta en: mayo de 2021]. Disponible en:

https://laleydigital.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1CTEAAmNDY3NLU7Wy1KLizPw827DM9NS8klS1zGLHgoKi_LLUFFsjAyNDAzMjS0MLAwMA1ke76jgAAAA=WKE

CAZURRO BARAHONA, V. *Antecedentes y fundamentos del Derecho a la protección de datos*. 1ª ed. J.B. Bosch Editor, 2020.

CERVERA NAVAS, L; PACHECO COSTA, G; PERIS BRINES, N. *2020:* un año de desafíos globales para la protección de datos. La Ley Digital. 2020. [consulta: marzo de 2021]. Disponible en: https://laleydigital.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEABXMwQrEIAwE0K9Zz4ndVj3ksNBPKHu3GkpgqaVav3_jwlOBgWlxr4QAL5cGVJN6q1ktyimvwtjBxNSe-FtLIhxdOm9xHxdGcqZ1A80E3gUwne8q5aSvHHw2NlI_13WXzpksWITFBvQAfw7jMjqEAAAAWKE

COMISIÓN EUROPEA. Recomendación (UE) 2020/518 de la Comisión de 8 de abril de 2020 relativa a un conjunto de instrumentos comunes de la Unión para la utilización de la tecnología y los datos a fin de combatir y superar la crisis de la COVID-19, en particular por lo que respecta a las aplicaciones móviles y a la utilización de datos de movilidad anonimizados, de 14 de abril de 2020. DOUE, 14 de abril de 2020, número 114. Disponible en:

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32020H0518&from=ES

COMISIÓN EUROPEA. Comunicación (2020/C124) de la Comisión, orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de covid-19 en lo referente a la protección de datos, de 17 de abril de 2020. DOUE, 17 de abril de 2020, número 124. Disponible en:

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=ES

CONSEJO EUROPEO. Recomendación (UE) 2021/119 del Consejo, de 1 de febrero de 2021, por la que se modifica la Recomendación (UE) 2020/1475 sobre un enfoque coordinado de la restricción de la libre circulación en respuesta a la pandemia de COVID-19, de 2 de febrero de 2021. DOUE, 2 de febrero de 2021, número 36. Disponible en:

https://www.boe.es/doue/2021/036/M00001-00006.pdf

COTINO HUESO, L. Inteligencia artificial, Big Data y aplicaciones contra la COVID-19: privacidad y protección de datos. *IDP. Internet, Derecho y Política*. 2020, núm. 31, pp. 1-17. [consulta: abril 2021]. ISSN 1699-8154. Disponible en:

https://dialnet.unirioja.es/servlet/articulo?codigo=7633148

DOMÍNGUEZ ÁLVAREZ, J. L., La tutela jurídica de la protección de datos de carácter personal en el horizonte post COVID-19. Nuevos compromisos para las Administraciones públicas. *Revista Aranzadi de Derechos y Nuevas Tecnologías.* 2021, núm. 55. [consulta: mayo 2021]. Disponible en:

https://insignis.aranzadidigital.es/maf/app/document?srguid=i0ad82d9a0000017a588cca928c965dd3&marginal=BIB\2021\1470&docguid=I0fece2f078a211ebb5bdb02ec177fcb7&ds=ARZ_LEGIS_CS&infotype=arz_biblos;&spos=1&epos=1&td=0&predefinedRelationshipsType=documentRetrieval&global-result-list=global&fromTemplate=&suggestScreen=&&selectedNodeName=&selec_mod=false&displayName=

NAVAL PARRA, M. La protección de datos personales en la lucha contra la propagación del Coronavirus. *La Ley Digital*, 2020. [consulta en: abril de 2021] Disponible en:

https://laleydigital.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAAEAE2QwU7DMAyGn2a5VELZxjp2yIFuR4QQFO5eYtqI4HSJ061vj0s5EOlTIv2f4l--FExTizc2AaohRUZr_apo_bmlymHlgGOuBkw5EgTMFVIlZii2B5UnijR9mzYVVAznbNZar_Z2Zi1shXthJ9TCXngQDnOuFVguEE7RmvX89iO2cDa1islhaiajFUeG8IrZbHYq9_H6DKPvgH2kBtIy1jtnTq2Ws9WHTb1Ro3QVwXz4DolR9b7rnwRe_IyQbP8CHZqm5EtBB3eQh5sK9CVV3n7jRR09Xo0nh7cjJPdIbt6T8vmdpGqG8N9dvm0Ks4w-My2ZskHuEzAeZXnk_kr_AFEjwZd1AQAAWKE

RAMS RAMOS, L. El derecho fundamental a la protección de datos de carácter personal como límite ¿(in)franqueable? Para la transparencia administrativa. Estudios de Deusto. 2018, vol 66, núm 2, pp. 119-152. [consulta: abril de 2021]. ISSN 0423-4847. Disponible en:

https://dialnet.unirioja.es/servlet/articulo?codigo=6746632

Bibliografía complementaria

AGENCIA ESPAÑOLA DE AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Informe (N/REF: 210070/2018), sobre el tratamiento de datos relativos a opiniones políticas por los partidos políticos al amparo del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General. Disponible en:

https://www.aepd.es/sites/default/files/2019-09/2018-0181-tratamiento-datos-opiniones-politicas-por-partidos-polticos.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Comunicado de la AEPD en relación con la toma de temperatura por parte de comercios, centros de trabajo y otros establecimientos, 2020. Disponible en:

https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-aepd-temperatura-establecimientos

COMISIÓN EUROPEA. Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo y al Consejo. Por una senda común hacia una reapertura segura y sostenida, 2021. Disponible en:

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52021DC0129&from=ES

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS. Directrices 03/2020 sobre el tratamiento de datos relativos a la salud con fines de investigación científica en el contexto del brote de COVID-19. Disponible en:

https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-032020-processing-data-concerning-health-purpose_es

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS. Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-19. Disponible en:

https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-042020-use-location-data-and-contact-tracing-tools_es

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, 2014. Disponible en:

https://www.aepd.es/sites/default/files/2019-12/wp217_es_interes_legitimo.pdf

LEIVA ESCUDERO, G. Constitucionalidad de las restricciones a la libertad de circulación en el estado de alarma por el coronavirus Covid-19. Diario La Ley. 2020, núm. 9642 [consulta: junio 2021]. Disponible en: https://diariolaley.laleynext.es/content/Inicio.aspx

ORGANIZACIÓN MUNDIAL DE LA SALUD. Declaración sobre la reunión del Comité de Emergencia del Reglamento Sanitario Internacional (2005) acerca del brote de nuevo coronavirus (2019-nCoV). Disponible en:

https://www.who.int/es/news/item/23-01-2020-statement-on-the-meeting-of-the-international-health-regulations-(2005)-emergency-committee-regarding-the-outbreak-of-novel-coronavirus-(2019-ncov).

Legislación citada

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, DOUE, 15 de junio de 2021, número 211. Disponible en:

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32021R0953&from=ES

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), DOUE, 4 de mayo de 2016, número 119. Disponible en:

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a un marco para la expedición, verificación y aceptación de certificados interoperables de vacunación, de test y de recuperación para facilitar la libre circulación durante la pandemia de COVID-19 (certificado verde digital). Disponible en:

https://eur-lex.europa.eu/resource.html?uri=cellar:38de66f4-8807-11eb-ac4c-01aa75ed71a1.0014.02/DOC_1&format=PDF

Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a un marco para la expedición, verificación y aceptación de certificados interoperables de vacunación, de test y de recuperación para los nacionales de terceros países que residan legalmente o se encuentren legalmente en el territorio de los Estados miembros durante la pandemia de COVID-19 (certificado verde digital). Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52021PC0140&from=ES

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, número 294, Referencia: BOE-A-2018-16673. Disponible en:

https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, Boletín Oficial del Estado, 14 de diciembre de 1999,número 298, Referencia: BOE-A-1999-23750. Disponible en:

https://www.boe.es/buscar/pdf/1999/BOE-A-1999-23750-consolidado.pdf

Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública, Boletín Oficial del Estado, 29 de abril de 1986, número 102, Referencia: BOE-A-1986-10498. Disponible en: https://www.boe.es/buscar/pdf/1986/BOE-A-1986-10498-consolidado.pdf

Jurisprudencia citada

Sentencia de la Sala Primera del Tribunal Constitucional, número 186/2000, de 10 de julio. Boletín Oficial del Estado, 11 de agosto de 2000, número 192, ECLI:ES:TC:2000:186. Disponible en:

http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4170#complete_resolucion